

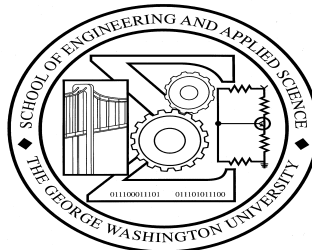
Growing Development of Foreign Encryption Products in the Face of U. S. Export Regulations

Lance J. Hoffman
David M. Balenson
Karen A. Metivier-Carreiro
Anya Kim
Matthew G. Mundy

June 10, 1999
Report GWU-CPI-1999-02

Cyberspace Policy Institute

The George Washington University
School of Engineering and Applied Science
2033 K St. NW Suite 340 • Washington, DC 20006
Phone: 202.994.5512 • Fax: 202.994.5505
Website: <http://www.seas.gwu.edu/seas/institutes/cpi/>
Email: cpi@seas.gwu.edu



GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS IN THE FACE OF U.S. EXPORT REGULATIONS

Lance J. Hoffman*
David M. Balenson**
Karen A. Metivier-Carreiro*
Anya Kim*
Matthew G. Mundy**

June 10, 1999
Report No. GWU-CPI-1999-02

*Cyberspace Policy Institute, School of Engineering and Applied Science, The George Washington University, Washington, DC

**NAI Labs, The Security Research Division of Network Associates, Inc., Glenwood, MD

This research was supported in part by Americans for Computer Privacy (ACP).

EXECUTIVE SUMMARY

Development of cryptographic products outside the United States is not only continuing but is expanding to additional countries; with rapid growth of the Internet, communications-related cryptography especially is experiencing high growth, especially in electronic mail, virtual private network, and IPsec products. This report surveys encryption products developed outside the United States and provides some information on the effect of the United States export control regime on American and foreign manufacturers.

We have identified 805 hardware and/or software products incorporating cryptography manufactured in 35 countries outside the United States. The most foreign cryptographic products are manufactured in the United Kingdom, followed by Germany, Canada, Australia, Switzerland, Sweden, the Netherlands, and Israel in that order. Other countries accounted for slightly more than a quarter of the world's total of encryption products. A full summary listing of the foreign cryptographic products can be found in an appendix to the report.

The 805 foreign cryptographic products represent a 149-product increase (22%) over the most recent previous survey in December 1997. A majority of the new foreign cryptographic products are software rather than hardware. Also, a majority of these new products are communications-oriented rather than data storage oriented; they heavily tend towards secure electronic mail, IP security (IPsec), and Virtual Private Network applications.

We identified at least 167 foreign cryptographic products that use strong encryption in the form of these algorithms: Triple DES, IDEA, BLOWFISH, RC5, or CAST-128. Despite the increasing use of these stronger alternatives to DES, there also continues to be a large number of foreign products offering the use of DES, though we expect to see a decrease in coming years.

New cryptography product manufacturers have appeared in six new countries since December 1997, and there has been a large increase in the number of products produced by certain countries. The new countries are Estonia, Iceland, Isle of Man, Romania, South Korea, and Turkey. The United Kingdom jumped by 20 products from 119 to 139, and Germany jumped from 76 products to 104. Also notable was Japan's increase, from six products to 18, and Mexico's, from a single product to six at the present time.

We identified a total of 512 foreign companies that either manufacture or distribute foreign cryptographic products in at least 67 countries outside the United States. A full summary listing of these is given in an appendix to the report.

On average, the quality of foreign and U. S. products is comparable. There are a number of very good foreign encryption products that are quite competitive in strength, standards compliance, and functionality.

We present sketches of some representative competitors to U.S. manufacturers of software and hardware with encryption capabilities; all are developing products with

strong encryption and have as customers a number of large foreign or multinational corporations. The specific companies highlighted are Baltimore Technologies, Brokat, Check Point, Data Fellows, Entrust, Radguard, Seguridata Privada, Sophos, and Utimaco.

We found some examples of advertising used by non-U. S. companies that generally attempted to create a perception that purchasing American products may involve significant red tape and the encryption may not be strong due to export controls. This almost always appeared on Web sites.

We observed that companies vie to have encryption products that meet certain accepted worldwide standards. Encryption experts from all over the world have contributed to two important international standards efforts, IPsec and the Advanced Encryption Standard..

Finally, we suggested that our empirical product data could be combined with economic measures and economic theories to better explain why we are seeing the observed growth and to examine the effects of Internet growth, e-commerce development, and regulatory actions on the international cryptographic market over time, thus getting better insights into the implications of various policy options.

CONTENTS

1. INTRODUCTION.....	1
2. PRIOR WORK	2
2.1 U.S. Department of Commerce / National Security Agency Study	2
2.2 National Research Council CRISIS Report	2
2.3 President's Export Council Subcommittee on Encryption Report	3
3. SURVEY OF CRYPTOGRAPHIC PRODUCTS OUTSIDE THE U.S.....	4
3.1 Overview.....	4
3.2 Data Collection Methodology	5
3.3 Results of Update to Cryptographic Products Survey.....	5
3.3.1 <i>More "Strong" Encryption is on the Market</i>	6
3.3.2 <i>New Countries and Growth Countries for Cryptographic Products</i>	8
3.3.3 <i>Growing Numbers of Foreign Products & Companies</i>	8
3.3.4 <i>Quality of Foreign Cryptographic Products</i>	9
4. SOME COMPETITORS TO U. S. PRODUCTS EMPLOYING CRYPTOGRAPHY ..	10
5. FOREIGN MARKETING USE OF U. S. EXPORT CONTROLS.....	17
5.1 Introduction	17
5.2 Advertising Related to Cryptographic Controls.....	17
6. STANDARDS AND THEIR INFLUENCE.....	22
6.1 Pervasiveness of Standards.....	22
6.1.1 <i>IPsec</i>	22
6.1.2 <i>Advanced Encryption Standard (AES)</i>	22
7. CONCLUSIONS	24
7.1 Foreign Development of Cryptography Continues to Grow	24
7.2 Communications-Related Cryptography Leads Storage Cryptography	24
8. FUTURE RESEARCH	25
9. REFERENCES.....	27
APPENDICES.....	32
A. CALL FOR INFORMATION	33
B. SUMMARY LISTING OF FOREIGN CRYPTOGRAPHIC PRODUCTS	36
C. FOREIGN ENCRYPTION MANUFACTURERS AND DISTRIBUTORS BY COUNTRY	47
D. REPORT OF THE PRESIDENT'S EXPORT COUNCIL SUBCOMMITTEE ON ENCRYPTION, WORKING GROUP ON INTERNATIONAL ISSUES.....	53

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

1. INTRODUCTION

This project has three main goals: to provide a comprehensive survey of foreign encryption products available worldwide; to identify specific foreign competitors likely to present a significant economic threat to U. S. manufacturers of software and hardware with encryption capabilities; and to provide evidence, if found, of potential threats to U. S. leadership in information technology as a result of U. S. export regulations on encryption products.

While this work was undertaken within a very short time frame, and with limited resources, it still provides much new evidence to support the conclusions in Section 7. This evidence can be augmented with additional information as time permits. We do not offer opinions or analysis of key escrow or recovery policies, do long-term technological forecasting, or offer detailed political/social analysis of export control policies. Our goal is to provide an accurate, up-to-date survey of encryption products developed outside the United States and to provide some information on the United States export control regime and its effect on American and foreign manufacturers.

2. PRIOR WORK

One of our first tasks in this project was to examine prior relevant work. Several important documents were studied in this regard.

2.1 U.S. Department of Commerce / National Security Agency Study

The U.S. Department of Commerce Bureau of Export Administration (BXA) and the National Security Agency (NSA) jointly issued a study [Commerce/NSA Study 1996] that assessed the then current and future market for software products containing encryption and the impact of export controls on the U.S. software industry. Quoting from the press release that accompanied the study, " ... The study found that the U.S. software industry still dominates world markets. In those markets not offering strong encryption, U.S. software encryption remains the dominant choice. However the existence of foreign products with labels indicating DES (Data Encryption Standard) or other strong algorithms, even if they are less secure than claimed, can nonetheless have a negative impact on U.S. competitiveness. The study also notes that the existence of strong U.S. export controls on encryption may have discouraged U.S. software producers from enhancing security features of general purpose software products to meet the anticipated growth in demand by foreign markets. All countries that are major producers of commercial encryption products were found to control exports to some extent. The study found that because customers lack a way to determine actual encryption strength, they sometimes choose foreign products over apparently weaker U.S. ones, giving those foreign products a competitive advantage." [U.S. DoC 1996]

2.2 National Research Council CRISIS Report

A report [CRISIS 1996] was published in 1996 by the National Research Council's Committee to Study National Cryptography Policy. It examined a number of issues related to our study. Based on work by a committee chaired by former Deputy Secretary of State Kenneth Dam and populated by a number of professionals from the law, intelligence, and computer science communities, it concluded that the United States should promote widespread commercial use of technologies that can prevent unauthorized access to electronic information, that the export of the Data Encryption Standard (DES) should be allowed to provide (what was then considered) an acceptable level of security, and that the United States should progressively relax but not eliminate export controls.

The report also states "widespread commercial and private use of cryptography in the U.S and abroad is inevitable in the long run and its advantages, on balance, outweigh the disadvantages". The committee concludes by noting "the interests of the government and the nation would be best served by a policy that fosters a judicious transition toward a broad use of cryptography".

2.3 President's Export Council Subcommittee on Encryption Report

The President's Export Council Subcommittee on Encryption (PECSENC) is chartered by the Secretary of Commerce to provide the private and public sector with the opportunity to advise the U.S. Government on the future of commercial encryption export policy. The members of the PECSENC consist of representatives from industry, academia, nonprofit foundations, state and local law enforcement, and elsewhere in the private sector. In September 1998, its Working Group on International Issues issued a report [PECSENC 1998, included as Appendix D] that found "the difference between U.S. encryption controls and those of other nations is a serious -- but not the only -- factor determining success in the computer security market." It also concluded that, "the adverse impact of controls on U.S. industry is palpable. For many software applications, business customers simply demand security and encryption; it is a checklist item, and its absence is a deal breaker."

The report also highlighted an example of a non-U. S. company using the difference in export control regimes as "leverage" to ultimately attempt to dominate particular applications:

"... Brokat, a German company that scarcely existed four years ago, now has 250 employees and offices in several countries including the United States. Brokat's specialty is Internet banking and electronic commerce, but it broke into that business on the strength of being able to offer stronger encryption than German banks could obtain in Netscape or Microsoft browsers. It is now a major player in this niche, with 50% of the European Internet banking market and enough U.S. customers to justify a 20-person U.S. branch office. Meanwhile, encryption constitutes 10% or less of Brokat's revenue, and it has expanded its initial Internet banking offerings to include support for other forms of electronic commerce. Loss of U.S. competitiveness in the electronic commerce software market obviously raises concerns not just about encryption software but other software opportunities. Indeed, it foreshadows a weakening of the U.S. position as a leader in electronic commerce generally."

The report also was concerned that "the persistent emphasis in U.S. export control policy over the past two years on key recovery, or "lawful access," has also taken a toll on the credibility of U.S. security products. ... Foreign governments and competitors, particularly in Europe, have misinterpreted this U.S. policy, perhaps deliberately. In essence, foreign customers are told often by their governments as well as local security companies that all U.S. encryption products come with a back door allowing the U.S. government to read the contents. In part this is the result of outmoded "Recovery" supplements to U.S. export rules that demand an unrealistic level of U.S. government access to key recovery products."

3. SURVEY OF CRYPTOGRAPHIC PRODUCTS OUTSIDE THE U.S.

3.1 Overview

The principal investigator and the subcontractor of this current project also studied the worldwide availability of cryptographic products since April 1993 as part of what has become known as the "TIS Survey" [TIS 1997]. The results of this earlier work have been presented to the Computer Systems Security and Privacy Advisory Board (CSSPAB) of the National Institute of Standards and Technology (NIST) and presented by Stephen T. Walker, President of Trusted Information Systems, to two Congressional subcommittees [Walker 1993, Walker 1994]. The survey was also provided to numerous government agencies and departments as part of their efforts to understand the availability of cryptographic products and its impact on U.S. export control policies.

The TIS Survey continued until December 1997, at which time it identified 656 foreign cryptographic products from 29 countries. The survey also identified 963 domestic products, for a worldwide total of 1619 products produced and distributed by 949 companies (474 foreign and 475 domestic) in at least 68 countries.

Our goal for this current study was to update the foreign product portion of the TIS Survey. We focused mainly on discovering new products from foreign manufacturers and also spent some time updating entries for the existing foreign products in the database.

Information collected by the TIS Survey was assembled into an MS Access database. The database includes two tables, one for cryptographic products and a second table for companies that either produce or distribute cryptographic products. Each entry in the product table includes the following information:

Name/Version

Manufacturer and Country

Platforms

- PC, Mac, Workstation, Mainframe, DOS, Windows, UNIX, etc.

Interfaces

- RS232, X.21, X.25, V.21, V.24, RJ-11, etc.

Type

- HW, SW, HW/SW combo

What It Encrypts

- Data, Files, Directories, Disks, Communications, Voice, Fax, Tape, Email, etc.

Embodiment

- Program, Kit, Chip, Board, Box, Tokens, PCMCIA, Smart Card, Phone, etc.

Cryptographic Algorithms

- DES, Triple DES (3DES), Blowfish, IDEA, CAST, Proprietary, RC2/4/5, SKIPJACK, Stream Ciphers, RSA, El Gamal, DH, DSA, ECC, MD2/4/5, SHA-1, etc.

How Distributed

- Mass-Market, Direct, Shareware, Internet, etc.

Company Information

- Name, Country, Address, Contact Information, etc.

3.2 Data Collection Methodology

We used the following methods of data collection: issue a call for information and examine the results, plumb existing work available to us, and use the World Wide Web to conduct searches for new products and information.

The call for information to elicit information from the computer cryptography community regarding new products (Appendix A) was posted in the following newsgroups and mailing lists (IETF is the Internet Engineering Task Force [IETF]):

- sci.crypt newsgroup: discussion of the science of cryptology, including cryptography, cryptanalysis, and related topics such as one-way hash functions.
- Risks mailing list: describes many of the technological risks that happen in today's environment.
- Cypherpunks mailing list: forum for discussing cryptography, privacy, and related social issues.
- Cryptography mailing list: mailing list devoted to cryptographic technology and its political impact.
- Firewalls mailing list: discussion of Internet "firewall" security systems and related issues.
- IETF Web Transaction Security (wts) Working Group mailing list: discussion of the development of requirements and a specification for the provision of security services to Web transaction.
- IETF Secure Shell (secsh) Working Group mailing list: discussion of efforts to update and standardize the SSH protocol.
- IETF IP Security Protocol (ipsec) Working Group mailing list: discussion of the standards efforts on IP Security.
- IETF An Open Specification for Pretty Good Privacy (openpgp) Working Group mailing list: discussion of extending the current PGP protocol.

The Call and Survey were also posted on the Web site of the Cyberspace Policy Institute of The George Washington University [CPI 1999]. Additionally, project team members sent the survey out to individuals who they believed might know of foreign products.

The existing work available to us included trade magazines, journals, buyers guides [CSI, ICISA Survey], and other print material.

Most of our new information on foreign cryptography products was found by using Web search engines and gathering information from Web pages.

3.3 Results of Update to Cryptographic Products Survey

Our effort to update the cryptographic products survey focused mainly on discovering new products from foreign producers, but also involved updating information on some of the existing foreign products in the database. Since we did not set out to update information on cryptographic products produced in the U.S., the number of domestic cryptographic products changed only slightly (when we came across something and thus updated the information). However, we expect that the number of cryptographic products produced in the U.S. has in fact

also increased. NAI Labs plans to further update the domestic portion of the survey in the near future.

The updated foreign cryptographic product survey (see summary table on following page) now identifies a total of 805 hardware and/or software products incorporating cryptography manufactured in 35 countries outside the United States. The most foreign cryptographic products are manufactured in the United Kingdom, followed by Germany, Canada, Australia, Switzerland, Sweden, the Netherlands, and Israel in that order. Other countries accounted for slightly more than a quarter of the world's total of encryption products. A full summary listing of the foreign cryptographic products can be found in Appendix B.

The 805 foreign cryptographic products resulting from the current update represents a 149-product increase over the December 1997 survey. A majority of the new foreign cryptographic products are software rather than hardware.

Another notable finding is that a majority of new foreign cryptographic products are oriented toward communications rather than data storage applications; and these heavily tended towards secure electronic mail, IP security (IPsec), and Virtual Private Network (VPN) applications. The results also showed a lot of activity in IPsec implementation, which is likely prompted by the recent emergence of new IPsec specifications from the IETF [IPSEC].

The updated foreign cryptographic product survey also identified a total of 512 foreign companies that either manufacture or distribute foreign cryptographic products in at least 67 countries outside the United States. A full summary listing of these is given in Appendix C.

3.3.1 More "Strong" Encryption is on the Market

The updated foreign cryptographic products survey also showed increasing use of "strong" alternative cryptographic algorithms to DES, which uses a 56-bit key. Altogether, we identified at least 167 foreign cryptographic products that use Triple DES, IDEA, BLOWFISH, RC5, or CAST-128, which support larger key lengths. Despite the increasing use of these stronger alternatives to DES, there also continues to be a large number of foreign products offering the use of DES, though we expect to see a decrease in coming years.

We identified at least 123 foreign cryptographic products that use Triple DES, which employs either two traditional DES keys, for an effective key length of 112 bits, or three DES keys, for an effective key length of 168 bits.

We identified at least 54 foreign cryptographic products that use the International Data Encryption Algorithm (IDEA), a Swiss-developed symmetric block cipher with a 128-bit key length [Lai 1990, Lai 1991].

We identified at least 36 foreign cryptographic products that use BLOWFISH, a symmetric block cipher developed by Bruce Schneier with a variable key length ranging from 32 to 448 bits [Schneier 1993, Schneier 1994]. Many of these products appear to use BLOWFISH with the full 448-bit key length.

We identified at least 2 foreign cryptographic products that use RC5, a symmetric block cipher developed by Ron Rivest (one of the RSA inventors) with a variable length key up to 2040 bits [Rivest 1996].

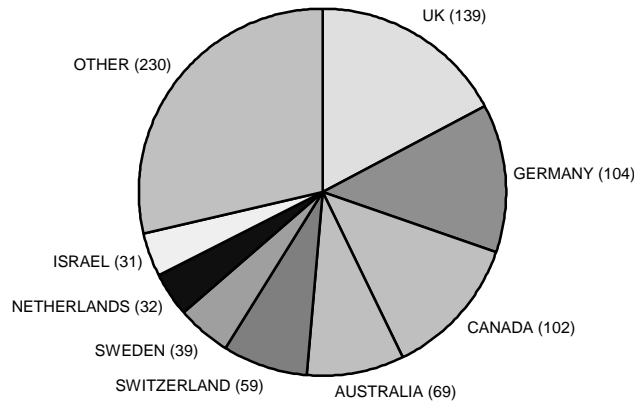
We identified at least 12 foreign cryptographic products that use CAST-128, a symmetric block cipher developed by Carlisle Adams of Entrust Technologies in Canada with a variable length key up to 128 bits [Adams 1997].

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

Foreign Cryptographic Survey Results (as of May 1999)

The updated survey identified a total of 805 foreign cryptographic products from 35 countries:

- | | | |
|-----------|--------------|----------------|
| Argentina | Australia | Austria |
| Belgium | Canada | Czech Republic |
| Denmark | Estonia | Finland |
| France | Germany | Greece |
| Hong Kong | Iceland | India |
| Iran | Ireland | Isle Of Man |
| Israel | Italy | Japan |
| Mexico | Netherlands | New Zealand |
| Norway | Poland | Romania |
| Russia | South Africa | South Korea |
| Spain | Sweden | Switzerland |
| Turkey | UK | |



At least 167 of these foreign cryptographic products implement "strong" cryptographic algorithms, including Triple DES, IDEA, BLOWFISH, RC5, or CAST.

We identified 512 foreign cryptography companies (including distributors as well as manufacturers) in at least 67 countries.

Table 1. Foreign cryptographic products survey results

3.3.2 *New Countries and Growth Countries for Cryptographic Products*

The update identified six new countries producing cryptographic products. The countries that have started producing encryption products since December 1997 are Estonia, Iceland, Isle of Man, Romania, South Korea, and Turkey.

We also noticed a large increase in the number of products produced by certain countries, such as the United Kingdom, which jumped by 20 products from 119 to 139, and Germany, which jumped from 76 products to 104.

Japan also showed a large increase, jumping from 6 products in the December 1997 survey to 18 products in the updated survey. Most of the new products come from Mitsubishi Electronic Corporation, which has introduced a number of hardware and software cryptographic products that make use of a Japanese cryptographic algorithm known as MISTY, which uses a 128-bit key, as well as Triple DES [Matsui 1996, MISTY].

Mexico also increased, from a single "freeware" product in the December 1997 survey to six products in the updated survey, due to the discovery of five new commercial cryptographic products from Seguridata Privada S.A. de C.V., which is described in greater detail in Section 4.

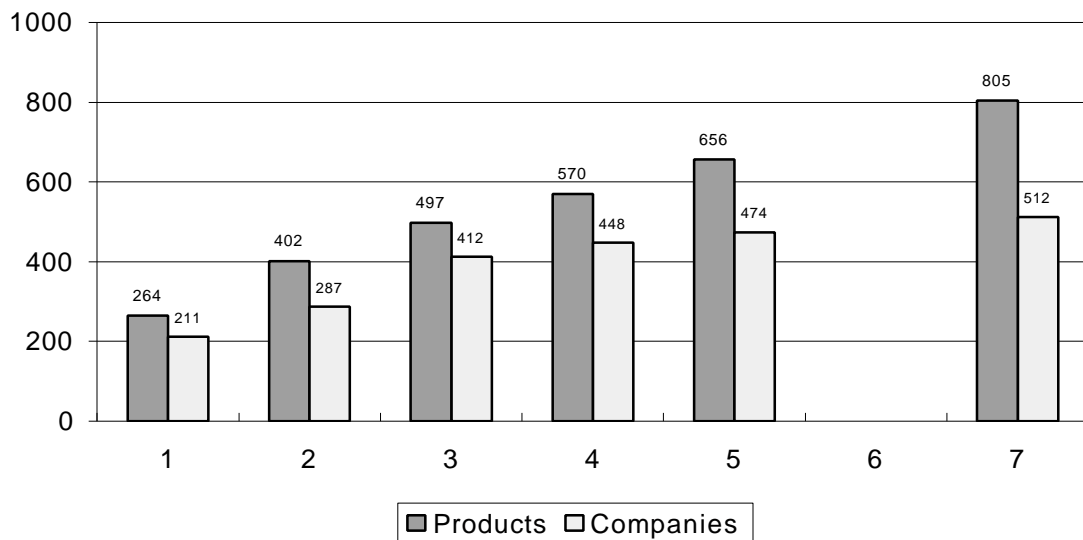


Figure 2. Growing numbers of foreign cryptographic products and companies

3.3.3 *Growing Numbers of Foreign Products & Companies*

The TIS Survey was initiated in April 1993 and conducted on an ongoing basis through December 1997. Figure 2 depicts the evolution of the survey in terms of the increasing numbers of foreign cryptographic products and companies (manufacturers and distributors) identified each

year of the survey effort and after the recent update. Overall, there clearly continues to be increasing and expanding development of foreign cryptographic products.

3.3.4 Quality of Foreign Cryptographic Products

NAI Labs has obtained a number of foreign cryptographic products over the life of the survey effort. The products were all purchased via routine channels, either directly from the foreign manufacturer, a foreign distributor, or an U.S. distributor. We have also downloaded a large number of foreign cryptographic products over the Internet via the World Wide Web.

The quality of cryptographic products varies greatly both within and outside the U.S. We have encountered poor quality products both within and outside the U.S., and we have encountered good quality products both within and outside the U.S. On average, the quality of foreign and U.S. products is comparable. There are a number of very good foreign encryption products that are quite competitive in strength, standards compliance, and functionality. We highlight some of these in the next section.

4. SOME COMPETITORS TO U. S. PRODUCTS EMPLOYING CRYPTOGRAPHY

After updating the cryptography product database, based on prior surveys and new information, we searched out information on the foreign manufacturers that were representative competitors to U. S. manufacturers of software and hardware with encryption capabilities. We did this by examining traditional sources such as business magazines, major newspapers, and trade publications; interviewing industry leaders and security professionals; and using various Web-based search methods [Lexis-Nexis, ABI/Inform, FirstSearch, Gale] to find appropriate combinations of keywords (encryption, U.S., US, United States, foreign, overseas, regulation, export, export controls).

We identified a substantial number of foreign companies that are developing a number of products with strong encryption and have as customers a number of large foreign or multinational corporations. We sketch nine of these in this section to provide a representative sampling. All but one already provide strong encryption (as defined in Section 3.3.1).

Some of the material below has references to cryptographic algorithms, protocols, and other computer science terms that may not be familiar to some readers. More information on these can generally be found in [Stallings 1999] and [Rivest 1978].

Baltimore Technologies Plc., IRELAND/UNITED KINGDOM/AUSTRALIA

Baltimore Technologies plc. was formed by the merger in January 1999 of Zergo Holdings plc. (UK) and Baltimore Technologies Ltd. (Ireland). Its regional headquarters are located in Dublin (Ireland), Plano (Texas) and Sydney (Australia). Corporate headquarters are located in London, UK [Baltimore 1999a].

Baltimore develops and markets security products and services for a wide range of e-commerce and enterprise applications. Its products include Public Key infrastructure (PKI) systems, cryptographic toolkits, security applications and hardware cryptographic devices.

Baltimore's security toolkits include PKI-Plus, ECS Desktop, C/SSL, J/SSL, SMT, CST, and J/CRYPTO. The PKI-Plus toolkit provides clients with the functionality to support a Public Key Infrastructure and provides encryption capabilities with full strength DES, Triple DES and IDEA. ECS Desktop is a high level GSS toolkit that supports 64-bit DES and 128-bit Triple DES. C/SSL and J/SSL are cryptographic toolkits for developing SSL 3.0 applications written in C and Java respectively. C/SSL supports 56-bit DES and 128-bit Triple DES, IDEA and RC4. J/SSL supports 56-bit DES, and 128-bit Triple DES and RC4. SMT (Secure Messaging Toolkit) provides developers the ability to add security to messaging (email) applications. The encryption algorithms supported are 56-bit DES, 128-bit Triple DES, and 40-bit, 64 bit, and 128-bit RC2. CST (Crypto Systems Toolkit) is a set of cryptographic components enabling developers to build strong information security systems. It contains implementations of a variety of encryption algorithms including DES, Triple DES with up to 192 bits key length, IDEA, BSA4, BSA5, RC2, RC4, up to 2048-bit RSA, and DSA. J/CRYPTO is a cryptographic class library for Java applications that supports 56-bit DES, 112-bit Triple DES, and RC4 encryption, and 512-, 1024- and 2048-bit RSA key exchange and digital signature.

Security application solutions include FormSecure, MailSecure, MailSecure Enterprise, and WebSecure. Of its security applications, FormSecure which provides PKI security for Web browser forms uses DES and triple-DES encryption with 128-bit keys. MailSecure provides

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

secure email for MS Outlook, Exchange and Eudora using 128-bit DES, Triple DES and RC2. MailSecure Enterprise, a centralized secure email product, provides encryption with 128-bit Triple DES. WebSecure enhances web server to browser communication in cases where export versions of specific browsers are limited to 40 bits of encryption by diverting all web traffic to its Java programs that use 128-bit RC4 encryption.

Baltimore's hardware cryptographic device, HS4000-Assure provides a security kernel for high speed servers and workstations and features 56-bit DES and 112-bit Triple DES data encryption, and up to 4096-bit RSA key exchange and digital signatures.

“Baltimore has customers in over forty countries including some of the world's leading financial, e-commerce, telecommunications companies and government agencies. Customers include: ABN-AMRO Bank, Australian Tax Office, Bank of England, Bank of Ireland, Belgacom, Digital Equipment, European Commission, Home Office (UK), IBM, Lehman Brothers, Ministry of Defence (UK), NatWest, NIST (USA), PTT Post (Netherlands), S.W.I.F.T., Tradelink (Hong Kong), TradeVan (Malaysia) and VISA International” [Baltimore 1999a].

“Baltimore has also formed alliances with other major global providers of information security technology and services, including ActivCard, Axent Technologies, CDC, Certicom, Chrysalis, CISCO, Dascom, DataKey, GemPlus, Gradient, Hewlett-Packard, ICL, Isocor, Kyberpass, Logica, Netscape, Oracle, Racal and Valicert” [Baltimore 1999a].

Brokat Infosystems AG, GERMANY

BROKAT was founded in 1994. Its headquarters is in Stuttgart, Germany. Subsidiaries are located in Great Britain, Ireland, Luxembourg, Austria, Switzerland, Singapore, Australia, South Africa and the United States. Brokat develops secure solutions for Internet-banking, Internet-brokerage and Internet-payment by allowing companies through the use of its products to develop secure electronic banking and electronic commerce solutions [Brokat 1999a]. Its main product, Brokat Twister, is a software package enabling secure electronic business solutions and provides Java-based 128-bit encryption. Brokat's X-PRESSO Security Gateway provides Twister with a secure Internet channel, using strong SSL encryption. It supports 128-bit IDEA and Triple DES for data encryption, and RSA up to 2048 bits for key exchange and digital signatures.

In its press release of May 19, 1999 Brokat claims a sales increase of 125% in the third quarter of 1998/1999 compared to the same quarter in the previous year [Brokat 1999b].

More than 100 financial service companies use Twister. Brokat customers include Deutsche Bank, Bank 24, Allianz, Fortis Bank Luxembourg the Zurich Kantonalbank, Hypo Bank of Munich, and The Swiss National Telephone Company [Andrews 1997].

Brokat's "Product Partners" include AOL Bertelsmann Online, Corporate Interactive, Inc., Intershop Communications, Micrologica, Netscape Communications, Giesecke & Devrient, and Concord-Eracom.

Check Point Software Technologies Ltd., ISRAEL

“Check Point provides secure enterprise networking solutions through an integrated architecture that includes network security, traffic control and IP address management. Check Point solutions are aimed at enabling customers to implement centralized policy-based management with enterprise-wide distributed deployment” [Check Point 1999a].

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

“The company's integrated architecture includes network security (FireWall-1, VPN-1, Open Security Manager and Provider-1), traffic control (FloodGate-1 and ConnectControl) and IP address management (Meta IP)” [Check Point 1999b].

“Check Point products protect and manage the corporate assets of the majority of Fortune 100 companies and other leading companies and government agencies across the globe. As of April 1999, the company had more than 30,000 registered customers with over 77,000 installations worldwide and 17,000+ networks worldwide using its VPN solution. The Meta IP and Meta DNS products had some 15,000 installations worldwide” [Check Point 1999b].

The company's international headquarters are located in Ramat-Gan, Israel. International subsidiaries are located in the United Kingdom, France, Germany, Japan, Singapore, Australia, the Middle East and Canada. U.S. subsidiaries are located in northern and southern California, Colorado, Georgia, Illinois, Massachusetts, Michigan, New York, North Carolina, Philadelphia, Texas, Virginia and Washington.

In an April 19, 1999 press release, Check Point announced that “revenues for the first quarter ending March 31 were \$43,772,000 compared to \$31,956,000 for the same period in 1998, an increase of 37%. Net income for the quarter was \$19,703,000, or \$0.49 per share compared to net income of \$15,149,000, or \$0.39 per share in the same quarter in 1998, an increase of 30% in net income and 26% in net income per share. Check Point experienced growth across all geographic regions, particularly in Japan. Revenues from the U.S. accounted for 45% of revenues, Europe 34% and Rest of World 21%. In addition, revenues from Technical Services reached 17% in the first quarter. OEM revenues, including those from Nokia and Sun Microsystems, represented 11% of revenues” [Check Point 1999c].

Based on figures from 1997, Check Point is the leading vendor of firewalls with a 23% share in the firewall market – a revenue of \$83 million in firewall sales [Inter@ctive Week 1998].

Checkpoint's firewall solution, Firewall-1 provides a comprehensive set of security solutions which includes VPN through the support of encryption algorithms such as 40- and 56-bit DES, 168-bit Triple DES, 40-bit RC4, 40- and 128-bit CAST, and 48-bit FWZ-1 (FWZ-1 is Check Point's 48-bit exportable proprietary symmetric encryption algorithm).

Check Point's VPN solution products include VPN-1 Gateway, VPN-1 SecuRemote, VPN-1 Accelerator Card, and VPN-1 Appliance. VPN-1 Gateway products are software solutions that provide encryption supporting the following algorithms: 40- and 56-bit DES, 168-bit Triple DES, 40-bit RC4, 40- and 128-bit CAST, and 48-bit FWZ-1. VPN-1 SecurRemote provides VPN support for remote and mobile users. It supports 40- and 56-bit DES, 168-bit Triple DES, 40-bit CAST, and 48-bit FWZ-1. VPN-1 Accelerator Card provides hardware-based data encryption using 56-bit DES and 168-bit Triple DES. VPN-1 Appliance uses 40- and 56-bit DES, 40-bit RC4, and 48-bit FWZ-1.

Check Point's Open Platform for Secure Enterprise Connectivity (OPSEC) is an alliance that delivers the industry's first enterprise-wide security framework. OPSEC provides a single framework that integrates and manages all aspects of secure enterprise networking through an open, extensible management framework. Via the OPSEC Alliance, Check Point Software's products seamlessly integrate with "best-of-breed" products from more than 200 leading industry partners. A complete listing of OPSEC partners can be found at <http://www.opsec.com/>.

Data Fellows Ltd., FINLAND

“Data Fellows develops, markets and supports data security products for corporate computer networks. Its products include anti-virus software, and data security and cryptography software. Its main offices are in San Jose, California and Espoo, Finland, and it has branch offices as well as corporate partners, VARs and other distributors in over 80 countries around the world. Its products have been translated into over 20 languages” [Data Fellows 1999a].

Data Fellows' F-Secure cryptography products are a family of cryptography software to protect the integrity and confidentiality of sensitive information. Its family of products include F-Secure VPN+, F-Secure VPN, F-Secure SSH, F-Secure FileCrypto, and F-Secure Desktop. F-Secure VPN+ provides IPSec protocol based security for secure networking between remote offices, business partners and travelling salesmen using 56-bit DES, 168-bit Triple DES, 128-bit Blowfish, and 128-bit CAST. F-Secure VPN (Virtual Private Network) is an SSH security protocol based solution for pure LAN-to-LAN encryption using a variety of user selectable algorithms including Triple DES, Blowfish, RSA, and IDEA (optional). The symmetric algorithms all use at least 128 bits. F-Secure SSH Server provides users with secure login connections, file transfer, X11, and TCP/IP connections over untrusted networks using 128-bit Triple DES and 128-bit IDEA. F-Secure SSH Terminal&Tunnel provides the user with secure login connections over untrusted networks and to create local proxy servers for remote TCP/IP services. F-Secure SSH Tunnel&Terminal products support the following cryptographic algorithms: 56-bit DES, 168-bit Triple DES, 128-bit IDEA, 128-bit Blowfish, 256-bit Twofish, and 128-bit ARC4 (an RC4 compatible stream cipher). F-Secure FileCrypto is a product that encrypts and decrypts files using 256-bit Blowfish and 168-bit Triple DES. F-Secure Desktop provides encryption and decryption of files, directories, and Windows 95/NT 4.0 folders using 256-bit Blowfish and 168-bit DES.

“The Company's net sales have doubled annually since it was founded in 1988. Turnover has reached \$3.3 million, \$7.6 million and \$14.1million in the fiscal years 1995, 1996 and 1997, respectively” [Data Fellows 1999a].

“Data Fellows has customers in more than 100 countries. These include many of the world's largest industrial corporations and best-known telecommunications companies; major international airlines; several European governments, post offices and defense forces; and several of the world's largest banks. Customers include NASA, the US Air Force, the US Department of Defense Medical branch, the US Naval Warfare Center, the San Diego Supercomputer Center, Lawrence-Livermore National Laboratory, IBM, Unisys, Siemens-Nixdorf, EDS, Cisco, Nokia, Sonera (formerly Telecom Finland), UUNet Technologies, Boeing, Bell Atlantic, and MCI” [Data Fellows 1999a].

Entrust Technologies, CANADA

Entrust is a Canadian company that spun off from Northern Telecom (Nortel). It develops cryptographic products in Canada and exports them from there. It now has offices across the United States, Canada, the United Kingdom, Switzerland, Germany, and Japan.

Entrust develops products for trusted electronic transactions. Its products include solutions for secure Internet transactions including digital certificate services and public-key infrastructures (PKI) products.

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

Entrust File Toolkit delivers a set of application programming interfaces (APIs) to add encryption and digital signatures to store-and-forward (email, e-forms) applications. It supports DES, Triple DES, RSA and RC2. Entrust Session Toolkit is designed for third-party applications that need to protect data communications in real-time. It supports DES, Triple DES, and RC2. Entrust/Solo is a product that provides data encryption, digital signature and data compression functionality for the desktop and e-mail using DES, Triple DES and CAST.

The company's more than 800 corporate customers include J.P. Morgan, the Salomon Smith Barney unit of Citigroup, ScotiaBank, S.W.I.F.T, FedEx, the Canadian Government and several U.S. government agencies.

Entrust's industry partners include development partners such as Hewlett-Packard, Network Associates, Oracle, Nortel Networks and others, 25 channel partners including Hewlett-Packard and Compaq OEM Partners: IBM, Tandem, Check Point and others, specifiers and referral partners such as PriceWaterhouse Coopers, Deloitte & Touche; KPMG Peat Marwick, Ernst & Young, and others, and service provider partners such as BCE Emergis, EDS, Scotiabank and others [Entrust 1999].

Radguard, ISRAEL

RADGUARD was founded in 1994 as a member of the RAD Group of data communications companies. Privately held, the company is backed by American and foreign corporate investors. The company's international headquarters are located in Tel Aviv, Israel; its US headquarters are in Mahwah, NJ.

Radguard is a pioneer and leader in the secure Virtual Private Network (VPN) market. Incorporating security technologies and industry standards into high-performance hardware architectures, Radguard provides solutions to Internet-based virtual private networking, secure non-Internet transmission, safe Internet connectivity and client encryption. Its VPN and network security products include cPro, CryptoWall, and NetCryptor. cPRO is an internetworking security system for VPNs. The cPRO family uses DES and up to 168-bit Triple DES for encryption. CryptoWall is an encrypting firewall that supports subnet-to-subnet security in TCP/IP environments. It supports DES for data encryption and RSA for key exchange and digital signature. NetCryptor is a hardware-based encryption device that employs DES.

Customers include NTT Data, a subsidiary of Japan's Nippon Telephone and Telegraph (NTT), Germany's major car makers and component suppliers including BMW, Bosch, BEHR, Dröxlmaier, Audi, Freudenberg, DaimlerChrysler, Volkswagen and Hella.

Seguridata Privada S.A. de C.V., MEXICO

SeguriDATA is a Mexican company founded in 1996 with the purpose of participating actively in the construction of security standards in Mexico and Latin America by means of integration in committees, with products in electronic security. It has offices in Peru and Spain as well as Mexico. The company provides confidentiality and authenticity of electronic documents with applications to electronic commerce, financial transactions and confidential systems of communications.

Its products include SeguriDOC, SeguriEDIFACT, SeguriLIB, SeguriPROXY, and SeguriTELNET. SeguriDOC offers Triple DES for confidentiality of archived data.

SeguriEDIFACT provides security for EDI communications using Triple DES. SeguriPROXY provides security between web server and web browser sessions using 128-bit RC4.

Sophos Plc., UK

Sophos Plc was founded in 1980 and moved into data security in 1985, producing software and hardware for data encryption, authentication and secure erasure. Its virus detection product has positioned the company as a leading supplier of enterprise-wide virus protection tools. Subsidiaries include Sophos Pty Ltd, Australia, established in April 1999, Sophos Plc, France, established in May 1998, Sophos GmbH, Germany established in October 1997, and Sophos Inc, USA, a wholly owned subsidiary of Sophos Plc based in Massachusetts, USA [Sophos 1999]. Sophos data security products include D-Fence 4 HMG, D-Fence 4 SPA, E-DES, and PUBLIC. D-FENCE HMG is a disk authorization and encryption system for HMG, providing encryption and authentication of floppy and hard disks using SEVERN BRIDGE, a U.K. Government standard algorithm. D-FENCE SPA is a data encryption system for PCs and laptops using SPA (Sophos Proprietary Algorithm) for encryption of floppy and hard disks. SPA is a 64-bit block cipher with 64-bit keys. E-DES and PUBLIC are products used for secure file storage and transmission. E-DES encrypts files using DES or SPA, while PUBLIC encrypts files using 512-bit RSA or MDH in combination with DES or SPA.

Customers include government, financial institutions and multi-national corporations.

Utimaco Safeware AG, GERMANY

Utimaco Safeware AG has subsidiaries in Belgium, France, Finland, Great Britain, Austria, the Netherlands, Norway, Sweden and Switzerland and additional distribution partners (Value-Added-Resellers) in almost all European countries, in the USA, Australia, Asia and in South Africa. Utimaco also has strategic alliances with IBM Deutschland Informationssysteme GmbH, SIEMENS AG and Toshiba Europe.

Utimaco develops IT security solutions for the areas of mobile/desktop security (authentication, access control, encryption), network security (authentication, encryption), e-commerce security (digital signature, encryption) and security infrastructure (smart card reader).

“Utimaco has three development centres. The SafeGuard product line focussing on the "Mobile/Desktop Security" area is developed in Munich, Germany. The development of the SafeGuard product family for "Network Security" and the smart card technology and card reader family CardMan is done in Linz, Austria. The third development centre near Brussels (Holsbeck), Belgium, is responsible for the SafeGuard "E-Commerce Security" product line (digital signatures, e-mail security) and the CryptWare technology (high-performance implementations of standardized basis-crypto algorithms and interfaces)” [Utimaco 1999a].

Products for mobile/desktop security include SafeGuard Easy, and SafeGuard Desktop. SafeGuard Easy is a security program for the online-encryption of hard disks and diskettes. It operates with the encryption algorithms Blowfish, STEALTH, 56-bit DES and 128-bit IDEA to guarantee the confidential storage of sensitive data. SafeGuard Desktop is a security solution for OS/2 operating systems offering boot and virus protection as well as user logon, and allows online encryption of hard disks and floppies with DES, IDEA, STEALTH, Blowfish, and XOR.

Utimaco network security products include SafeGuard LAN Crypt and SafeGuard VPN. SafeGuard LAN Crypt provides protection of selected files against access by persons who are

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

physically capable of accessing the data carrier. The solution guarantees the security of encrypted data through a key length of 128 bits and globally accepted, strong algorithms such as IDEA. SafeGuard VPN provides Virtual Private Networks with secure data transmission using 168-bit Triple DES and 128-bit IDEA.

Utimaco's E-commerce security products include CryptWare Board, CryptWare Server, Cryptware Toolkit, and SafeWare Sign&Crypt. Cryptware Board comes with a DES chip, but allows any other encryption algorithm to be easily installed. The CryptWare Server is a cryptographic black box designed for applications with high security requirements and/or high-speed cryptographic capabilities. It employs DES and 1024-bit RSA. The CryptWare Toolkit is a library that provides all necessary cryptographic and administrative functions to build secure electronic messaging systems. It supports RSA, Triple DES, IDEA, RIPEMD160, MD5, and SHA-1. SafeWare Sign&Crypt offers signing and verification of electronic documents. It can provide encryption with 128-bit IDEA.

The breakdown of Utimaco Group sales by industry in the last business year, 1997/98, is as follows: 29.7% for public institutions, 29.3% for banks, 26.8% for industry and commerce and 14.1% for insurance companies. In the last business year 57 percent of sales were made outside Germany. Its customers include Bertelsmann (Gütersloh) Colonia Nordstern Versicherungsmanagement AG (Cologne), Daimler-Benz Aerospace AG (Kiel), Dresdner Bank, Eduscho GmbH (Bremen), Frankfurter Sparkasse (Frankfurt), Goldwell GmbH (Darmstadt), Innenministerium Mecklenburg-Vorpommern (Schwerin), Landesamt für Datenverarbeitung, (Potsdam), Motorola GmbH (Taunusstein), Otto Versand International GmbH (Hamburg), Oberverwaltungsgericht Thüringen (Weimar), Price Waterhouse (Frankfurt), Police Forces (Belgium), Isaserver (Belgium), State Police (Belgium), Unisys for Christelijke Mutualiteiten (Belgium), The European Commission (Belgium and Luxembourg), Danfoss A/S (Denmark), ICL Pathway Ltd. (Great Britain), Robert Fleming & Co. Ltd. (Great Britain), Standard Chartered Bank (Great Britain), Conseil de l'Union Européenne (Luxembourg), KPN Telecom (The Netherlands), ABN AMRO Bank N.V. (The Netherlands), Nycomed Amersham Group (Norway), Schweizer Post (Switzerland), DDJ, and Justizdirektion des Kantons Zürich (Switzerland).

5. FOREIGN MARKETING USE OF U. S. EXPORT CONTROLS

5.1 Introduction

As Under Secretary of Commerce William A. Reinsch noted in recent Congressional testimony, "encryption remains a hotly debated issue. The Administration continues to support a balanced approach that considers privacy and commerce as well as protecting important law enforcement and national security equities. We have been consulting closely with industry and its customers to develop a policy that provides that balance in a way that also reflects the evolving realities of the market place" [Reinsch 1999]. As the Commerce Department struggles to craft and finely tune export regulations to satisfy these objectives, many foreign cryptography manufacturers are citing these regulations as reasons for their prospects to not "buy American". Even foreign governments sometimes overtly use these regulations. For example, "In a letter sent [in January 1999] to India's Central Vigilance Commission (CVC)--an intelligence agency comparable to the United States' National Security Agency--the Indian Defense Research and Development Organization said the limits the U.S. government places on exported encryption products render the products too weak for reliable use. The CVC responded that it might mandate that all Indian financial institutions buy security software from India" [Dunlap 1999].

5.2 Advertising Related to Cryptographic Controls

Trade magazines, industry reports, and news articles were searched for consumer preference data, including checklists, ease of use" and "best buy" ratings, etc., to try to find anecdotal justification or rebuttal of the claim that consumers strongly prefer U.S.-made encryption products and systems incorporating U.S.-made encryption, as asserted, for example, in [Ernst 1999].

We did find a reference to a U. S. government study that acknowledged that "in many countries surveyed, exportable U. S. encryption products are perceived to be of unsatisfactory quality" [Commerce/NSA 1996] {date given as June 1995, page ES-3, possibly a draft, in [Olbeter 1998]}. We also found some information from companies that claimed or implied that their products are more secure and/or easier to use than American products burdened by U.S. export controls. Descriptions of the various export control regimes are found in [Baker 1998, Koops 1999, and GILC 1998].

Examples of the statements of foreign companies are given below.

Brokat Infosystems AG (Germany)

Brokat, on its web page [Brokat 1999c] discusses "Secure Communication using 128-bit encryption" and states that "In comparison to other solutions, X-AGENT allows very secure communication. Highly sensitive information can be exchanged using this consultation tool. All data is encrypted with the 128-bit Twister security component. Even so-called 'weak' Internet browsers, which only use a 40-bit encryption due to US government export restrictions can be 'topped up' accordingly for the duration of the session."

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

Baltimore Technologies plc. (Ireland/United Kingdom/Australia)

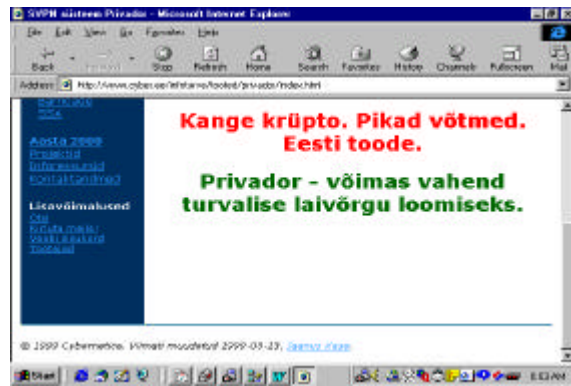
Baltimore Technologies states that WebSecure, a product designed to provide secure web server to browser communication is useful because "US export restrictions dictate that most web servers and browsers cannot perform 128-bit encryption for security. Instead, export versions of browsers like Internet Explorer and Netscape Navigator and export versions of web servers like Netscape Enterprise Server and Microsoft Internet Information Server are limited to 40 bits of encryption, which is not secure enough for most applications" [Baltimore 1999b].

Cybernetica (Estonia)

Cybernetica advertises "... full strength cryptographic security with long keys and no backdoors" and its Web pages for their products prominently feature this selling point.



[Cybernetica 1999a]



[Cybernetica 1999b]

In their Frequently Asked Questions list on the Web, they go on to celebrate the differences between their product and U. S. products:

Strong crypto? What algorithms are supported? And what key lengths?

IDEA. Triple DES. Blowfish. RSA. Diffie-Hellman. The end user has the opportunity of selecting the algorithms he trusts. And, if the user so requires, support for further algorithms may be added. You can use as long keys as the algorithms you have selected allow you to. There are no "political" restrictions on key lengths to be used in the Privador system.

What about back doors, key recovery etc?

There are no back doors built into the Privador system. We can - and will - prove it if so required.

How come you don't care about export restrictions?

Because there are none. The Privador System is entirely developed by Cybernetica, the first private-law R&D institution in Estonia. The laws of the Republic of Estonia

allow us to export strong cryptographic technologies to almost any country in the world.

Utimaco Safeware AG (Germany)

On its web site, Utimaco states that [Utimaco 1999b] "... As a German manufacturer, Utimaco guarantees that no national key depositing requirements (ESCROW) exist which could jeopardize the security of the solution..."

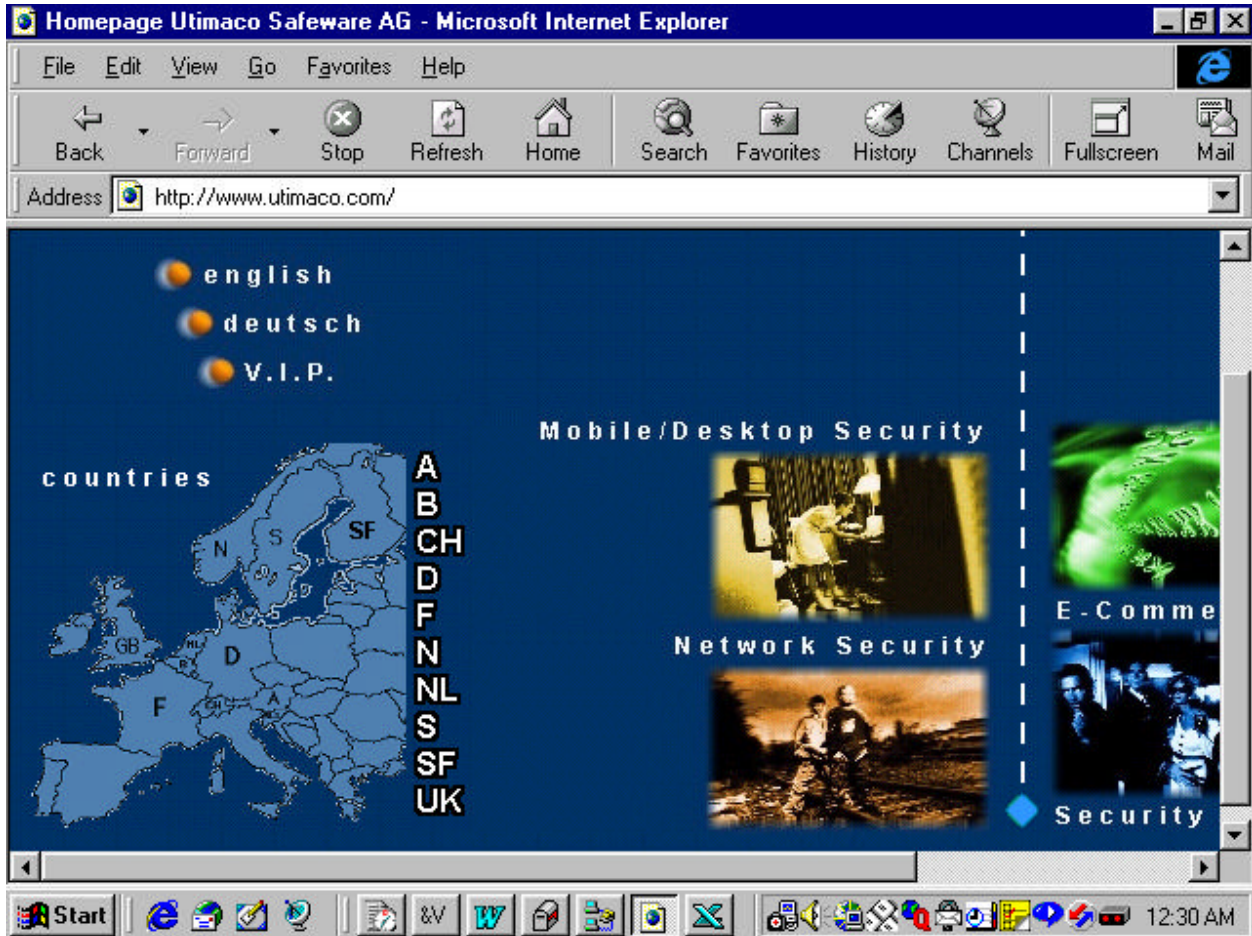


Figure 3. Homepage of Utimaco Safeware AG

Note Utimaco's home page, illustrated in Figure 3. It is user-friendly for speakers of a number of languages. It makes the point that Utimaco has representatives in a number of European countries. If the user clicks on his or her country (either on the map or on the country abbreviation in the vertical list), he or she is transported to a page in their native language that further presents Utimaco and its products and services. As an example, Figure 4 shows the homepage of Utimaco Norway that the user is transported to when Norway is selected from the map.

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

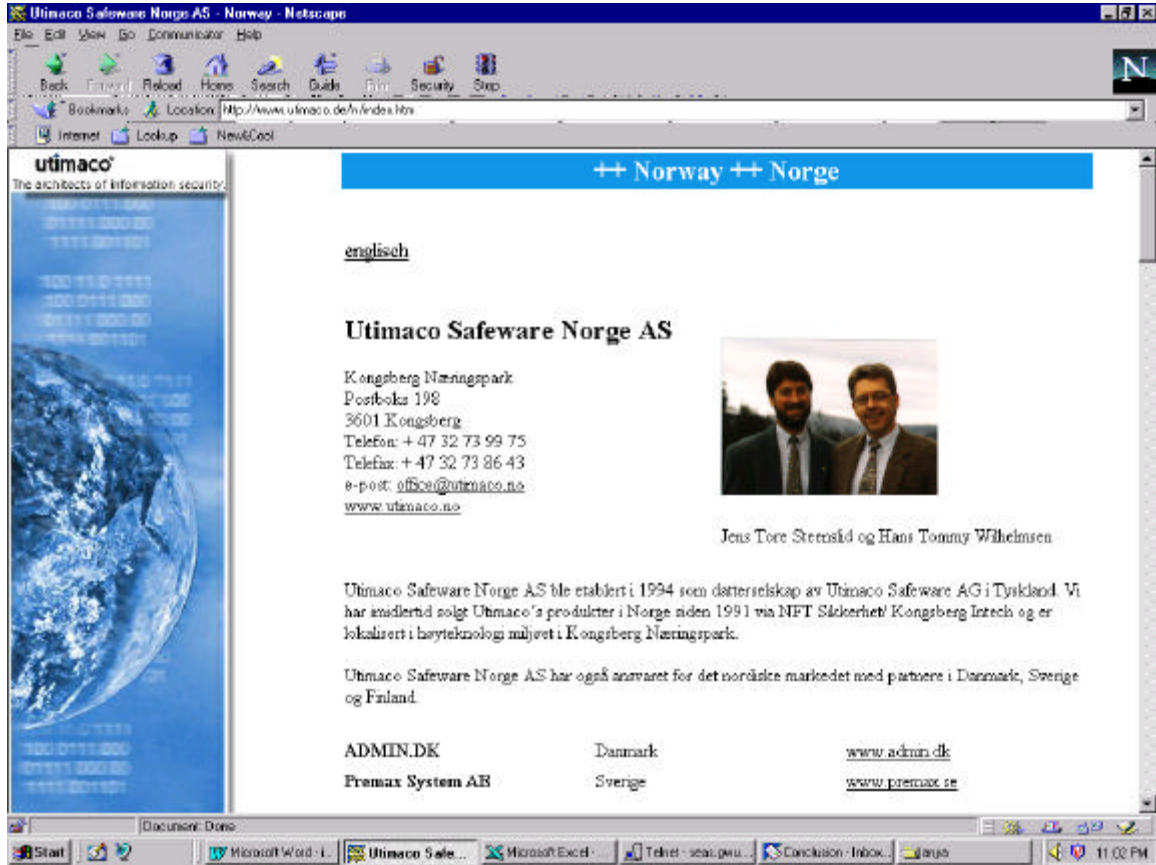


Figure 4. Homepage of Utimaco Safeware Norge AS

Data Fellows Corporation (Finland)

Data Fellows makes the readers of its web page aware of U. S. export restrictions and states that its products are designed with "much more security" than U. S. products:

"... The encryption technology used in the F-Secure products has been developed in Europe and thus does not fall under the US ITAR export regulations. F-Secure products can be used in every country where encryption is legal, including the United States of America..." [Data Fellows 1999b]

"... F-Secure FileCrypto uses well-known fast block cipher algorithms. You can choose either three-key 3DES or Blowfish. Both algorithms have been analyzed by the world's leading cryptographers. They are known to be strong and safe. These algorithms provide security with a minimum of 168-bit keys. They provide much more security than

DES-based or U.S. products that fall under U.S. ITAR export restrictions." [Data Fellows 1999c].

JCP Computer Services (United Kingdom)

JCP takes on U. S. products directly based on export controls [JCP 1999]:

"Many companies are using or considering using implementations of these algorithms which originate in the US. The US government prohibits export of strong cryptographic tools, and, except under specific conditions, only permits the export of weak implementations. These 'crippled' cryptographic tools do not provide sufficient protection to allow Internet e-commerce and communications to proceed securely. In an amateur attack on a US export-strength cryptographic routine, the key was broken in 56 hours. And such times will decrease markedly as computer processing power continues to improve.

"JCP has developed full strength implementations outside of the US using industry proven standard algorithms. JCP are the leading company outside the US producing high performance cryptographic tools in Java, which has become the Internet's standard programming language. The product provides a set of packages that implement specific cryptography algorithms for use within any Internet application."

SSH Communications Security (Finland)

SSH states on their web site [SSH 1999] that "The software from SSH is free from strict US export restrictions" as one of "six good reasons why SSH IPSEC Express is the best choice (sic)"; it goes on "IPSEC is supposed to be an international standard. However, because of export restrictions in different countries. (sic) SSH is one of the few to deliver full standards compliance and strong security virtually anywhere in the world."

RPK Security, Inc. (New Zealand, Switzerland, United Kingdom)

RPK advertises on its web site of its flagship RPK Encryptonite Engine [RPK 1999], "Developed outside the U.S., the RPK Encryptonite Engine is not subject to US government regulations. It is available with strong encryption worldwide, with dramatically better performance at significantly lower implementation cost compared with competing technologies." Reading further on its web site, one finds that "RPK's cryptographic research and product development is based in New Zealand, Switzerland and the U.K, with worldwide sales and marketing operations in San Francisco, CA."

6. STANDARDS AND THEIR INFLUENCE

6.1 Pervasiveness of Standards

From the material above, one can see that companies vie to have encryption products that meet certain accepted worldwide standards. If the products do not, they often will not interoperate successfully with other computer systems. This section highlights two important international standards efforts. Note the contribution of encryption expertise from all over the world to both.

6.1.1 *IPsec*

Today's widespread and pervasive use of the Internet has accentuated the need for security for the underlying Internet Protocol (IP). The IETF has developed the IP Security (IPsec) protocol as an integral element of Internet security. IPsec is a proposed standard Internet protocol designed to provide cryptographic-based security, including authentication, integrity, and (optional) confidentiality services. While the use of IPsec is currently optional, its use will be mandatory for the next version of the Internet Protocol, IPv6 [IPSEC].

As a result of the dramatic impact IPsec will have on improving the security of the Internet, there has been enormous interest in developing implementations of IPsec. This interest has extended throughout the entire world, due to the global nature of the Internet and need for cryptographic-based security. Many freely available and commercial implementations of IPsec are available or are under development. Ted Ts'o of MIT, co-chair of the IETF IPsec Working Group, maintains a list of companies implementing (or planning to implement) IPsec. The list currently cites implementations from 49 companies around the world. At least nine of the companies are from outside the U.S. There is also one effort, the KAME Project, being conducted by a combination of several Japanese companies (Fujitsu, Hitachi, IJ Research Laboratory, NEC, Toshiba, and Yokogawa) [KAME 1999].

Another important aspect of IPsec is that it supports encrypted "tunnels", whereby an IP packet is completely encrypted as it travels from one point of a network to another. Encrypted tunnels are one of the primary means for establishing Virtual Private Networks, or VPNs, which emulate private networks over public, shared IP networks, such as the Internet.

IPsec is designed to be independent of any specific cryptographic algorithms; it can support several, but it will require one strong algorithm, Triple DES; the relatively weak DES will be permitted but not required. Specifications have also been developed for the use of the IDEA, BLOWFISH, RC5, and CAST strong cryptographic algorithms with long key lengths for IPsec [Stallings 1999].

6.1.2 *Advanced Encryption Standard (AES)*

In 1997, NIST solicited algorithms for the Advanced Encryption Standard (AES), to replace the Data Encryption Standard (DES) [FIPS PUB 46-2] as a government encryption

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

standard. Individuals and companies from eleven different foreign countries proposed 10 out of the 15 candidate algorithms submitted to NIST [Smid 1998]:

Country	Candidate Algorithm	Submittor(s)
Australia	LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
Belgium	RIJNDAEL	Joan Daemen, Vincent Rijmen
Canada	CAST-256	Entrust Technologies, Inc.
	DEAL	Outerbridge, Knudsen
Costa Rica	FROG	TecApro Internacional S.A.
France	DFC	Centre National pour la Recherche Scientifique (CNRS)
German	MAGENTA	Deutsche Telekom AG
Japan	E2	Nippon Telegraph and Telephone Corporation (NTT)
Korea	CRYPTON	Future Systems, Inc.
USA	HPC	Rich Schroepel
	MARS	IBM
	RC6	RSA Laboratories
	SAFER+	Cylink Corporation
	TWOFISH	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson
UK/Israel/Norway	SERPENT	Ross Anderson, Eli Biham, Lars Knudsen

"Of the five submissions likely to be chosen for the next round, about half will be from outside the U.S. It is very possible that the next U.S. government encryption standard will have been designed outside the U.S." [Schneier 1999].

7. CONCLUSIONS

Based on the research described above, we arrive at two conclusions:

1. *Foreign development of cryptographic products is not only continuing but is expanding to additional countries.*
2. *Communications-related cryptography is experiencing high growth, especially in electronic mail, VPN, and IPsec products.*

7.1 Foreign Development of Cryptography Continues to Grow

There are now 805 cryptography products produced in 35 countries outside the United States. In at least 67 countries, 512 foreign manufacturers and distributors are involved. In just three weeks, with limited resources, we identified 149 foreign cryptographic products new to market since the December 1997 TIS survey.

It is difficult to gauge how many additional products would be identified, given sufficient time and resources, but it is safe to anticipate that we would identify many more products from the countries within the database, and possibly several additional countries.

Development of cryptographic products in nations around the world is increasing. Moreover, as additional nations seize opportunities in e-commerce, nation-centric islands of competence develop, as do ultimately international markets. Often these islands of competence are developed by bright young entrepreneurs and computer scientists who have trained elsewhere (often the United States) and then play key roles in jump-starting their native countries' e-commerce. This fits nicely in the theory of technoglobalization, as espoused by Robert Reich, discussed more in Section 8.

7.2 Communications-Related Cryptography Leads Storage Cryptography

Within the 149 new products we discovered, communications-related products, as opposed to data storage encryption, were predominant. It appears that the efforts of the Internet Engineering Task Force (IETF) to provide standardized protocols for the Internet has facilitated the development of solutions and products to communications related problems. We conjecture that this and the expansion of e-commerce have resulted in a high growth of communications related cryptographic products such as those for electronic mail, VPNs, and IPsec.

IPsec's support of encrypted tunnels will greatly improve security for private, enterprise-based networks. As the comfort level of users (and organizations) grows, and as the potential and actual gains of (consumer to business and business to business) e-commerce become apparent, there will be increased worldwide need for communications-related cryptography.

8. FUTURE RESEARCH

To date there have been only a few efforts to attempt to quantify the impact of regulatory measures on the international cryptographic market [Olbeter 1998, BSA 1998, CDT 1997]. The TIS survey and this effort to update the foreign products inventory of the database have been one of the few ways to quantitatively assess the state of the market over time. As noted in Section 7, we saw developments both in countries already producing cryptographic products and expansion into new countries that did not have cryptographic product development as of December 1997. We saw a number of firms become multinational.

In the face of continuing U. S. export controls on encryption products, technology, and services, some American companies have financed the creation or growth of foreign cryptographic firms. We have seen some U. S. companies (e.g., PGP, RSA, Sun) buy some foreign expertise, leaving it in place (rather than bringing the talent back to the United States). With this expertise offshore, the relatively stringent U. S. export controls for cryptographic products can be avoided, since products can be shipped from countries with less stringent controls. All of these facts indicate that both nations and companies see opportunities in this rapidly changing technological market, and it could be argued that globalization plays a major role in future growth for this market.

This is not a case of the technology slipping away from the United States. The technological expertise is already available in many places around the world. Indeed, we noted earlier that the majority of submissions for the Advanced Encryption Standard (AES) have been designed outside the United States. This may be simply an example of the general thesis of economists David Mowery and Nathan Rosenberg [Mowery 1989], who argue that, in general, foreign firms' technological sophistication has caught up with that of the United States in many cases. In those cases, they reason

"Since foreign firms now are more technologically sophisticated and technology is more internationally mobile, however, the competitive advantages that accrued in the past from basic research and a strong knowledge base have been eroded. Faster international transfer of new technologies is undercutting a major source of America's postwar superiority in high-technology markets." (p. 218)

Our empirical product data could be combined with economic measures and economic theories to better explain why we are seeing the observed growth in encryption products and companies around the world, and to examine the effects of Internet growth, e-commerce development, and regulatory actions on the international cryptographic market over time.

Porter [1990], for example, tests his theses by using quantitative measures from several nations, by industrial sector. His national economic profiles include primary goods, machinery, and specialty inputs and services data for each industrial sector. Given appropriate quantitative measures, similar work could be done for the international cryptography market.

As the global information-based economy continues to grow, and as the nature of industrial research and development continues to shift from nation-centric to international collaboration, we will continue to witness more rapid technological development and global economic growth. We should be able to put together previous economic work [Duysters 1996] with material already available on the information technology sector [Mowery 1996, Rosenberg

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

1992] and the data in this study to better understand the changes we are seeing in the global marketplace and thus be able to more easily adjust national laws for a global economy.

9. REFERENCES

- [ABI/Inform] ProQuest Direct, <http://proquest.umi.com/pqdweb>.
- [Acey 1999] Acey, Madeleine, TechWeb, CMPNet, in New York Times Technology, http://www.nytimes.com/techweb/TW_Key_Escrow_Bill_Slammed_By_Parliament_Inquiry.html, 5/19/99.
- [Adams 1997] C. Adams, The CAST-128 Encryption Algorithm, RFC 2144, May 1997.
- [Andrews 1997] Andrews, Edmund L., "U. S. Restrictions of Exports Aid German Software Maker," *New York Times*, April 3, 1997.
- [Argentina 1999] Description of PGP and links to download it, in *Firma Digital y Documento Electrónico*, <http://www.sfp.gov.ar/firma.html>, downloaded May 27, 1999.
- [Baker 1998] Baker, S. and Hurst, P., *The Limits of Trust: Cryptography, Governments, and Electronic Commerce*, Kluwer Law International, 1998.
- [Baltimore 1999a] Baltimore Company Profile, <http://www.baltimore.ie/corporate/profile.html>.
- [Baltimore 1999b] WebSecure, <http://www.baltimore.ie/products/websecure/index.html>.
- [Brokat 1998] Brokat Offering Prospectus, http://www.brokat.com/int/ir/facts/annual_report.html.
- [Brokat 1999a] Brokat Company, <http://www.brokat.com/int/company/index.html>.
- [Brokat 1999b] Brokat Continues Success in Third Quarter, <http://www.brokat.com/int/press/1999/pr19990519-01.html>.
- [Brokat 1999c] Consulting Via Internet With X-Agent From Brokat, <http://www.brokat.com/int/press/1999/pr19990318-02.html>.
- [BSA 1998] Business Software Alliance, The Cost of Government-Driven Key Escrow Encryption, 1998, http://www.bsa.org/ceoforum/pdfs/key_escrow.pdf
- [CDT 1997] Center for Democracy and Technology, The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption, a report by an *ad hoc* Group of Cryptographers and Computer Scientists, Washington, 1997.
- [Check Point 1999a] Check Point Corporate Information and News, <http://www.checkpoint.com/corporate/index.html>.
- [Check Point 1999b] Check Point Corporate Profile, <http://www.checkpoint.com/corporate/corporate.html>.
- [Check Point 1999c] Check Point Software Technologies Ltd Reports Financial Results for

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

- First Quarter 1999, <http://www.checkpoint.com/press/1999/q1earnings041999.html>.
- [Commerce/NSA 1996] *A Study of The International Market for Computer Software with Encryption*, Prepared by the U.S. Department of Commerce and the National Security Agency for the Interagency Working Group on Encryption and Telecommunications Policy, January 11, 1996.
- [CPI 1999] Non-U.S. Cryptographic Product Survey Call-for-Information, <http://www.seas.gwu.edu/seas/institutes/cpi/cryptosurvey/call4info.html>
- [CSI 1997] *Computer Security Products Buyers Guide 1997*, Computer Security Institute, San Francisco, 1997.
- [Cybernetica 1999a] Cybernetica English Web Site, <http://www.cyber.ee/infosecurity/products/privador/intro.html>.
- [Cybernetica 1999b] Cybernetica Estonian Web site, <http://www.cyber.ee/infoturve/tooted/privador/index.html>.
- [CRISIS 1996] *Cryptography's Role in Securing the Information Society*, Kenneth W. Dam and Herbert S. Lin, Editors; Committee to Study National Cryptography Policy, National Research Council, 1996.
- [Data Fellows 1999a] Data Fellows Company Fact Sheet, <http://www.datafellows.fi/df-info/>.
- [Data Fellows 1999b] F-Secure Cryptography Products, <http://www.datafellows.fi/f-secure/>.
- [Data Fellows 1999c] F-Secure FileCrypto - On-the-fly encryption, <http://www.datafellows.fi/f-secure/filecrypto/on-the-fly.htm>.
- [FIPS PUB 46-2] National Institute of Standards and Technology. FIPS PUB 46-2: Data Encryption Standard. December 30, 1993.
- [Dunlap 1999] "All Tied Up: U.S. Trade Rules Hobble VARs, ISVs Alike Dealing With Encryption. " by Charlotte Dunlap & Amy Rogers, Computer Reseller News, February 8, 1999.
- [Duysters 1996] Duysters, Geert. *The Dynamics of Technical Innovation: The Evolution and Development of Information Technology*. Cheltenham, U.K.: Edward Elgar.
- [EDS 1996] EDS, "When governments hamper encryption, they hamper commerce", advertisement, *Washington Post*, June 20, 1996.
- [Entrust 1999] Products: Entrust/SOLO, <http://www.entrust.com/solo/index.htm>.
- [Ernst 1999] Ernst & Young, Retail and Consumer Products: Key Technologies, <http://www.ey.com/industry/consumer/retailit/key.asp>, April 22, 1999.
- [FirstSearch] FirstSearch, http://gilligan.prod.oclc.org:3055/html/fs_areas.htm.
- [Gale] Gale Business Resources (integrated), <http://www.galenet.com/servlet/GBR>.
- [Gibson 1998] Paul Gibson, "The \$237 billion conundrum", *Electronic Business*,

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

- Highlands Ranch, November 1998.
- [GILC 1998] Global Internet Liberty Campaign, "Online International Encryption Policy Survey, <http://www.gilc.org/crypto/crypto-survey.html>.
- [Greenspan 1997] Greenspan, Alan, Remarks at the Conference on Privacy in the Information Age, Salt Lake City, Utah, March 7, 1997, <http://www.federalreserve.gov/boarddocs/speeches/19970307.htm>
- [Grossman 1999] Wendy Grossman, Connected - Analysis: Encryption proves a slithery beast to control, *Daily Telegraph* (London), January 21, 1999.
- [Hornstein 1999] Testimony of Richard Hornstein before the Telecommunications, Trade and Consumer Protection Subcommittee of the Committee on Commerce, U. S. House of Representatives, Washington DC, May 18, 1999.
- [ICSA Survey] ICSA Certified Cryptography Products ("Buyer's Guide"), list is at http://www.icsa.net/services/consortia/cryptography/certified_products.shtml.
- [IKE] Harkins, D., and D. Carrel, D., The Internet Key Exchange (IKE), RFC 2409, November 1998.
- [IPSEC] S. Kent and R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998.
- [IPSECIPM] Ted T'so, IPSEC/ISAKMP Company List, Companies which are Implementing (or Planning to Implement) IPSEC/ISAKMP, <http://web.mit.edu/tytso/www/ipsec/>.
- [IPSECWG] IPsec WG Charter, <http://www.ietf.org/html.charters/ipsec-charter.html>.
- [JCP 1999] JCP Computer Services, http://www.jcp.co.uk/secProduct/security_cdk_index.htm.
- [KAME 1999] KAME Project, <http://www.kame.net/>.
- [Koops 1999a] Koops, B-J, Crypto Law Survey, <http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm>.
- [Koops 1999b] Koops, B-J, *The Crypto Controversy: A Key Conflict in the Information Society*, Kluwer Law International, The Hague, 1999.
- [Lai 1990] Lai, X., and Massey, J., A Proposal for a New Block Encryption Standard, Proceedings EUROCRYPT '90, Springer Verlag, 1990.
- [Lai 1991] Lai, X., and Massey, J., Markov Ciphers and Differential Cryptanalysis, Proceedings of EUROCRYPT '91, Springer-Verlag, 1991.
- [Lexis Nexis] Lexis-Nexis, <http://www.lexis-nexis.com>.
- [Matsui 1996] Mitsuru Matsui, New Block Encryption Algorithm MISTY, Mitsubishi Electric Corp., 1996.
- [MISTY] MISTY - Mitsubishi Electronic's Encryption Algorithm,

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

- http://www.mitsubishi.com/ghp_japan/misty/200misty.htm.
- [Mowery 1989] Mowery, David C. and Nathan Rosenberg. *Technology and the Pursuit of Economic Growth*. Cambridge UK: Cambridge University Press, 1989.
- [Mowery 1996] Mowery, David C. (ed.). *The International Computer Software Industry: A Comparative Study of Industry Evolution and Structure*. New York: Oxford University Press.
- [Olbeter 1998] Olbeter, Erik R. and Christopher Hamilton, *Finding the Key: Reconciling National and Economic Security Interests in Cryptography Policy*, Economic Strategy Institute, Washington, DC, March 1998.
- [PECSENC 1998] Report of the president's Export Council Subcommittee on Encryption Working Group on International Affairs, September 1998, <http://209.122.145.150/PresidentsExportCouncil/PECSENC/iwgfind.htm>.
- [Porter 1990] Porter, Michael E., *The Competitive Advantage of Nations*, New York: The Free Press, 1990.
- [Randata 1999] Media Release, "Boost For Smart Aussie Company: SNS The First To Be Granted U.S. Export Licence For High Security Cryptography," Sept. 7 1998. <http://www.randata.com.au/infb1x.htm>.
- [Reich 1990] Robert B. Reich, "Does Corporate Nationality Matter?", *Issues in Science and Technology*, Winter 1990-91, pp. 40-44.
- [Reinsch 1999] Reinsch, William A., Testimony before the House Committee on Commerce, Subcommittee on Telecommunications, Trade and Consumer Protection, May 25, 1999.
- [Rivest 1978] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, February 1978, Volume 21, Number 2, pp. 120-126.
- [Rivest 1996] [Rivest 1996] R. Rivest and R. Baldwin, The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms, RFC 2040, October 1996.
- [Rosenberg 1992] Rosenberg, Nathan, Ralph Landau, and David C. Mowery (eds). *Technology and the Wealth of Nations*. Stanford, Calif.: Stanford University Press.
- [RPK 1999] RPK Security, <http://www.rpk.com/>.
- [RSA 1999] "RSA Provides Security Solutions to Worldwide Markets Through New Operation in Australia", January 6, 1999 press release, <http://www.aus.rsa.com/pressbox/990106-1.html>.
- [Schneier 1993] Schneier, B., Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish), *Proceedings of Workshop on Fast Software Encryption*, Springer Verlag, 1993.
- [Schneier 1994] Schneier, B., The Blowfish Encryption Algorithm, *Dr. Dobb's Journal*, April 1994.

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

- [Schneier 1995] Schneier, B., *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed., Wiley, 1995.
- [Schneier 1999] Bruce Schneier, The Internationalization of Cryptography, CRYPTOGRAM Newsletter, May 15, 1999, <http://www.counterpane.com/crypto-gram-9905.html>.
- [Smid 1998] Smid, M., and M. Dworkin, Special Report on the First AES Conference, presented at Crypto '98 Conference, August 1998, <http://csrc.nist.gov/encryption/aes/round1/crypto98.pdf>.
- [Sophos 1999] Sophos Company Info, <http://www.sophos.com/companyinfo/profile/>.
- [SSH 1999] 6 Good Reasons Why SSH IPSEC Express is the Best Choice, <http://www.ipsec.com/6reasons.html>.
- [Stallings 1999] William Stallings, *Cryptography and Network Security: Principles and Practice*, Second Edition, Prentice Hall, 1999.
- [Thayer 1997] Rodney Thayer, "Bulletproof IP" in *Data Communications*, November 21, 1997, <http://data.com/tutorials/bullet.html>.
- [TIS 1997] Worldwide Survey of Cryptographic Products, http://www.nai.com/products/security/tis_research/crypto/crypt_surv.asp, December 1997.
- [United Nations 1986] U.N. International Trade Statistics Yearbook, 1986. New York: United Nations.
- [U.S. DoC 1996] U.S. Department of Commerce Press Release, "Department of Commerce Releases Study on the International Market for Encryption Software", January 11, 1996.
- [Utimaco 1999a] Utimaco Safeware AG Facts and Figures, <http://www.utimaco.de/english/index1.htm>.
- [Utimaco 1999b] SafeGuard VPN Product Description, http://www.utimaco.com/english/products/sgvpn_e.htm.
- [Walker 1993] Testimony of Stephen Walker before the U.S. House of Representatives Foreign Affairs Subcommittee on Economic Policy, Trade and Environment, October 12, 1993.
- [Walker 1994] Testimony of Stephen Walker before the U.S. Senate Judiciary Subcommittee on Technology and the Law, Hearing on the Administration's "Clipper Chip" Key Escrow Encryption Program, May 3, 1994.

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

APPENDICES

A. CALL FOR INFORMATION

Please forward this message to others who are interested on the topic. A WWW-version of this message can be found at <http://www.seas.gwu.edu/seas/institutes/cpi/cryptosurvey/call4info.html>

**NON-U.S. CRYPTOGRAPHIC PRODUCT SURVEY
CALL FOR INFORMATION**

The George Washington University and NAI Labs, The Security Research Division of Network Associates (formerly the research division of Trusted Information Systems) are conducting a survey to identify cryptographic products manufactured outside the United States and are examining product specifications to assess their functionality and security.

We are soliciting input from those with knowledge of cryptographic products through the use of this survey form. If you know of cryptographic products that are manufactured in countries other than the United States, please complete this form and submit it to the Cyberspace Policy Institute (CPI) NO LATER THAN TUESDAY MAY 18, 1999. You may submit this form via email to cpi@seas.gwu.edu or fax at (202) 994-5505 in Washington D.C.

In addition, we ask you to send or post this survey to anyone or place that would have knowledge of cryptographic products. Inquiries about this survey may be made to the Cyberspace Policy Institute at cpi@seas.gwu.edu or (202) 994-5512. This survey may also be found on the CPI Web site at

<http://www.seas.gwu.edu/seas/institutes/cpi>.

Your cooperation is greatly appreciated.

Professor Lance J. Hoffman, The George Washington University David Balenson, NAI Labs, The Security Research Division of Network Associates

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

NON-U.S. CRYPTOGRAPHIC PRODUCT SURVEY

DATE:

COMPLETED BY:

Your Name:

Phone:

E-mail:

NAME AND ADDRESS OF MANUFACTURER

Name:

Address:

City:

State:

Zip Code:

Country:

URL:

MANUFACTURER CONTACT INFORMATION

Name:

Title:

Phone:

FAX:

E-mail:

800#:

PRODUCT DESCRIPTION

Name (including model and version information):

Product-specific URL:

Is it software-only, hardware-only, or a software/hardware combination?

What does it encrypt (e.g., disk, file, communications, FAX, voice, magnetic tape, electronic mail)?

If embedded software or hardware, what platforms does it support (e.g., PC, Mac, UNIX workstation, IBM mainframe), else if standalone hardware, what interfaces does it support (RS-232, telephone, V.24, V.35)?

If software, is it in the form of a kit or as an end-user program, else if hardware, what is the embodiment (e.g., chip, board, PCMCIA card, smart card, box, phone)?

What algorithms does it employ for data encryption (including proprietary algorithms and key length)?

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

If applicable, what algorithms does it employ for key management (including proprietary algorithms and key length)?

If applicable, what algorithms does it employ for data authentication (including proprietary algorithms)?

How is the product sold or distributed (e.g., store front, mail order, telephone order, World Wide Web, anonymous ftp over the Internet)?

If applicable, what is the quantity one purchase price?

(Optional) Approximate number of units sold or distributed?

(Optional) Approximate date product was first available?

Please provide a list of the names and relationships of any associated companies (e.g., parent company, sister company, distributors). Include full address and contact name, title, phone, FAX, and e-mail address. Other information:

PLEASE PROVIDE A COPY OF ANY RELEVANT PRODUCT LITERATURE.

Send completed forms and product literature via e-mail to cpi@seas.gwu.edu or via fax to the Cyberspace Policy Institute at 202-994-5505 in Washington D.C.

THANK YOU!

~~~~~  
This survey is part of an ongoing worldwide study of cryptographic products started in April 1994 by Trusted Information Systems and Dr. Lance J. Hoffman of the George Washington University. The December 1997 summary results of the survey are available on the World Wide Web at [http://www.nai.com/products/security/tis\\_research/crypto/crypt\\_surv.asp](http://www.nai.com/products/security/tis_research/crypto/crypt_surv.asp).  
~~~~~

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

B. SUMMARY LISTING OF FOREIGN CRYPTOGRAPHIC PRODUCTS

The following table is a summary listing of the foreign products currently contained in the cryptographic product database. We cannot guarantee the accuracy and completeness of this information. In many cases, products may support additional platforms or interfaces, encrypt additional types of information, include additional embodiments, or support additional encryption algorithms. Additional information will be available on the NAI Labs Crypto Products Survey Web page at http://www.nai.com/products/security/tis_research/crypto/crypt_surv.asp.

COUNTRY	COMPANY	PRODUCT	PLATFORMS/ INTERAFACES	TYPE	ENCRYPTS	EMBODIMENT	ENC ALG
ARGENTINA	DataCrypt	Software implimentation of Cryptography	DOS	SW	GENERAL	PGM	DES
ARGENTINA	Newnet S.A.	DSD 9612 Data Security Device	TTL	HW	GENERAL	CHIP	DES
AUSTRALIA	Andrei Souleimanian	Xboct		SW	FILE	PGM	PROP
AUSTRALIA	Banksia Technology Pty. Ltd.	Citadel	V.34	HW	COMMS	BOX	DES
AUSTRALIA	Banksia Technology Pty. Ltd.	Pro 144	V.32	HW	COMMS	BOX	DES
AUSTRALIA	Banksia Technology Pty. Ltd.	Pro 34	V.34	HW	COMMS	BOX	DES
AUSTRALIA	Banksia Technology Pty. Ltd.	Procard 34	V.34	HW	COMMS	PCMCIA	DES
AUSTRALIA	Carbon Based Software	CryptStream	OS2	SW	FILE	PGM	DES
AUSTRALIA	Carbon Based Software	Zipstream Secure	OS2	SW	FILE	PGM	DES
AUSTRALIA	Cipher Research Laboratories	??					
AUSTRALIA	Cryptsoft Pty Ltd.	SSLeay	DOS	SW	SSL	PGM	RSA
AUSTRALIA	Cryptsoft Pty Ltd.	SSLftp	DOS	SW	FTP	PGM	DES
AUSTRALIA	Cybanim Pty Ltd.	DES32 v1.02	PC	SW	GENERAL	KIT	DES
AUSTRALIA	Cybanim Pty Ltd.	DESf v1.4	PC	SW	GENERAL	PGM	DES
AUSTRALIA	Cybanim Pty Ltd.	LUC 2.03	PC	SW	GENERAL	PGM	LUC
AUSTRALIA	Cybanim Pty Ltd.	SIFR v2.0	PC	SW	GENERAL	PGM	RSA
AUSTRALIA	DataCrypt	LetterCrypt	PC	SW	COMMS	PGM	
AUSTRALIA	DataCrypt	NoteCrypt	PC	SW	FILE	PGM	
AUSTRALIA	DataCrypt	PassCrypt	DOS	SW	FILE	PGM	
AUSTRALIA	Eracom Pty Ltd.	CP 7000 Intelligent Encryption Adaptor	PCI	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	CP500 Slave Encryption Adaptor	PCI	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	CPROV	SOLARIS	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	CSA 7000 PCI Hardware Crypto Adaptor	PCI	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	Encryption Services API	OS2	SW	GENERAL	KIT	DES
AUSTRALIA	Eracom Pty Ltd.	ERA 2007 Line Encryptor	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Eracom Pty Ltd.	ERA 4007 Line Encryptor	V.24	HW	COMMS	BOX	DES
AUSTRALIA	Eracom Pty Ltd.	JPROV	SOLARIS	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	MCE Slave Encryption Adaptor	PC	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	PC Vault	DOS	SW	DISK	PGM	DES
AUSTRALIA	Eracom Pty Ltd.	PCASM Intelligent Encryption Adaptor	ISA	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	PCE Slave Encryption Adaptor	ISA	HW	GENERAL	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	ProtectSNA	ERACOM BOARDS	SW/HW	COMMS	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	RSA API	OS2	SW	GENERAL	PGM	RSA
AUSTRALIA	Eracom Pty Ltd.	SECLink	X.25	HW	COMMS	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	SECPac	X.25	HW	COMMS	BOARD	DES
AUSTRALIA	Eracom Pty Ltd.	Series 90 Eracom Security Module (ESM)	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Eric Young	CryptL99	ANY	SW	GENERAL	PGM	DES
AUSTRALIA	Eric Young	fcrypt	ANY	SW	FILE	PGM	DES
AUSTRALIA	Eric Young	libdes	ANY	SW	GENERAL	KIT	DES
AUSTRALIA	Microlock	Kinetic Access		SW	FILE		
AUSTRALIA	Mosaic Industries	Touch Lock	WIN95	SW	DISK	PGM	PROP
AUSTRALIA	Mosaic Industries	Touch Net II		SW/HW	FILE		
AUSTRALIA	NetSafe	EXE Guardian	ANY	SW	PROGRAMS	KIT	DES
AUSTRALIA	News Datacom	N-Sure Access 1000	WK	HW	COMMS	BOARD	DES
AUSTRALIA	NexSol	Ntrust	WIN	SW	FILE	KIT	
AUSTRALIA	Nick Payne	Cryptext	WIN95	SW	FILE	PGM	RC4
AUSTRALIA	Randata	Megacrypt High Speed Data Encryptor	RS422/V.11	HW			PROP
AUSTRALIA	Robust Software	Block-It					
AUSTRALIA	RSA Data Security Australia	RSA BSAFE SSL-C v1.0	WIN32	SW	SSL	KIT	DES
AUSTRALIA	Secure Network Solutions	FAXSAFE	telephone	HW	VOICE	BOX	PROP
AUSTRALIA	Secure Network Solutions	GSA 1000 Duplex Mini Scrambler	RADIO	HW	VOICE	BOARD	
AUSTRALIA	Secure Network Solutions	GSA 1300	RADIO	HW	VOICE	BOARD	PROP
AUSTRALIA	Secure Network Solutions	Guardian-E Data Encryptor	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	Guardian-EM Encryptor Modem	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	Guardian-EMP Data Encryptor	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	Guardian-EP Data Encryptor	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	Megacrypt High Speed Data Encryptor	RS422/V.11	HW	COMMS	BOX	PROP

**GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS**

AUSTRALIA	Secure Network Solutions	RD185 Fax	telephone	HW	FAX	BOX	PROP
AUSTRALIA	Secure Network Solutions	RD187 Data Encryptor	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	Secure Management Systems(SMS)	ETHERNET	SW/HW	COMMS	PGM	3DES
AUSTRALIA	Secure Network Solutions	SecureLine	TELEPHONE	HW	FAX	BOX	DES
AUSTRALIA	Secure Network Solutions	SecureNET Data Encryptor	X.25	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	SecureNET HSP	ETHERNET	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	SecurLAN Network Encryption Unit - Router (NEU-RT)		HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	Securlink Data Encryptor	RS232	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	SecurPAC EM Encryptor Modem	V.24	HW	COMMS	BOX	DES
AUSTRALIA	Secure Network Solutions	SecurPAC IEM	ETHERNET	HW	COMMS	PCMCIA	DES
AUSTRALIA	Secure Network Solutions	SecurPac PEM Data Encryptor	X.25	HW	COMMS	BOX	DES
AUSTRALIA	Security Domain Pty Ltd	Secure Attache	WIN	SW	FILE	PGM	DES
AUSTRALIA	TRAC Systems	??					
AUSTRALIA	Tracom	??					
AUSTRIA	Eshelbeck, Steiner, Beitelmaier	Coded Drag	WIN95	SW	FILE	PGM	DES
AUSTRIA	IAIK, TU Graz	IAIK JCE (Java Cryptographic Extension) System 700	JAVA	SW	GENERAL	KIT	DES
AUSTRIA	Mils Elektronik		PC			PGM	PHONE
AUSTRIA	Mils Elektronik			HW	VOICE	PHONE	
AUSTRIA	Mils Elektronik	Fax Encryptor		HW	FAX	BOX	
AUSTRIA	Siemens AG Austria	Document Security Service (DSS) Version 2	WIN	SW	FILE	KIT	DES
AUSTRIA	University of Linz	Coded Drag	WIN95	SW	FILE	PGM	DES
BELGIUM	CNET	RSA chip	TTL	HW	GENERAL	CHIP	RSA
BELGIUM	GSA Ran Data Europe	MARTLET					
BELGIUM	Highware, Inc.	FileCrypt	MAC	SW	EMAIL	PGM	
BELGIUM	Highware, Inc.	Fileguard 3.0	MAC	SW	FILE	PGM	DES
BELGIUM	Lintel Security	CRY12C102 DES Chip		HW	GENERAL	CHIP	3DES
BELGIUM	Lintel Security	PC DES/RSA Card	PC	SW/HW	COMMS	PCMCIA	DES
BELGIUM	Lintel Security	PQR 512 RSA Chip	TTL	HW	GENERAL	CHIP	RSA
BELGIUM	UTI-MACO Belgium	CryptMail	ANY	SW	EDI	PGM	DES
BELGIUM	Vector	??					
CANADA	Adam Berent	ABI-Coder 2.0	WIN32	SW	FILE	PGM	PROP
CANADA	Atlantic Systems Group (ASG)	TurnStyle Firewall System (TFS)	UNIX	SW	COMMS	PGM	DES
CANADA	Authentex/NovaStor	DataSafe	WIN	SW	FILE	PGM	BLOWFISH
CANADA	Authentex/NovaStor	QuickSafe	WIN	SW	FILE	PGM	BLOWFISH
CANADA	Authentex/NovaStor	Security Suite	WIN32	SW	FILE	PGM	BLOWFISH
CANADA	Certicom	CardSecrets CS 1000	ANY	HW	COMMS	PCMCIA	DES
CANADA	Certicom	Elliptic Curve Toolkit (Beta Version)	DOS	SW	GENERAL	KIT	DES
CANADA	Certicom	FaxSecrets FS 1000	RJ-11	HW	FAX	BOX	DES
CANADA	Certicom	FS 3000		HW	FAX	BOX	
CANADA	Certicom	MOBIUS Integrated Security Solutions	ANY	SW	GENERAL	KIT	DES
CANADA	Certicom	Security Builder Crypto Toolkit		SW		KIT	DES
CANADA	Certicom	TaxSecrets	PC	SW	FILE	PGM	DES
CANADA	Certicom	TradeSecrets TS 2000	PC	HW	COMMS	BOARD	DES
CANADA	Chrysalis ITS	LUNA 2	WIN/NT	SW/HW	COMMS	PCMCIA	DES
CANADA	Chrysalis ITS	LUNA CA	WIN/NT	SW/HW	KEYS	PCMCIA	DES
CANADA	Chrysalis ITS	LUNA Toolkit	WIN/NT	SW/HW	COMMS	PCMCIA	DES
CANADA	Chrysalis ITS	LUNA VPN	WIN/NT	SW/HW	VPN	BOARD	DES
CANADA	Compression Technologies, Inc.	CTI WARP II	RS232	HW	COMMS	BOX	PROP
CANADA	Compression Technologies, Inc.	CTI WARP III	RS232	HW	COMMS	BOX	PROP
CANADA	Compression Technologies, Inc.	WARP IV Frame Master	V.35	SW/HW	COMMS	KIT	
CANADA	CRYPTOCARD Corporation	SB-1 Electronic Diskette Token	PC	HW	DISK	DISK	PROP
CANADA	Earthworks Communications	??		SW			
CANADA	Entrust Technologies	Entrust File Toolkit		SW	COMMS	KIT	DES
CANADA	Entrust Technologies	Entrust Lite	WIN	SW	FILE	PGM	DES
CANADA	Entrust Technologies	Entrust/Client	MAC	SW	FILE	PGM	DES
CANADA	Entrust Technologies	Entrust/Direct	WIN	SW	COMMS	PGM	RSA
CANADA	Entrust Technologies	Entrust/ICE 4.0	WIN/NT	SW	FILE	PGM	DES
CANADA	Entrust Technologies	Entrust/Manager	MAC	SW	COMMS	PGM	PROP
CANADA	Entrust Technologies	Entrust/Session Toolkit	MAC	SW	COMMS	KIT	DES
CANADA	Entrust Technologies	Entrust/Solo	WIN95	SW	DISK	PGM	CAST
CANADA	Freestyle Software, Inc.	Avalanche Java Cryptographic Toolkit		SW	GENERAL	KIT	DES
CANADA	Gandalf	GandalfLZA Plus	PC	SW	COMMS	PGM	PROP
CANADA	Ilex Systems Inc.	Securafile	WIN	SW	EMAIL	PGM	DES
CANADA	Inforon Technologies, Inc.	NETSEC		SW			
CANADA	Isolation Systems	Infocrypt Desktop	WIN95	SW	COMMS	PGM	DES
CANADA	Isolation Systems	Infocrypt Enterprise	ENET	HW	COMMS	BOX	DES
CANADA	Isolation Systems	Infocrypt Extreme PCI	DOS	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	Infocrypt Server	WIN/NT	SW	COMMS	PGM	DES
CANADA	Isolation Systems	Infocrypt Solo	WIN95	SW	VPN	PGM	DES
CANADA	Isolation Systems	ISAC 1100	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 1500	TOSHIBA	SW/HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 2200	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 2400	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 2500	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 3200	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 3500	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISAC 4200	MAC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISBR		HW	COMMS		
CANADA	Isolation Systems	ISE 2100	PC	HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISFE Frame Relay	NETWORK	SW/HW	COMMS	PGM	DES
CANADA	Isolation Systems	ISPE/M		HW	COMMS		DES
CANADA	Isolation Systems	ISPE/R (Isolation System Packet Encryptor/Router)	NETWORK	SW/HW	COMMS	BOARD	DES
CANADA	Isolation Systems	ISPE/SA (Standalone Version)	NETWORK	HW	COMMS		DES
CANADA	Isolation Systems	ISTM (Isolation System Table Management)	NETWORK				
CANADA	Isolation Systems	ISXE/M	X.25				
CANADA	Kyberpass Corporation	Kyberpass	WIN	SW	COMMS	PGM	DES

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

CANADA	Micro Tempus, Inc.	Tempus-CLIP	DOS	SW/HW		PGM	
CANADA	Milkyway Networks Corporation	Black Hole	ANY	SW	COMMS	PGM	
CANADA	MPR Teltech	??			SATELLITE		
CANADA	Northern Telecom Canada Ltd. (Data Comm. Products)	Packet Data Security Overlay (PDSO)	ANY	HW	COMMS	BOX	DES
CANADA	Northern Telecom Secure Networks	DMS NTX Switch (Cellular) CDPD					
CANADA	Octothor Industries	Canine Mail	WIN32	SW	EMAIL	PGM	BLOWFISH
CANADA	Okiok Data	Data Encryption Board (DEB)	PC	HW	FILE	BOARD	DES
CANADA	Okiok Data	FileSafe Light	WIN	SW	FILE	PGM	
CANADA	Okiok Data	RAC/M IX IPC	PCI	HW	EDI	SMART CARD	DES
CANADA	Okiok Data	RAC/M Open Cryptographic Server	OS2	HW	EDI	PC	DES
CANADA	Okiok Data	Secure Server for Netware	NOVELL	SW/HW	FILE	WK	DES
CANADA	Queen's University	RSA chip		HW		CHIP	RSA
CANADA	Scientific Atlantic	??			Pay TV	PROP	
CANADA	Secure Computing Corporation	BorderWare Firewall Server	PC	SW/HW	COMMS	KIT	DES
CANADA	Secure ISDN Terminals	Ilex					
CANADA	Secured Communications Inc. (SCI)	Session Key	PC	HW	FILE	PCMCIA	DES
CANADA	Sierra Wireless	CDPD (Cellular Digital Packet Data)	V.32		EMAIL		RSA
CANADA	Sierra Wireless	PocketPlus	WIN	HW		BOX	CDPD
CANADA	Silanis Technology	Approvelt CAD	WIN	SW	FILE	PGM	DES
CANADA	Silanis Technology	Approvelt Desktop	WIN	SW	FILE	PGM	PROP
CANADA	Silanis Technology	Approvelt Toolkit	WIN	SW	GENERAL	KIT	DES
CANADA	The Enigma Group	ENIGMA-7 Encryption	WIN	SW	FILE	PGM	PROP
CANADA	TimeStep Corporation	PERMIT 1010 PC LAN Security Module	pc	SW/HW	COMMS	PGM	DES
CANADA	TimeStep Corporation	PERMIT 1011 PC LAN Security ISA Card	pc	SW/HW	COMMS	PGM	DES
CANADA	TimeStep Corporation	PERMIT 1012 PC LAN Security PCI Card	pc	SW/HW	COMMS	PGM	DES
CANADA	TimeStep Corporation	PERMIT 1013 PC LAN Security MCA Card	pc	SW/HW	COMMS	PGM	DES
CANADA	TimeStep Corporation	PERMIT 1060 Secure Ethernet Bridge	WIN	SW/HW	COMMS	BOX	3DES
CANADA	TimeStep Corporation	PERMIT 2010 PC LAN Security Module	PC	SW/HW	COMMS	BOARD	DES
CANADA	TimeStep Corporation	PERMIT 2018 PC Remote Security		SW	COMMS	PGM	DES
CANADA	TimeStep Corporation	PERMIT 3010	PC	SW/HW	DISK	BOARD	DES
CANADA	TimeStep Corporation	PERMIT 9010 SNMS	PC	SW/HW	IPSEC		DES
CANADA	TimeStep Corporation	PERMIT 9300	pc	SW/HW	COMMS	PGM	
CANADA	TimeStep Corporation	PERMIT S/Token	PC	HW	GENERAL	PCMCIA	
CANADA	TimeStep Corporation	PERMIT Security Gateway	NETWORK	HW	COMMS	BOX	
CANADA	TimeStep Corporation	PERMIT Security MicroGate	ENET	HW	COMMS	BOX	
CANADA	TimeStep Corporation	PERMIT SVPN		HW	VPN		
CANADA	Tundra Semiconductor Corp.	CA20C03A	TTL	HW	GENERAL	CHIP	DES
CANADA	Tundra Semiconductor Corp.	CA20C03A/W DES Encryption Processor					DES
CANADA	Tundra Semiconductor Corp.	CA20C03W		HW	GENERAL	CHIP	DES
CANADA	Tundra Semiconductor Corp.	CA95C68/18/09	TTL	HW	GENERAL	CHIP	DES
CANADA	Tundra Semiconductor Corp.	NM830	PC	SW/HW	FILE	PGM	
CANADA	Tundra Semiconductor Corp.	Permit LAN Encryption modules for LAN adapters					
CANADA	Tundra Semiconductor Corp.	Transmission Access Platform (TAP)	RS232	HW		BOX	DES
CANADA	Xcert International Inc.	Sentry CA	WIN/NT	SW/HW	KEYS		RSA
CANADA	Xcert International Inc.	Sentry RA	WIN/NT	SW/HW	KEYS		RSA
CANADA	Zoomit Corporation	Remote Link Plus	PC	SW	COMMS		RSA
CZECH REPUBLIC	Alwil Software	Access Control SUPervisor	DOS	SW	FILE	PGM	
CZECH REPUBLIC	Alwil Software	Fort Knox		SW	DISK	PGM	
CZECH REPUBLIC	Decros spol. s r.o.	Protect95	WIN95	SW	FILE	PGM	PROP
CZECH REPUBLIC	Decros spol. s r.o.	ProtectNT	WIN/NT	SW	FILE	PGM	PROP
CZECH REPUBLIC	Decros spol. s r.o.	Security Card		HW			
DENMARK	Aarhus University, Computer Science Department	VICTOR	TTL	HW	GENERAL	CHIP	RSA
DENMARK	CryptoMathic A/S	6303 SIS	6303MP	SW	GENERAL	PGM	SIS
DENMARK	CryptoMathic A/S	8051 DES	INTEL 8031	SW	GENERAL	PGM	DES
DENMARK	CryptoMathic A/S	DES for IBM/370	MF	SW		KIT	DES
DENMARK	CryptoMathic A/S	DES Kernel	PC	SW	GENERAL	KIT	DES
DENMARK	CryptoMathic A/S	DES Security Mechanisms	PC	SW	GENERAL	KIT	DES
DENMARK	CryptoMathic A/S	DSP 56000 DES	DSP56000/1	SW	GENERAL	PGM	DES
DENMARK	CryptoMathic A/S	DSP 56000 RSA	DSP56000/1	SW	GENERAL	PGM	RSA
DENMARK	CryptoMathic A/S	F2F (File-to-File)	PC	SW	FILE	PGM	DES
DENMARK	CryptoMathic A/S	Multiprecision Kernel	PC	SW	GENERAL	KIT	RSA
DENMARK	CryptoMathic A/S	PrimeDrink Java Toolbox	JAVA	SW	GENERAL	KIT	DES
DENMARK	CryptoMathic A/S	PrimeLink C Toolbox	C CODE	SW	GENERAL	KIT	DES
DENMARK	CryptoMathic A/S	RSA Security Mechanisms	PC	SW	GENERAL	KIT	RSA
DENMARK	CryptoMathic A/S	Security API		SW		KIT	DES
DENMARK	GN Datacom	safeMatic Security Module	ANY	HW	COMMS	BOX	DES
DENMARK	Inteltech Omniware	iCrypt 3.2	WIN95	SW	FILE	PGM	DES
DENMARK	Kommunedata	EDI-SAFE	PC	HW	COMMS	CHIP	
DENMARK	LSI Logic/Dataco AS	Dataco L5A4043 2030025402	PC	HW	GENERAL	CHIP	DES
DENMARK	LSI Logic/Dataco AS	Dataco LSA4043 2030025402	TTL	HW	GENERAL	CHIP	DES
DENMARK	Telesec	Telesec	ANY	SW	EDI	KIT	DES
ESTONIA	Cybernetica	Privador SVPN	ETHERNET	SW/HW	IPSEC	BOX	DES
ESTONIA	Cybernetica	Secure Socket Agent	WIN95	SW	COMMS	PGM	3DES
FINLAND	Antti Louko	AloDES	ANY	SW	GENERAL	PGM	DES
FINLAND	Datafellows Ltd.	F-Secure Commerce	WIN	SW	COMMS	PGM	DES
FINLAND	Datafellows Ltd.	F-Secure Desktop	WIN	SW	FILE	PGM	BLOWFISH
FINLAND	Datafellows Ltd.	F-Secure FileCrypto	WIN/NT	SW	FILE	PGM	3DES
FINLAND	Datafellows Ltd.	F-Secure SSH Client	MAC	SW	COMMS	PGM	

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

FINLAND	Datafellows Ltd.	F-Secure SSH Server	UNIX	SW	COMMS	PGM	3DES
FINLAND	Datafellows Ltd.	F-Secure SSH Tunnel&Terminal	MAC	SW	COMMS	PGM	RSA
FINLAND	Datafellows Ltd.	F-Secure Virtual Private Network	PC	SW	VPN	PGM	3DES
FINLAND	Datafellows Ltd.	F-Secure VPN+	WIN95	SW	IPSEC	PGM	DES
FINLAND	Jetico, Inc	BestCrypt NP	WIN95	SW	FILE	PGM	BLOWFISH
FINLAND	Jetico, Inc.	BestCrypt Lite	WIN	SW	FILE	PGM	DES
FINLAND	Jetico, Inc.	BestCrypt+	WIN	SW/HW	FILE	PGM	GOST 28147-89
FINLAND	Jetico, Inc.	LS06C20		HW		CHIP	GOST28147
FINLAND	SSH Communications Security	SSH	MAC	SW	COMMS	PGM	ELGAMAL
FINLAND	SSH Communications Security	SSH IPsec Express Toolkit	ANY	SW	IPSEC	KIT	3DES
FINLAND	SSH Communications Security	SSH ISAKMP/Oakley Toolkit	ANY	SW	ISAKMP	KIT	3DES
FRANCE	ActivCard	ActivCard X9.9 Token	PC	HW	COMMS	TOKEN	DES
FRANCE	Atlantis	CSA / X.25	X.25	SW/HW	COMMS	BOX	PROP
FRANCE	Bull Worldwide Information Systems Inc.	CP8 Log	WK	SW/HW	DISK	PGM	
FRANCE	Bull Worldwide Information Systems Inc.	OpenMaster	WIN/NT	SW	COMMS	PGM	DES
FRANCE	Bull Worldwide Information Systems Inc.	SecurWare VPN	ETHERNET	SW/HW	VPN	BOX	DES
FRANCE	CCETT	??					
FRANCE	CSEE - Division Communication et Informatique	??					
FRANCE	Dassault Automatismes et Telecommunications	??					
FRANCE	Digital Equipment Corp. (DEC), Paris Research Lab	RSA chip		HW		CHIP	RSA
FRANCE	Herve Schauer Consultants	HSC-GK (Gate Keeper)	UNIX				DES
FRANCE	Hewlett Packard France	Cryptographic Security Module for the HP9000	HP/UX	HW	GENERAL	SMART CARD	DES
FRANCE	LAAS	RSA implementations					RSA
FRANCE	Philips Communication Systems	P83C852 Smart Card Crypto Controller	TTL	HW	GENERAL	CHIP	RSA
FRANCE	Rast Electronics	Crypt It					
FRANCE	SAGEM	??					
GERMANY	Andreas Kupries	TCL Binary Large Objects,eXtension(Tcl-BlobX) v1.2	TCL 7.5	SW	GENERAL	KIT	DES
GERMANY	Andreas Muller Software	??					
GERMANY	Baller & Huwig	Louis Cypher LC-1	telephone	HW	VOICE	BOX	RSA
GERMANY	BioData GmbH	Babylon Meta ISDN		HW	COMMS	BOX	3DES
GERMANY	BioData GmbH	Babylon Meta Serial	RJ-45	HW	COMMS	BOX	3DES
GERMANY	BioData GmbH	Babylon Standard	ISDN	HW	COMMS	BOX	3DES
GERMANY	BioData GmbH	BIGFire+	ETHERNET	HW	COMMS	BOX	3DES
GERMANY	BROKAT Infosystems AG	X*PRESSO Security Package 3.0	JAVA	SW	SSL	KIT	IDEA
GERMANY	CCI (Competence Center Informatik GmbH)	??					
GERMANY	CE Infosys GmbH	CD-Crypt	WIN32	SW	CD-ROM	PGM	3DES
GERMANY	CE Infosys GmbH	CryptCard	PC	HW	GENERAL	PCMCIA	DES
GERMANY	CE Infosys GmbH	DataCrypt	WIN32	SW/HW	FILE		3DES
GERMANY	CE Infosys GmbH	Elkey	PC	HW	DISK	BOX	DES
GERMANY	CE Infosys GmbH	Fastcrypt	PCI	HW	GENERAL	BOARD	DES
GERMANY	CE Infosys GmbH	IP-Crypt	WIN32	SW/HW	COMMS	PGM	3DES
GERMANY	CE Infosys GmbH	IPC-Box	UNIX	HW	COMMS	BOX	3DES
GERMANY	CE Infosys GmbH	PCI-Crypt	WIN32	HW	GENERAL	CHIP	3DES
GERMANY	CE Infosys GmbH	RSA Smart Card	PCMCIA	HW	COMMS	SMART CARD	3DES
GERMANY	CE Infosys GmbH	RSA-Crypt	WIN32	SW/HW	FILE	PGM	3DES
GERMANY	CE Infosys GmbH	Simo PCI/AT	WIN32	HW	GENERAL	BOARD	3DES
GERMANY	CE Infosys GmbH	SuperCrypt	TTL	HW	GENERAL	CHIP	DES
GERMANY	Cedric Reinartz	ASPICrypt		SW	FILE	PGM	BLOWFISH
GERMANY	Celticon	Scrypt	WIN	SW	DISK		DES
GERMANY	Christoph Martin	SSL-MZ telnet	UNIX	SW	TELNET	PGM	IDEA
GERMANY	CryptoSoft GmbH	Blowfish Development Kit	DOS	SW	GENERAL	KIT	BLOWFISH
GERMANY	CryptoSoft GmbH	DES3 Development Kit	DOS	SW	GENERAL	KIT	3DES
GERMANY	CryptoSoft GmbH	Enigma for Windows 98	WIN95	SW	FILE	PGM	DES
GERMANY	CryptoSoft GmbH	Enigma for Windows v 3.1	WIN	SW	FILE	PGM	DES
GERMANY	DataSafe	ENCRYPT-IT v3.06	PC	SW	FILE	PGM	DES
GERMANY	DataSafe	WINDEX! v2.01 for DOS	PC	SW	FILE	PGM	PROP
GERMANY	DataSafe	WINDEX! v2.01 for Windows	PC	SW	FILE	PGM	PROP
GERMANY	DemCom	Steganos	WIN95	SW	FILE	PGM	PROP
GERMANY	DTM Data TeleMark GmbH	DICA 7800 ISDN Line Encryptor	ISDN	HW	COMMS	BOX	DES
GERMANY	EZI GmbH	H-Crypt		SW			FEAL
GERMANY	FAST ComTec GmbH	MACS 1000	PC	SW/HW	COMMS	PGM	DES
GERMANY	GAO	??					
GERMANY	Gliss & Herweg	GH-DES		SW	FILE		DES
GERMANY	Glück & Kanja GmbH	CryptoEx Security Suite	WIN32	SW	EMAIL	PGM	IDEA
GERMANY	GMD	SecuDE PEM	UNIX	SW	EMAIL	PGM	DES
GERMANY	GMD	SECUDE-5.0	DOS	SW	GENERAL	KIT	
GERMANY	Interconnect	Babylon		HW	COMMS		DES
GERMANY	Interconnect	BIGfire	telephone	HW			DES
GERMANY	Jurgen Meyer, Frank Gadegast	SECMPEG		SW	VIDEO		DES
GERMANY	Karl Huwig	LC-1 Fax/Data Encryption Unit		HW	FAX	BOX	RSA
GERMANY	Karl Huwig	LC-1 Voice Encryption Unit	telephone	HW	VOICE	BOX	RSA
GERMANY	KryptoKom	KryptoGuard Modem	PC	HW	COMMS	BOX	DES
GERMANY	KryptoKom	KryptoGuard X.25	X.25	HW	GENERAL	BOX	DES
GERMANY	KryptoKom	KryptoServer	V.24	HW	GENERAL	BOARD	DES
GERMANY	KryptoKom	SmartGuard B	DOS	SW/HW	GENERAL	PGM	DES
GERMANY	Mathias Kretschmer	ProCrypt	AMIGA	SW	FILE	PGM	DES
GERMANY	Roland Mundloch	Acrypt	WIN95	SW	FILE	PGM	PROP
GERMANY	Siemens Vertrauliche Kommunikation	ISDN - Channel			VOICE		
GERMANY	Siemens-Nixdorf	??					DES
GERMANY	Siemens-Nixdorf	SESAME	UNIX	SW	COMMS	PGM	
GERMANY	Siemens-Nixdorf	SICURE		HW		CHIP	DES

**GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS**

GERMANY	Siemens-Nixdorf	Trusted Web		SW/HW	COMMS	PGM	
GERMANY	SIT	ComSave SIC 410	V.24	HW	COMMS	BOARD	PROP(FEAL 16X) DES
GERMANY	T. Billenstein	tbCrypt	DOS	SW	FILE	PGM	
GERMANY	Tela Versicherung	??					
GERMANY	Tele Security Timmann GmbH & Co.	TST 3010 High Performance Mil- Spec Cipher Terminal	RADIO	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 3550 Handy Crypt	PRINTER	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 3570 Pocketcrypt	telephone	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 3677 VDU/Screen-Oriented Headquarter Cipher		HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 4043 HF Slow Speed Modem with encryption	PC	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 4045 HF Modem 2.4Kbps with encryption	PC	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5500 Crypto Modem	PC	SW/HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5560 DataCipher Set	RS232	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5573 C Data Encryptor	PC	HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5573 F/C		HW	FAX		PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5573 H/C		HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5573 PC		HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 5573 X/C		HW	COMMS	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 7595 HF voice encryption	telephone	HW	VOICE	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 7610 Secure Office Telephone	telephone	HW	VOICE	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 7698 Miniature Military Voice Coder	telephone	HW	VOICE	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 7700 Telephone Vocoder and Modem	telephone	HW	VOICE	BOX	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 8010 Spreadpectrum Radio	RS232	HW	COMMS	BOARD	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 9669 Telex Cipher Module	TELEX	HW	COMMS	BOARD	PROP
GERMANY	Tele Security Timmann GmbH & Co.	TST 9700 INMARSAT "C" encryptor	PC	SW/HW	COMMS	BOX	PROP
GERMANY	Telenet Kommunikation Systeme	File Transfer	IBM/MVS	SW	FILE	KIT	DES
GERMANY	Toshiba Europe GmbH	CryptCard	PC	HW	DISK	PCMCIA	DES
GERMANY	Utimaco Safeware AG	BACK-Guard	PC	SW	DISK	PGM	DES
GERMANY	Utimaco Safeware AG	C:Crypt	PC	SW	FILE	PGM	PROP
GERMANY	Utimaco Safeware AG	Cryptware Board 1.3		HW	EMAIL	BOARD	DES
GERMANY	Utimaco Safeware AG	Cryptware Server 3.0		HW	COMMS	BOX	DES
GERMANY	Utimaco Safeware AG	Cryptware Toolkit	ANY	SW	GENERAL	KIT	3DES
GERMANY	Utimaco Safeware AG	PC/DACS for DOS + Windows	DOS	SW	FILE	PGM	
GERMANY	Utimaco Safeware AG	SAFE-Board I	PC	HW	DISK	BOARD	XOR
GERMANY	Utimaco Safeware AG	SAFE-Board II	PC	HW	DISK	BOARD	DES
GERMANY	Utimaco Safeware AG	SAFE-Board III	PC	HW	DISK	BOARD	DES
GERMANY	Utimaco Safeware AG	SAFE-Guard OS/2 3.0	PC	SW	DISK	PGM	DES
GERMANY	Utimaco Safeware AG	SAFE-Guard Professional 3.2C	PC	SW	DISK	PGM	DES
GERMANY	Utimaco Safeware AG	SafeGuard DACS for Windows 95	WIN95	SW	GENERAL	PGM	
GERMANY	Utimaco Safeware AG	SafeGuard Desktop 2.10	OS2	SW	DISK	PGM	DES
GERMANY	Utimaco Safeware AG	SafeGuard Easy 1.01	WIN/NT	SW	DISK	PGM	DES
GERMANY	Utimaco Safeware AG	SafeGuard Easy 1.13	WIN95	SW	DISK	PGM	DES
GERMANY	Utimaco Safeware AG	SafeGuard Easy 2.18	OS2	SW	DISK	PGM	DES
GERMANY	Utimaco Safeware AG	SafeGuard Easy 2.24	DOS	SW	DISK	PGM	DES
GERMANY	Utimaco Safeware AG	SafeGuard LAN Crypt 1.0	WIN/NT	HW	COMMS	PGM	DES
GERMANY	Utimaco Safeware AG	SafeGuard Professional 2.10	OS2	SW	DISK	PGM	DES
GERMANY	Utimaco Safeware AG	SafeGuard Sign&Crypt	WIN32	SW	FILE	PGM	IDEA
GERMANY	Utimaco Safeware AG	SafeGuard VPN	UNIX	SW	VPN	PGM	3DES
GERMANY	Utimaco Safeware AG	SIGN-Guard	PC	SW	EMAIL	PGM	DES
GERMANY	Wilhelm Heibl Werke	??			VOICE		
GREECE	John Ioannidis	Jl's IPsec	BSD	SW	IPSEC	PGM	DES
HONG KONG	ROCTEC Enterprises, Ltd.	??					
HONG KONG	Techtrend Engineering, Ltd. (TEL)	??					
HONG KONG	Triple D Ltd.	P-8 Security Master Card	PC	SW/HW	GENERAL	PGM	DES
ICELAND	Logi Ragnarsson	Cryptonite Java Package	JAVA	SW	FILE	KIT	
ICELAND	Softis hf	LOUIS Security Package	JAVA	SW	COMMS	PGM	3DES
INDIA	Bharat Electronics Ltd.	Analogue Code Encryption Unit	RADIO	HW	PW	BOX	
INDIA	Bharat Electronics Ltd.	AZ7308 E Speech Encryption Unit	RADIO	HW	VOICE	BOX	
INDIA	Chenab Info Technology	Cryptic	PC	SW	FILE	PGM	PROP
IRAN	Communications Industries Group	AEU-212 Encryption Unit	RADIO	HW	VOICE	BOX	
IRAN	Communications Industries Group	AEU-313/A Encryption System	RADIO	HW	VOICE	BOX	
IRAN	Communications Industries Group	DEU-104 Digital Voice Encryption Unit	RADIO	HW	VOICE	BOX	
IRAN	Communications Industries Group	FEU-4110 Facsimile Encryption Unit	telephone	HW	FAX	BOX	
IRAN	Communications Industries Group	LEU-313 Telephone Encryption Unit	telephone	HW	VOICE	BOX	
IRAN	Communications Industries Group	TEU-520 Telex Encryption Unit	TELEX	HW	COMMS	BOX	
IRELAND	AT&T Network Systems Ireland	AT&T StrarLAN 10		SW			
IRELAND	Eurologic Systems, Ltd.	Datacrypt	SCSI	HW	TAPE	BOX	PROP(BSA) BSA
IRELAND	Eurologic Systems, Ltd.	DC-200		HW	DISK	BOX	
IRELAND	Key Exchange Ireland Ltd.	??	PC				
IRELAND	Priority Data Systems Ltd	??					
IRELAND	Shamus Software Ltd.	??					
IRELAND	Silicon Software Systems Ltd.	??					
IRELAND	Software and Systems Engineering Ltd.	TrustedMIME	WIN95	SW	S/MIME	PGM	3DES
IRELAND	Software and Systems Engineering Ltd.	TrustedWeb Express	WIN95	SW	COMMS	PGM	
IRELAND	Software and Systems Engineering Ltd.	TrustedWeb v. 2.0	WIN95	SW	COMMS	PGM	3DES
IRELAND	Software Systems Engineering Ltd.	??					
IRELAND	Systemics Ltd.	Cryptix Cryptographic Library for Java 3.03	JAVA	SW	GENERAL	KIT	DES
IRELAND	Systemics Ltd.	Cryptix Java Cryptographic Extensions	JAVA	SW	GENERAL	KIT	DES
IRELAND	Systemics Ltd.	Elliptix	JAVA	SW	GENERAL	KIT	ECC
IRELAND	Systemics Ltd.	PGP Library for Perl	PERL	SW	GENERAL	KIT	PGP
ISLE OF MAN	Invisimail International Ltd.	Invisimail V3.1	WIN	SW	EMAIL	PGM	RPK

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

ISRAEL	Aladdin Knowledge Systems, Ltd.	ASECrypto	WIN95	SW	FILE	KIT	DES
ISRAEL	Aladdin Knowledge Systems, Ltd.	HASP	DOS	HW			
ISRAEL	Algorithmic Research Ltd.	CryptoKit	DOS	SW	GENERAL	KIT	DES
ISRAEL	Algorithmic Research Ltd.	CryptoSafe		HW	KEYS		DES
ISRAEL	Algorithmic Research Ltd.	CryptoServer	ETHERNET	SW		SMART CARD	
ISRAEL	Algorithmic Research Ltd.	CryptoServer	ETHERNET	HW	GENERAL	BOX	DES
ISRAEL	Algorithmic Research Ltd.	PrivateWire	ETHERNET	SW/HW	COMMS	PGM	DES
ISRAEL	Aliroo Ltd.	PrivaFile	WIN	SW	FILE	PGM	PROP
ISRAEL	Aliroo Ltd.	PrivaMail	WIN	SW	EMAIL	PGM	PROP
ISRAEL	Aliroo Ltd.	PrivaSoft	DOS	SW	FAX	PGM	PROP
ISRAEL	Carmel Software Engineering Ltd.	INFOLOCK	PC	SW	FILE	PGM	PROP
ISRAEL	CheckPoint Software Technologies Ltd	FireWall -1 4.0	UNIX	SW/HW	VPN	KIT	3DES
ISRAEL	CheckPoint Software Technologies Ltd	VPN-1 Accelerator Card	PCI BUS	HW	VPN	BOARD	DES
ISRAEL	CheckPoint Software Technologies Ltd	VPN-1 Appliance	V.35	HW	VPN	BOX	DES
ISRAEL	CheckPoint Software Technologies Ltd	VPN-1 SecuRemote	WIN95	SW	VPN	PGM	DES
ISRAEL	Elementrix Technologies Ltd.	POTP Secure FTP	WIN	SW		PGM	POTP
ISRAEL	Elementrix Technologies Ltd.	POTP Secure Mail	WIN	SW	EMAIL	PGM	POTP
ISRAEL	Iris Software	Comlock	UNIX				
ISRAEL	Iris Software	Irllock	UNIX				
ISRAEL	RADGUARD, Ltd	clPro-client	WIN32	SW	IPSEC	PGM	
ISRAEL	RADGUARD, Ltd	clPro-DMZ	ETHERNET	HW	IPSEC	BOX	DES
ISRAEL	RADGUARD, Ltd	clPro-HQ	ETHERNET	HW	IPSEC	BOX	3DES
ISRAEL	RADGUARD, Ltd	clPro-VPN	ETHERNET	HW	IPSEC	BOX	
ISRAEL	RADGUARD, Ltd	CryptoWall	ETHERNET	HW	COMMS	BOX	DES
ISRAEL	RADGUARD, Ltd	NetCryptor	X.25	HW	VPN	BOX	DES
ISRAEL	Secure Network Systems, Ltd.	Only You	DOS	HW	DISK	PCMCIA	
ISRAEL	Secure Network Systems, Ltd.	You & Me	DOS	HW	COMMS	PCMCIA	
ISRAEL	Tadiran	SEC-13					
ISRAEL	Tadiran	SEC-15					
ISRAEL	Tadiran	SEC-22					
ISRAEL	Vanguard Security Technologies Ltd.	MailGuardian	WIN/NT	SW	EMAIL	PGM	DES
ITALY	AMTEC SPA	AMTEC SPA Cryptocard	PCMCIA	HW	COMMS	SMART CARD	RSA
ITALY	AMTEC SPA	Crypto Device	PC	HW	COMMS	BOARD	RSA
ITALY	AMTEC SPA	CryptoBox	X.25	HW	COMMS	BOX	RSA
ITALY	AMTEC SPA	CryptoFile	WIN95	SW/HW	FILE	PGM	RSA
ITALY	AMTEC SPA	CS-860	X.25	HW	IPSEC	BOARD	3DES
ITALY	AMTEC SPA	RSA 512		HW	COMMS	CHIP	RSA
ITALY	CERT-IT	STEL	SUNOS	SW	COMMS	PGM	DES
ITALY	Eutron Spa	SmartKey plus / GSS	DOS	SW/HW		KIT	PROP
ITALY	Eutron Spa	SmartKey plus Buss /GSS	DOS	SW/HW	FILE	KIT	PROP
ITALY	Eutron Spa	SmartLock BASE	LAN	SW	DISK	PGM	PROP
ITALY	Eutron Spa	SmartLock DEFence	DOS	SW	DISK	PGM	PROP
ITALY	Eutron Spa	SmartLock DEScription	DOS	SW	DISK	PGM	DES
ITALY	Eutron Spa	SmartLock PROfessional	DOS	SW	DISK	PGM	PROP
ITALY	Systems Comunicazioni srl	Secure Desk-Top	WIN	SW	FILE	PGM	DES
ITALY	Systems Comunicazioni srl	Secure Plug-in for Eudora	WIN	SW	EMAIL	PGM	DES
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	ALLFAX 1000		HW	FAX	BOX	PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	Cryptophone 7000	TELEPHONE	HW	COMMS		PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	Cryptophone 7000 plus	TELEPHONE	HW	COMMS		PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	Cryptophone 7900		HW	COMMS	BOX	PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	KD111 C		HW	COMMS	BOX	PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	KV3000		HW	COMMS	BOX	PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	TX1020 C Mk III		HW	COMMS	BOX	PROP
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.	TX2020 C		HW	COMMS	BOX	PROP
JAPAN	ADVANCE Co., Ltd.	KPS Cipher Card		HW			
JAPAN	Compal Inc.	Pandora		HW	GENERAL	CHIP	RSA
JAPAN	Fujitsu Labs Ltd.	FJPEM v1.0	MANY	SW	EMAIL	PGM	DES
JAPAN	Mitsubishi Electric Corporation	CERTMANAGER v.B00	WIN32	SW	S/MIME	PGM	MISTY1
JAPAN	Mitsubishi Electric Corporation	CertMISTY V.B00	WIN32	SW	GENERAL	PGM	MISTY1
JAPAN	Mitsubishi Electric Corporation	Cryptofile vB00	WIN32	SW	DISK	PGM	MISTY1
JAPAN	Mitsubishi Electric Corporation	CryptoSign v.B00	WIN32	SW	EMAIL	PGM	MISTY1
JAPAN	Mitsubishi Electric Corporation	MELWALL A3000-1	ETHERNET	HW	COMMS	BOX	MISTY1
JAPAN	Mitsubishi Electric Corporation	MELWALL H3000-1	ETHERNET	HW	COMMS	BOX	MISTY1
JAPAN	Mitsubishi Electric Corporation	MELWALL P3000 v.E00	WIN32	SW	COMMS	PGM	MISTY1
JAPAN	Mitsubishi Electric Corporation	MELWALL P3000CL	WIN95	SW	COMMS	PGM	MISTY1
JAPAN	Mitsubishi Electric Corporation	PowerMisty v.B00	WIN/NT	SW	GENERAL	KIT	MISTY1
JAPAN	Mitsubishi Electric Corporation	TrustWeb v.B00	WIN32	SW	COMMS	PGM	MISTY1
JAPAN	Mitsubishi Electric Engineering Company Ltd	MISTYKEYPER v.B00	WIN/NT	SW/HW	KEYS	BOARD	MISTY1
JAPAN	Nihon RSA	RSA Chip		HW	GENERAL	CHIP	RSA
JAPAN	Nipon Telephone & Telegraph	Encryption Chip	ANY	HW	GENERAL	CHIP	3DES
JAPAN	Toshiba Information Systems (Japan)	Cypher Mail	WIN95	SW	EMAIL	PGM	
JAPAN	Yokohama National University	KPS L1CARD					
KOREA	Future Systems, Inc.	Future/TCP v4.0	DOS	SW	COMMS	PGM	DES
KOREA	JiranSoft	FileSafe v1.0	PC	SW	FILE	PGM	BLOWFISH
KOREA	Penta Security Systems Inc.	ISSAC v. 1.0	ANY	SW	GENERAL	KIT	PROP
KOREA	Senex Technologies Inc. Ltd	Assure Web CA	WIN/NT	SW		PGM	RSA
KOREA	Senex Technologies Inc. Ltd	Assure X-filer for WorkGroup v3.0	WIN	SW	FILE	PGM	BLOWFISH
KOREA	Senex Technologies Inc. Ltd	Assure X-Mailer	WIN	SW	FILE	PGM	BLOWFISH

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

KOREA	SoftForum	XecureDoc 1.0	WIN32	SW	FILE	PGM	RC4
KOREA	SoftForum	XecureMail 2.0	WIN32	SW	EMAIL	PGM	RC4
KOREA	SoftForum	XecureWeb 3.0	WIN	SW	COMMS	PGM	RC4
MEXICO	Seguridata Privada S.A. de C.V.	SeguriDOC	WIN	SW	FILE	PGM	3DES
MEXICO	Seguridata Privada S.A. de C.V.	SeguriEDIFACT	JAVA	SW	EDI	PGM	3DES
MEXICO	Seguridata Privada S.A. de C.V.	SeguriLIB	C CODE	SW	GENERAL	KIT	3DES
MEXICO	Seguridata Privada S.A. de C.V.	SeguriPROXY	WIN32	SW	COMMS	PGM	RC4
MEXICO	Seguridata Privada S.A. de C.V.	SeguriTELNET	WIN32	SW	COMMS	PGM	RC4
MEXICO	The King of Hearts	Potassium Hydroxide (KOH)	DOS	SW	DISK	IDEA	DES
NETHERLANDS	Ad Infinitum Programs (AIP-NL)	UltraCompressor II	PC	SW	FILE	PGM	DES
NETHERLANDS	Alco Blom Software	Web Confidential	MAC	SW	PW	PGM	BLOWFISH
NETHERLANDS	Ascit B.V.	ThunderCrypt	WIN/NT	SW	FILE	PGM	BLOWFISH
NETHERLANDS	Ascit B.V.	ThunderSafe	WIN/NT	SW	FILE	PGM	BLOWFISH
NETHERLANDS	Concord Eracom Nederland BV	DEA Crypto Toolkit	PC	SW	GENERAL	KIT	DES
NETHERLANDS	Concord Eracom Nederland BV	Multi-Functional PC Security (MFPS) Card	PC	HW	GENERAL	BOARD	DES
NETHERLANDS	Concord Eracom Nederland BV	SCORE	PC	SW	GENERAL	KIT	DES
NETHERLANDS	Concord Eracom Nederland BV	SECNET (FCM)	PC	SW/HW	DISK	DES	DES
NETHERLANDS	Concord Eracom Nederland BV	SECNET (HCM)	PC	HW	DISK	BOARD	DES
NETHERLANDS	Concord Eracom Nederland BV	SECNET (SCM)	PC	SW	DISK	PGM	DES
NETHERLANDS	Concord Eracom Nederland BV	SECNET FBI-Encryptor	PC	HW	GENERAL	BOARD	DES
NETHERLANDS	Concord Eracom Nederland BV	SECNET MFPS	PC	SW/HW	COMMS	PGM	DES
NETHERLANDS	Concord Eracom Nederland BV	SECNET PC SoftLock 4.5	PC	SW	DISK	PGM	DES
NETHERLANDS	DigiCash	Electronic cash systems					
NETHERLANDS	DigiCash	Electronic toll payment systems					
NETHERLANDS	DigiCash	Infor Guard i-1200 (The Kryptor)	DOS	SW/HW	GENERAL	PGM	DES
NETHERLANDS	Incaa Datacom BV	AUTHORIZER	RS232	HW	COMMS	BOX	PROP
NETHERLANDS	Philips Crypto B.V.	PFDF 2035 Fax Encryptor	FAX	HW	COMMS	SMART CARD	PROP(high end)
NETHERLANDS	Philips Crypto B.V.	PNVX 2116 Crypto Switch	PBX	HW	COMMS	BOX	DES
NETHERLANDS	Philips Crypto B.V.	PNVX 2118 Secure Telephone	RS232	HW	COMMS	SMART CARD	PROP(high end)
NETHERLANDS	Philips Crypto B.V.	PPSX 2061 Data Encryptor	X.25	HW	COMMS	BOX	DES
NETHERLANDS	Philips Crypto B.V.	Vkaart	WIN/NT	SW/HW	FILE	PCMCIA	DES
NETHERLANDS	Pijnenburg	PCC100 Bulk Data Encryptor Chip	TTL	HW	GENERAL	CHIP	DES
NETHERLANDS	Pijnenburg	PCC100 High Speed DES Chip	TTL	HW	GENERAL	CHIP	DES
NETHERLANDS	Pijnenburg	PCC101	ANY	HW	GENERAL	CHIP	DES
NETHERLANDS	Pijnenburg	PCC200 RSA Chip	TTL	HW	GENERAL	CHIP	RSA
NETHERLANDS	Pijnenburg	PCC201	ANY	HW	GENERAL	CHIP	DES
NETHERLANDS	Tulip Computers BV	Disk Encryption Unit					
NETHERLANDS	Verspeck & Soeters b.v.	Securio	ANY	HW	COMMS	BOARD	DES
NETHERLANDS	Verspeck & Soeters B.V.	Securio I	ANY	HW	COMMS	BOX	DES
NETHERLANDS	Verspeck & Soeters B.V.	Securio II	ANY	HW	COMMS	BOX	DES
NETHERLANDS	Verspeck & Soeters B.V.	Securio III	ANY	HW	COMMS	BOX	DES
NEW ZEALAND	CES Communications Ltd.	Elite2000 XL	TTL	HW	FAX		PROP
NEW ZEALAND	CES Communications Ltd.	Elite2000 XT	TTL	HW	VOICE	PHONE	PROP
NEW ZEALAND	CES Communications Ltd.	Fax Guardian	TTL	HW	FAX		PROP
NEW ZEALAND	CES Communications Ltd.	Phone Guardian	TTL	HW	VOICE		PROP
NEW ZEALAND	John Gilmore	Free S/WAN 1.00	LINUX	SW	COMMS	PGM	3DES
NEW ZEALAND	LUC Encryption Technology, Ltd. (LUCENT)	LCP Library	ANY	SW	GENERAL	KIT	LUC
NEW ZEALAND	LUC Encryption Technology, Ltd. (LUCENT)	sifr	PC	SW	FILE	PGM	LUC
NEW ZEALAND	Peter Gutmann	Cryptlib		SW	GENERAL	KIT	<SEE NOTES>
NEW ZEALAND	Peter Gutmann	HPACK Archiver 0.79	PC	SW	FILE	PGM	MDC
NEW ZEALAND	Peter Gutmann	Secure File System (SFS) 1.1	PC	SW	DISK	PGM	MDC
NEW ZEALAND	RPK New Zealand	Invisimail Professional	WIN95	SW	EMAIL	PGM	RPK
NEW ZEALAND	RPK New Zealand	RPK File 1.01	WIN	SW	FILE	PGM	RPK
NEW ZEALAND	RPK New Zealand	RPK Public Key Cryptosystem	UNIX	SW	GENERAL	KIT	RPK
NEW ZEALAND	RPK New Zealand	TRPKC	WIN	SW	GENERAL	KIT	RPK
NEW ZEALAND	RPK New Zealand Ltd	RPK Encryptonite Software Toolkit V3.1	C++ CODE	SW	GENERAL	KIT	RPK
NEW ZEALAND	RPK New Zealand Ltd	RPK SecureMedia V1.0	WIN/NT	SW	MEDIA	PGM	RPK
NORWAY	Alladin Software	??					
NORWAY	Columbi Micro a.s.	??					
NORWAY	Ericsson Semafor	??					
NORWAY	InfoMedica AS	??					
NORWAY	Informasjonskontroll A/S	??					
NORWAY	Informatikk A/S	??					
NORWAY	Kirkedam Elektronikk EDB	??					
NORWAY	Notis A.S.	??					
NORWAY	Scand PC Sys/Sectra	??					
NORWAY	Siemens Nixdorf, Informationssystemer A/S	??					
NORWAY	Sterling Software Scandinavia A/S	??					
NORWAY	Telepartner as	??					
NORWAY	Voicetech A.S.	??					
POLAND	Enigma Information Security Systems	PEM - HEART	PC	SW	EMAIL	PGM	DES
ROMANIA	Interscope s.r.l.	Interscope Blackbox	WIN/NT	SW	FILE	PGM	DES
RUSSIA	Ancort	Ancrypt	HW	SW	GENERAL	BOX	PROP
RUSSIA	Ancort	Cryptocenter Version 1.5	PC	SW	FILE	PGM	PROP
RUSSIA	Ancort	CryptoGrapher	WIN/CE	SW	GENERAL	PGM	PROP
RUSSIA	Ancort	Cyberdog	WIN95	SW	FILE	PGM	PROP
RUSSIA	Ancort	File Cipher	WIN95	SW	FILE	PGM	PROP
RUSSIA	Askri	Cryptos	PC	SW	FILE	PGM	DES
RUSSIA	Elias Ltd.	Excellence for DOS	PC	SW	FILE	PGM	GOST
RUSSIA	INFORM - RTG	Absolute Cryptographer	ANY	SW	GENERAL	PGM	PROP
RUSSIA	LAN Crypto	CRYPTOBANK (NOTARY & VESTA utilities)	UNIX	SW	DISK	KIT	DES
RUSSIA	LAN Crypto	DIANA	WK	SW	LAN	KIT	DES
RUSSIA	LAN Crypto	Ortis	DOS	SW	FILE	KIT	DES

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

RUSSIA	LAN Crypto	Sphinx	PC	SW	DISK	PGM	
RUSSIA	LAN Crypto	VESTA	UNIX	SW	DISK	KIT	DES
RUSSIA	RESCrypto	??					
RUSSIA	ScanTech	Krypton		HW		BOARD	GOST
RUSSIA	TELECRYPT, Ltd.	TELECRYPT	PC	SW	FILE	PGM	DES
SOUTH AFRICA	Citadel Data Security	Citadel Firewall	UNIX	SW	VPN	PGM	DES
SOUTH AFRICA	Computer Security Associates	??					
SOUTH AFRICA	Denel Informatics	IWATCH	PC	SW	COMMS	PGM	DES
SOUTH AFRICA	EFT	??		HW		BOARD	DES
SOUTH AFRICA	Intelligent	??					
SOUTH AFRICA	Nanoteq	??		HW	COMMS	BOX	
SOUTH AFRICA	Net One	??					
SOUTH AFRICA	NetSec	Application Gateway	PC	SW	COMMS	PGM	DES
SOUTH AFRICA	NetSec	NetSec Manager		SW		PGM	DES
SOUTH AFRICA	NetSec	Secure Router		SW	COMMS	KIT	DES
SOUTH AFRICA	Sentera	N3000M		HW			
SOUTH AFRICA	Siemens Ltd. So. Africa -Pretoria	??					
SOUTH AFRICA	Spescom	??					
SOUTH AFRICA	Thawte Consulting	Thawte Personal Certificate	MANY	SW	S/MIME		IDEA
SOUTH AFRICA	Thawte Consulting	Thawte SSL Server Certificate	MANY	SW	S/MIME		DES
SPAIN	SECARTYS	??					
SWEDEN	Ardy Elektronics	SLD/OUS-200	RS232	HW	COMMS	BOX	PROP(ARD Y)
SWEDEN	Ardy Elektronics	SLF 2000	telephone	HW	FAX		PROP(ARD Y)
SWEDEN	Ardy Elektronics	SLP 2000	telephone	HW	VOICE		PROP(ARD Y)
SWEDEN	AU-System Communication AB	Avi - Boks	PC	SW/HW	COMMS	PGM	DES
SWEDEN	AV System Infocard	??	PC	SW/HW	DISK	KIT	RSA
SWEDEN	Business Security AB	Secureifile	PCMCIA	HW	FILE	SMART CARD	PROP(SBLH -E)
SWEDEN	Business Security AB	SecuriCrypto G.703/704		HW	COMMS	BOX	PROP
SWEDEN	Business Security AB	SecuriCrypto V.24 S	V.24	HW	COMMS	BOX	PROP(STRE AM)
SWEDEN	Business Security AB	SecuriCrypto V.24A (Asynchronous)	V.24	HW	COMMS	BOX	PROP(STRE AM)
SWEDEN	Business Security AB	SecuriCrypto V.24S / V.24SR (Synchronous)	V.24	HW	COMMS	BOX	PROP(STRE AM)
SWEDEN	Business Security AB	SecuriCrypto V.35 / V.35R	V.35	HW	COMMS	BOX	PROP
SWEDEN	Business Security AB	SecuriCrypto V.36	V.36	HW	COMMS	BOX	PROP(STRE AM)
SWEDEN	Business Security AB	SecuriCrypto X.21, Datex	X.27	HW	COMMS	BOX	PROP(STRE AM)
SWEDEN	Business Security AB	SecuriCrypto X.25	X.21bis	HW	COMMS	BOX	PROP(STRE AM)
SWEDEN	Business Security AB	SecuriCrypto X.28	V.24	HW	COMMS	BOX	PROP
SWEDEN	Business Security AB	SecuriFax		HW	FAX	FAX	PROP(STRE AM)
SWEDEN	Business Security AB	SecuriModem	V.34	HW	COMMS	MODEM	PROP(SBLH -E)
SWEDEN	Business Security AB	SecuriVideo	V.35	HW	VIDEO	BOX	PROP(SBLH -E)
SWEDEN	Business Security AB	SecuriVoice	telephone	HW	VOICE	SMART CARD	PROP(STRE AM)
SWEDEN	COST Computer Security Technologies International	COST SCS	PC	SW/HW	GENERAL	TOKEN	DES
SWEDEN	COST Computer Security Technologies International	COST-EDI	PC	SW	COMMS		DES
SWEDEN	COST Computer Security Technologies International	COST-EKS	PC	SW	FILE		DES
SWEDEN	COST Computer Security Technologies International	COST-PEM	PC	SW	EMAIL	PGM	DES
SWEDEN	COST Computer Security Technologies International	Generalized Security Library (GSL)	PC	SW	GENERAL	PGM	DES
SWEDEN	DynaSoft	Avi-BoKs	PC	SW/HW	FILE	PGM	DES
SWEDEN	DynaSoft	BoKS 4.2	UNIX	SW/HW	COMMS	PGM	DES
SWEDEN	DynaSoft	Boks Connect	UNIX	SW	COMMS	PGM	RSA
SWEDEN	DynaSoft	Boks Desktop	WIN	SW	FILE	PGM	
SWEDEN	Henry Padilla	GHOST File Manager v. 3.0	WIN95	SW	FILE	PGM	DES
SWEDEN	SECTRA AB	FKK 930 - G.703/G.704/G.751		HW		BOX	KM3
SWEDEN	SECTRA AB	KK 621 - ISA		HW		BOARD	KM3
SWEDEN	SECTRA AB	KK 621 - PCCARD		HW		PCMCIA	DES
SWEDEN	SECTRA AB	KM3		HW		CHIP	KM3
SWEDEN	SECTRA AB	KryptoLan KLB 1002		HW		BOX	DES
SWEDEN	SECTRA AB	KryptoLan KLB 2020 - V. 35/ IP		HW		BOX	KM3
SWEDEN	SECTRA AB	KryptoLan KLS 1001		HW		BOX	DES
SWEDEN	SONNOR Crypto AB	HR&S	ANY	SW	COMMS	PGM	PROP(HR&S)
SWEDEN	SONNOR Crypto AB	PCrypt	ANY	SW	FILE	PGM	PROP(HR&S)
SWEDEN	Stig Ostholm	DES Implementation 2.2	ANY	SW	GENERAL	PGM	DES
SWITZERLAND	ASCOM Tech AG	IDEA Toolkit	ANY	SW	GENERAL	KIT	IDEA
SWITZERLAND	ASCOM Tech AG	VINCI	TTL	HW	GENERAL	CHIP	IDEA
SWITZERLAND	Brown-Boveri	??					
SWITZERLAND	Crypto AG	CRYPTOCOM HC-265	RADIO	HW	VOICE	BOX	
SWITZERLAND	Crypto AG	CRYPTOMATIC HC-5700 / 5750		SW/HW	COMMS	KIT	
SWITZERLAND	Crypto AG	CRYPTOVOX HC-3300	telephone	HW	VOICE	PHONE	
SWITZERLAND	Crypto AG	CSE-160 Secure Handheld Radio	RADIO	HW	VOICE	RADIO	
SWITZERLAND	Crypto AG	CSE-660 Secure Mobile Radio	RADIO	HW	VOICE	BOX	
SWITZERLAND	Crypto AG	HC-2203 PSTN Voice Encryption	TELEPHONE	HW	VOICE	BOX	
SWITZERLAND	Crypto AG	HC-2403 Secure GSM	CELL PHONE	HW	VOICE	PHONE	
SWITZERLAND	Crypto AG	HC-3460 Radio Voice Encryption	RADIO	HW	VOICE	BOARD	
SWITZERLAND	Crypto AG	HC-4220 Facsimile Encryption	FAX	HW	FAX	BOX	

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

SWITZERLAND	Crypto AG	HC-5250 Secure Hand-Held Terminal	PHONE	HW	COMMS	TERMINAL		
SWITZERLAND	Crypto AG	HC-5500 Secure Email		SW/HW	EMAIL			
SWITZERLAND	Crypto AG	HC-5700 Secure Emmission Protected Terminal	TELEPHONE	HW	COMMS	TERMINAL		
SWITZERLAND	Crypto AG	HC-6830 Secure Field Communication Terminal	PHONE	HW	COMMS	TERMINAL		
SWITZERLAND	Crypto AG	HC-6950 Secure Emmission Protected WorkStation	PC	HW	DISK	PC		
SWITZERLAND	Crypto AG	HC-6950 Secure WorkStation System	WIN	SW/HW	DISK	PC		
SWITZERLAND	Crypto AG	HC-7210/7220 Secure Modem		HW	COMMS	MODEM		
SWITZERLAND	Crypto AG	HC-7305/7310 ISDN Encryption		HW	COMMS	BOX		
SWITZERLAND	Crypto AG	HC-7500 Link Encryptor	V.24	HW	COMMS	BOX		
SWITZERLAND	Crypto AG	HC-7550 Multi-Link Bulk Encryptor	EUROCOM D/1	HW	COMMS	BOX		
SWITZERLAND	Crypto AG	HC-7820 VPN Encryption	ENET	HW	VPN	BOX		PROP
SWITZERLAND	Crypto AG	HC-7830 VPN Encryption	WIN/NT	HW	VPN	PCMCIA		PROP
SWITZERLAND	Crypto AG	HC-7910 ATM Encryption	ENET	HW	ATM	BOX		
SWITZERLAND	Crypto AG	KHC-1500 Key Handling Center	WIN	HW	DISK	PC		
SWITZERLAND	Crypto AG	SECOS 400/610 Secure VHF/UHF Frequency Hopping System	RADIO	HW	VOICE	BOX		
SWITZERLAND	Crypto AG	TFP-3400 Digital Telephony Gateway		HW	VOICE	BOX		
SWITZERLAND	ETH Zurich	ENskip	UNIX	SW	IPSEC	PGM		DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 522	RS232	HW	COMMS	BOX		DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 524	RS232	HW	COMMS	BOX		DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 526	X.21	HW	COMMS	BOX		DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 545	RS232	HW	COMMS	BOX		DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 549	X.25	SW/HW	COMMS	PGM		DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 605	V.35	HW	COMMS	BOX		DES
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 705 Authenticator	RS232	HW	GENERAL	BOX		RSA
SWITZERLAND	Gretacoder Data Systems AG	Gretacoder 710 Authenticator	X.25	HW	GENERAL	BOX		DES
SWITZERLAND	Lightning Instrumentation SA	Multicom Software Release 2.1		SW	COMMS	PGM		IDEA
SWITZERLAND	Omnisec AG	Omniscard	WIN95	SW/HW	FILE	PGM		
SWITZERLAND	Omnisec AG	Omnisec 212 - Secure Telephone for PSTN	TELEPHONE	HW	VOICE	PHONE		
SWITZERLAND	Omnisec AG	Omnisec 212 A2 - Secure Telephone for PSTN Server Version	TELEPHONE	HW	VOICE	PHONE		
SWITZERLAND	Omnisec AG	Omnisec 213 - Secure Telephone for ISDN	TELEPHONE	HW	VOICE	PHONE		
SWITZERLAND	Omnisec AG	Omnisec 510	PC	HW	COMMS	BOX		PROP
SWITZERLAND	Omnisec AG	Omnisec 520 - Facsimile Encryptor	FAX	HW	FAX	FAX		
SWITZERLAND	Omnisec AG	Omnisec 545 - X.25 Data Encryptor	V.24	HW	COMMS	BOX		PROP
SWITZERLAND	Omnisec AG	Omnisec 610	RS232	HW	COMMS	BOX		PROP
SWITZERLAND	Omnisec AG	Omnisec 620	RS232	HW	COMMS	BOX		PROP
SWITZERLAND	Omnisec AG	Omnisec 621 - Field Wire Encryptor	EUROCOM D/1	HW	COMMS	BOX		
SWITZERLAND	Omnisec AG	Omnisec 630	RS449	HW	COMMS	BOX		PROP
SWITZERLAND	Omnisec AG	Omnisec 640	V.10	HW	COMMS	BOX		PROP
SWITZERLAND	Omnisec AG	Omnisec 644 - Multi-Link Encryption System		HW	COMMS	BOX		
SWITZERLAND	Omnisec AG	Omnisec 650 - High-Speed Link Encryptor	ETHERNET	HW	COMMS	BOX		
SWITZERLAND	Omnisec AG	Omnisec 670 - Encrypting Modem	V.17	HW	COMMS	MODEM		
SWITZERLAND	Omnisec AG	Omnisec 910 - Secure Message Field Terminal	RADIO	HW	COMMS	TERMINAL		
SWITZERLAND	Organa	mProtect						
SWITZERLAND	Safeware AG	SAFE-BOARD	ISA	HW	COMMS	BOARD		DES
SWITZERLAND	Safeware AG	SAFE-DISK	DOS	SW/HW	DISK	PGM		DES
SWITZERLAND	Safeware AG	SAFE-FILE	DOS	SW/HW	FILE	PGM		DES
SWITZERLAND	Thessen Security Systems Ltd.	Thss-PC	OS2	SW	FILE	PGM		DES
TURKEY	ASELSAN Inc.	2010 Data Crypto Equipment	V.10	HW	COMMS	BOX		PROP
TURKEY	ASELSAN Inc.	2020 Packet Crypto Equipment	X.25	HW	COMMS	BOX		PROP
TURKEY	ASELSAN Inc.	2025 Network Management system	X.25	SW/HW	COMMS	PC		PROP
TURKEY	ASELSAN Inc.	2101 Integrated Voice and Data Encryptor	RJ-11	HW	COMMS	BOX		
UK	Adam Back	Export-a-Crypto-System sig	UNIX	SW	GENERAL	PGM		RSA
UK	Andrew Brown	Wincredll	WIN	SW	GENERAL	PGM		DES
UK	Apricot Computers, Ltd.	APRICOT SECURITY SYSTEM, Release 5	PC	SW/HW	DISK	<See Notes>		
UK	Avant Guardian Ltd.	Proscriptor Security System	V.32	SW/HW	COMMS	BOX		Avant Guardian
UK	Baltimore Technologies plc.	C/SSL	SOLARIS	SW	SSL	KIT		DES
UK	Baltimore Technologies plc.	CG5000	ETHERNET	HW	COMMS	BOX		DES
UK	Baltimore Technologies plc.	Crypto Systems ToolKit v6.0	ANY	SW	COMMS	KIT		DES
UK	Baltimore Technologies plc.	ECS DeskTop	WIN/NT	SW	FILE	PGM		DES
UK	Baltimore Technologies plc.	ECS Server		SW		PGM		DES
UK	Baltimore Technologies plc.	ED2048R3 Rambutan	X.21	HW	COMMS	BOX		RAMBUTAN
UK	Baltimore Technologies plc.	ED8000RL	ETHERNET	HW	COMMS	BOX		RAMBUTAN
UK	Baltimore Technologies plc.	FileSecure 4.0		SW	FILE	PGM		DES
UK	Baltimore Technologies plc.	FormSecure 4.0		SW	COMMS	PGM		DES
UK	Baltimore Technologies plc.	HSP4000-Assure	WIN/NT	SW/HW	GENERAL	KIT		DES
UK	Baltimore Technologies plc.	J/Crypto 3.3	<SEE NOTES>	SW	GENERAL	KIT		DES
UK	Baltimore Technologies plc.	J/SSL	JAVA	SW	SSL	KIT		DES
UK	Baltimore Technologies plc.	MailSecure	<SEE NOTES>	SW	S/MIME	PGM		3DES
UK	Baltimore Technologies plc.	MailSecure Enterprise		SW	EMAIL	PGM		3DES
UK	Baltimore Technologies plc.	PKI-Plus SDK	ANY	SW	GENERAL	KIT		DES
UK	Baltimore Technologies plc.	WebSecure	<SEE NOTES>	SW	COMMS	PGM		
UK	Ben Laurie	Apache SSL		SW	COMMS	KIT		DES
UK	British Telecom	BT Lektor 3620 PC Secure v 3.02	PC	SW	FILE	PGM		PROP(B-CRYPT)
UK	British Telecom	BT Lektor 3620 PC Secure v1.1	PC	SW	FILE	PGM		RAMBUTAN
UK	British Telecom	RSA chip	TTL	HW	GENERAL	CHIP		RSA
UK	Business Simulations	Ultralock						

**GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS**

UK	Cambridge Electric Industries	??						
UK	Codepoint Systems Ltd.	??						
UK	Computer Security Ltd.	Safe Guard Systems						
UK	Data Innovation Ltd.	CG500	V.24	HW	COMMS	BOX	DES	
UK	Data Innovation Ltd.	ED2048	G703	HW	VOICE	BOX	DES	
UK	Data Innovation Ltd.	ED500	V.24	HW	COMMS	BOX	DES	
UK	Data Innovation Ltd.	ED600	V.24	HW	COMMS	BOX	PROP	
UK	Data Innovation Ltd.	ED600R		HW	COMMS	BOX	RAMBUTAN	
UK	Data Innovation Ltd.	Network Security Workstation (NSW)	PC	SW/HW	KEYS		DES	
UK	Data Innovation Ltd.	PSP400	PC	HW	GENERAL	BOARD	DES	
UK	DataSoft International Ltd.	DataCode		SW	GENERAL	KIT	BAZARIES	
UK	DataSoft International Ltd.	DataTalk		SW	COMMS	PGM	BAZARIES	
UK	Digital Crypto	Iris	DOS	SW	DISK	PGM	DES	
UK	Digital Crypto	OS2-IRIS	OS2	SW	FILE	PGM	DES	
UK	Digital Crypto	PC-IRIS V4.0 - 2	PC	SW	FILE	PGM	DES	
UK	Digital Crypto	PC-MERLIN V2.0 - 1	PC	SW	FILE	PGM	DES	
UK	Digital Crypto	VMS-IRIS	VMS	SW	FILE	PGM	DES	
UK	Emergent Technologies, Ltd.	Eurokey Personal Edition	WIN/NT	SW	FILE	PGM	IDEA	
UK	Emergent Technologies, Ltd.	Eurokey Professional Edition	WIN/NT	SW	FILE	PGM	IDEA	
UK	Ewen Associates Limited	Cryptix Security Toolkit	ANY	SW	GENERAL	KIT	DES	
UK	Ewen Associates Limited	SimpliCrypt for Windows	WIN/NT	SW	FILE	PGM	DES	
UK	Fauzan Mirza	IDEA86	PC	SW	GENERAL	PGM	IDEA	
UK	Finansa	Winmail		SW	EMAIL		LUCIFER	
UK	Fulcrum Communications	??						
UK	GEC-Marconi Secure Systems	DATALOK H	ANY	HW	COMMS	BOX	PROP	
UK	GEC-Marconi Secure Systems	DATALOK L	ANY	HW	COMMS	BOX	PROP	
UK	GEC-Marconi Secure Systems	FAXLOK	ANY	HW	FAX	BOX	PROP	
UK	GEC-Marconi Secure Systems	IC-H10SR	RADIO	HW	VOICE	BOX	PROP	
UK	GEC-Marconi Secure Systems	IC-RP1510SR	RADIO	HW	VOICE	BOX	PROP	
UK	GEC-Marconi Secure Systems	IC-V200SR	RADIO	HW	VOICE	BOX	PROP	
UK	GEC-Marconi Secure Systems	Marcrypt		HW		CHIP	PROP(MAR	
UK	GEC-Marconi Secure Systems	MASC Crypto Management System	PC	SW/HW	COMMS	BOX	CRYPT)	
UK	GEC-Marconi Secure Systems	MASC Module	RADIO	HW	VOICE	ADAPTOR	PROP	
UK	GEC-Marconi Secure Systems	SDT-100	telephone	HW	VOICE	BOX	PROP	
UK	Gelosia	??						
UK	Global CIS Ltd.	Safeguard Security System	PC	SW	FILE	PGM	PROP	
UK	Honeywell	??						
UK	ICL Secure Systems	TEAMcrypto		SW			FEAL8	
UK	InfoShare	Omnicdata	PC	SW	GENERAL	PGM		
UK	Instant Access	Digital Vault	MAC	SW	FILE	PGM		
UK	Interconnections	??						
UK	International Data Security, Ltd.	DataSave-ABA						
UK	International Data Security, Ltd.	Protec Net V4.1	DOS	SW	COMMS	PGM		
UK	International Data Security, Ltd.	Protec V4.1	DOS	SW	FILE	PGM		
UK	IQ International	Stealth		SW			PROP(HMX	
UK	IT Security International	Secure LAN					+))	
UK	ITV	??						
UK	J.R.Ward Computers Ltd.	Code-It	PC	SW	FILE	PGM	PROP	
UK	J.S.A. Kapp	RSAEURO 1.04 (Internet)	ANY	SW	GENERAL	KIT	DES	
UK	J.S.A. Kapp	RSAEURO 1.10 (Commercial)	ANY	SW	GENERAL	KIT	DES	
UK	Jaguar Communications Ltd.	ZCODA-A	RS232	HW	COMMS	BOX	PROP	
UK	Jaguar Communications Ltd.	ZCODA-X	RS232	HW	COMMS	BOX	PROP	
UK	Janus Sovereign	Padlock						
UK	JCP Computer Services	Crypto v2.0	JAVA	SW	GENERAL	KIT	DES	
UK	JPY Associates Ltd.	DataLock, Version 4.0	MF	SW	DISK	PGM	DES	
UK	Loadplan	??						
UK	Logica	??						
UK	Microft Technology Ltd.	CLAM	PC	SW	FILE	PGM	PROP	
UK	NEST Ltd.	CaGey Bee	WIN					
UK	Network Systems Corporation (UK)	Data Delivery/Management System						
UK	Novell, Ltd. (UK)	Trusted Netware 4		SW	COMMS	KIT		
UK	PC Security Ltd.	CP8-AuthentICC	PC	HW	FILE	SMART CARD	PROP	
UK	PC Security Ltd.	LapGUARD	PC	SW	FILE	PGM	PROP	
UK	PC Security Ltd.	Stoplock 95	WIN95	SW	DISK	PGM	PROP	
UK	PC Security Ltd.	Stoplock III	PC	SW	DISK	PGM	PROP	
UK	PC Security Ltd.	Stoplock IVE	PC	SW/HW	DISK	PGM	DES	
UK	PC Security Ltd.	Stoplock KE	PC	SW	DISK	PGM	PROP	
UK	PC Security Ltd.	Stoplock V	PC	SW	DISK	PGM	PROP	
UK	PC Security Ltd.	Stoplock V/SC	PC	SW/HW	DISK	SMART CARD	PROP	
UK	Plessy Crypto	RSA chip	HW			CHIP	RSA	
UK	Plus 5 Engineering Ltd.	Policeman	PC	SW	DISK	PGM	PROP	
UK	Portcullis Computer Security Ltd.	Cryptix Toolkit		SW	GENERAL	KIT	DES	
UK	Portcullis Computer Security Ltd.	Easycrypt		SW			DES	
UK	Portcullis Computer Security Ltd.	TRISPAN V.12130	DOS	SW/HW	FILE	<See Notes>		
UK	Protection Systems Ltd.	Disk Certification	PC	SW	DISK	PGM	PROP	
UK	Protection Systems Ltd.	Guardian Angel LAN	PC	SW	FILE	PGM	PROP	
UK	Protection Systems Ltd.	Guardian Angel Plus	PC	SW	FILE	PGM	PROP	
UK	Protection Systems Ltd.	Guardian Angel Plus LAN	PC	SW	FILE	PGM	PROP	
UK	Racal Airtech Ltd.	Datacryptor 64	RS232	HW	COMMS	BOX	DES	
UK	Racal Airtech Ltd.	Datacryptor 64E	X.25	HW	COMMS	BOX	DES	
UK	Racal Airtech Ltd.	Datacryptor 64F	RS232	HW	COMMS	BOX	DES	
UK	Racal Airtech Ltd.	Datacryptor 64HS	G.703	HW	COMMS	BOX	DES	
UK	Racal Airtech Ltd.	Datacryptor 64HSF	RS232	HW	COMMS	BOX	DES	
UK	Racal Airtech Ltd.	Datacryptor 64MS	RS232	HW	COMMS	BOX	DES	
UK	Racal Airtech Ltd.	Datacryptor&trade 2000	RS232	HW	COMMS	BOX	DES	
UK	Racal Airtech Ltd.	RG721 PC Security Module	DOS	SW/HW	GENERAL	ISA	DES	
UK	Racal Airtech Ltd.	Safe 64K Link Encryptor	RS232	HW	COMMS	BOX	DES	
UK	Racal Airtech Ltd.	Safe Megabit 2 Encryptor		HW	COMMS	BOX	DES	
UK	Racal Airtech Ltd.	Safe X.25	WIN	HW	COMMS	BOX	DES	
UK	Racal Airtech Ltd.	WatchWorld II Token		HW	PIN	TOKEN	DES	

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

UK	Racal Airtech Ltd.	WatchWorld Soft Token	Win	HW	PIN	DISK	DES
UK	Racal Airtech Ltd.	WebSentry Ethernet (WS-ES)	DOS	SW/HW	SSL	BOX	DES
UK	Radius	??					
UK	Reflex Magnetics Ltd.	Reflex Disknet		HW			
UK	S&S International PLC	Dr. Solomon's Ringfence II	PC	SW	DISK	PGM	PROP
UK	S&S International PLC	SAVEDIR	PC	SW	FILE	PGM	PROP
UK	Securicor 3net Ltd.	Secure IQ ENCO		HW	COMMS		DES
UK	Sington Associates	??					
UK	Smith's Associates	??					
UK	Soft Concepts	Ncrypt	WIN	SW	FILE	PGM	PROP
UK	Softdiskette	??					
UK	Sophos Ltd.	D-Fence 4 HMG	PC	SW	DISK	PGM	HMG
UK	Sophos Ltd.	D-Fence 4 SPA	PC	SW	DISK	PGM	PROP
UK	Sophos Ltd.	E-DES	DOS	SW	FILE	PGM	DES
UK	Sophos Ltd.	PUBLIC	pc	SW	COMMS	PGM	DES
UK	Stralfors Data	PS3					
UK	Sygnus Data Communications	??					
UK	Time & Data Systems	Microstop					
UK	Tricom	??					
UK	University College London	OSISEC Version 2.3		SW	GENERAL	PGM	DES
UK	University College London	UCL-PEM		SW	EMAIL	PGM	DES
UK	Widney Ash	??					
UK	Zeta Communications Ltd.	Zetacoda A	RS232	HW	COMMS	BOX	PROP
UK	Zeta Communications Ltd.	Zetacoda X	RS232	HW	COMMS	BOX	PROP

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

C. FOREIGN ENCRYPTION MANUFACTURERS AND DISTRIBUTORS BY COUNTRY

The following table is a summary listing of the foreign companies that manufacture or distribute cryptographic products.

COUNTRY	COMPANY
ARGENTINA	Data Crypt S.A.
ARGENTINA	Newnet S.A.
AUSTRALIA	Andrei Souleimanian
AUSTRALIA	Banksia Technology Pty. Ltd.
AUSTRALIA	Carbon Based Software
AUSTRALIA	Cipher Research Laboratories
AUSTRALIA	Cryptsoft Pty Ltd.
AUSTRALIA	Cybanim Pty Ltd.
AUSTRALIA	DataCrypt
AUSTRALIA	Datamatic Pty. Ltd.
AUSTRALIA	Eracom Pty Ltd.
AUSTRALIA	Eric Young
AUSTRALIA	Loadplan Australasia Pty Ltd.
AUSTRALIA	LUCENT
AUSTRALIA	Matthew Kwan
AUSTRALIA	Microlock
AUSTRALIA	Microsoft Pty.
AUSTRALIA	Mosaic Industries
AUSTRALIA	NetSafe
AUSTRALIA	News Datacom
AUSTRALIA	NexSol
AUSTRALIA	Nick Payne
AUSTRALIA	Robust Software
AUSTRALIA	Ross Williams
AUSTRALIA	RSA Data Security Australia
AUSTRALIA	Secure Network Solutions
AUSTRALIA	Security Domain Pty Ltd
AUSTRALIA	TRAC Systems
AUSTRALIA	Tracom
AUSTRIA	Eshelbeck, Steiner, Beitelmaier
AUSTRIA	IAIK, TU Graz
AUSTRIA	Mils Elektronik
AUSTRIA	Siemens AG Austria
AUSTRIA	University of Linz
BAHRAIN	International Information Systems
BALTIC REPUBLICS	LAN Vision
BANGLADESH	Quantum System Software
BELGIUM	ClassicSys
BELGIUM	CNET
BELGIUM	Cryptech NV/SA
BELGIUM	Data Alert International Elfhoven BV
BELGIUM	GSA Ran Data Europe
BELGIUM	Highware, Inc.
BELGIUM	Lintel Security
BELGIUM	Open Software Foundation / Europe
BELGIUM	UTI-MACO Belgium
BELGIUM	Vector
BRAZIL	PC Software e Consultoria Ltda
BRUNEI	Digitus Computer Systems
CANADA	A.B. Data Sales, Inc.
CANADA	Adam Berent
CANADA	Atlantic Systems Group (ASG)
CANADA	Authentex/NovaStor
CANADA	Certicom
CANADA	Chrysalis ITS
CANADA	Compression Technologies, Inc.
CANADA	Computer Security Corporation
CANADA	CRYPTOCARD Corporation
CANADA	Cycomm International, Inc.
CANADA	Earthworks Communications
CANADA	Entrust Technologies
CANADA	Freestyle Software, Inc.
CANADA	Gandalf
CANADA	Ilex Systems Inc.
CANADA	Inforon Technologies, Inc.
CANADA	Isolation Systems
CANADA	Jaws Technologies, Inc
CANADA	Kyberpass Corporation
CANADA	Micro Tempus, Inc.
CANADA	Microsoft Canada, Inc.
CANADA	Milkyway Networks Corporation
CANADA	MPR Teltech
CANADA	NetComServ Canada
CANADA	Newbridge Networks Corp.
CANADA	Nortel Secure Networks
CANADA	Northern Telecom Canada Ltd. (Data Comm. Products)
CANADA	Northern Telecom Canada Ltd. (Secure Networks)

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

CANADA	Octothorp Industries
CANADA	Okiock Data
CANADA	Ontrack Computer Systems, Inc.
CANADA	Paradyne Canada Ltd.
CANADA	Queen's University
CANADA	RAYBORG TECHNOLOGIES INC.
CANADA	Scientific Atlantic
CANADA	Secured Communications Inc. (SCI)
CANADA	Sierra Wireless
CANADA	Silanis Technology
CANADA	Symantec, Canada
CANADA	The Enigma Group
CANADA	TimeStep Corporation
CANADA	Tundra Semiconductor Corp.
CANADA	Xcert International Inc.
CANADA	Zoomit Corporation
CHILE	Bysupport Computacion SA
COLUMBIA	Economic Data sl
CYPRUS	A E C Consultants Ltd
CZECH REPUBLIC	Alwil Software
CZECH REPUBLIC	Decros spol. s r.o.
CZECH REPUBLIC	PCS spol sro
DENMARK	Aarhus University, Computer Science Department
DENMARK	CryptoMathic A/S
DENMARK	GN Datacom
DENMARK	Intelitech Omniware
DENMARK	Iversen & Martens A/S
DENMARK	Kommunedata
DENMARK	LSI Logic/Dataco AS
DENMARK	Swanholm Computing A/S
DENMARK	Swanholm Distribution A/S
DENMARK	Telesec
ESTONIA	Cybernetica
FINLAND	Antti Louko
FINLAND	Ascom Fintel OY
FINLAND	Datafellows Ltd.
FINLAND	Instrumentoiti OY
FINLAND	Jetico, Inc.
FINLAND	LAN Vision OY
FINLAND	SSH Communications Security
FINLAND	SSH Communications Security
FRANCE	AB Soft
FRANCE	ActivCard
FRANCE	Aladdin France SA
FRANCE	Atlantis
FRANCE	Bull Worldwide Information Systems Inc.
FRANCE	CCETT
FRANCE	Cryptech France
FRANCE	Crypto-Box Sarl
FRANCE	CSEE - Division Communication et Informatique
FRANCE	CSIL
FRANCE	Dassault Automatismes et Telecommunications
FRANCE	Digital Equipment Corp. (DEC), Paris Research Lab
FRANCE	Herve Schauer Consultants
FRANCE	Hewlett Packard France
FRANCE	Incaa France S.A.R.L.
FRANCE	LAAS
FRANCE	Netscape Communications CNIT
FRANCE	Philips Communication Systems
FRANCE	Premenos Europa
FRANCE	Rast Electronics
FRANCE	Research Institute
FRANCE	S.A. Gretag
FRANCE	SAGEM
GERMANY	Andreas Kupries
GERMANY	Andreas Muller Software
GERMANY	AR Datensicherungssysteme GmbH
GERMANY	Atlantis GmbH (deutschland)
GERMANY	Baller & Huwig
GERMANY	BioData GmbH
GERMANY	BROKAT Infosystems AG
GERMANY	CCI (Competence Center Informatik GmbH)
GERMANY	CE Infosys GmbH
GERMANY	Cedric Reinartz
GERMANY	Celticon
GERMANY	Christoph Martin
GERMANY	Concord-Eracom Computer GmbH
GERMANY	Controlware GmbH
GERMANY	CryptoSoft GmbH
GERMANY	CryptoSoft GmbH
GERMANY	DataSafe
GERMANY	DemCom
GERMANY	DTM Data TeleMark GmbH
GERMANY	Dynatech - Gesellschaft fur Datenverarbeitung GmbH
GERMANY	EuroCom EDV
GERMANY	EZI GmbH
GERMANY	FAST ComTec GmbH
GERMANY	GAO
GERMANY	Gliss & Herweg
GERMANY	Glück & Kanja GmbH
GERMANY	GMD
GERMANY	Gretag Elektronik GmbH
GERMANY	Interconnect

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

GERMANY	Jurgen Meyer, Frank Gadegast
GERMANY	Karl Huwig
GERMANY	KryptoKom
GERMANY	Markt & Technik Software Partners Intl. GmbH
GERMANY	MARX Datentechnik GmbH
GERMANY	Mathias Kretschmer
GERMANY	Paradyne GmbH
GERMANY	Roland Mundloch
GERMANY	S&S International Deutschland GmbH
GERMANY	Siemens Vertrauliche Kommunikation
GERMANY	Siemens-Nixdorf
GERMANY	SIT
GERMANY	T. Billenstein
GERMANY	Tela Versicherung
GERMANY	Tele Security Timmann GmbH & Co.
GERMANY	Telenet Kommunikation Systeme
GERMANY	The Compatibility Box GmbH
GERMANY	Toshiba Europe GmbH
GERMANY	Utimaco Safeware AG
GERMANY	Wilhelm Heibl Werke
GHANA	Software Marketing Consultancy
GREECE	A E C Consultancy
GREECE	G.J.Messaritis & Co. Ltd.
GREECE	John Ioannidis
GREECE	ORCO Ltd.
HONG KONG	Digitus Computer Systems
HONG KONG	Microsoft Hong Kong, Ltd.
HONG KONG	News Datacom
HONG KONG	ROCTEC Enterprises, Ltd.
HONG KONG	Techtrend Engineering, Ltd. (TEL)
HONG KONG	Triple D Ltd.
ICELAND	Logi Ragnarsson
ICELAND	Softis hf
INDIA	Bharat Electronics Ltd.
INDIA	Chenab Info Technology
INDIA	DCM Data Products
INDIA	Digital Electronics Ltd.
INDIA	Digital Equipment (India) Ltd.
INDIA	Hewlett-Packard (India) Pvt. Ltd.
INDIA	Hinditron Computers Pvt. Ltd.
INDIA	International Computers Indian Manufacture Ltd.
INDIA	International Data Management Ltd.
INDIA	OMC Computers Ltd.
INDIA	Patni Computer Systems Ltd., Export Division
INDIA	PSI Data Systems Ltd.
INDIA	Quantum System Software
INDIA	Rolta India Limited
INDIA	Tata Burroughs Ltd.
INDIA	Tata Consultancy Services
INDIA	Tata Unisys Ltd.
INDIA	Texas Instruments (India) Pvt. Ltd.
INDIA	Wipro Systems Limited
INDONESIA	Digitus Computer Systems
IRAN	Communications Industries Group
IRAN	Shabakeh Gostar Corporation
IRELAND	AT&T Network Systems Ireland
IRELAND	Eurologic Systems, Ltd.
IRELAND	Isocor Ireland
IRELAND	Priority Data Systems Ltd
IRELAND	Renaissance Contingency Services Ltd.
IRELAND	Shamus Software Ltd.
IRELAND	Silicon Software Systems Ltd.
IRELAND	Software and Systems Engineering Ltd.
IRELAND	Software Systems Engineering Ltd.
IRELAND	Systemics Ltd.
ISLE OF MAN	Invisimail International Ltd.
ISRAEL	Aladdin Knowledge Systems, Ltd.
ISRAEL	Algorithmic Research Ltd.
ISRAEL	Aliroo Ltd.
ISRAEL	Areshelt Systems Ltd.
ISRAEL	Carmel Software Engineering Ltd.
ISRAEL	Check Point Software Technologies Ltd
ISRAEL	Elementrix Technologies Ltd.
ISRAEL	Iris Software
ISRAEL	News Datacom
ISRAEL	RADGUARD, Ltd
ISRAEL	Secure Network Systems, Ltd.
ISRAEL	Tadiran
ISRAEL	Vanguard Security Technologies Ltd.
ITALY	AMTEC SPA
ITALY	CERT-IT
ITALY	Eutron Spa
ITALY	Incaa SRL
ITALY	Olivetti
ITALY	Ratio Srl
ITALY	Siosistemi ari
ITALY	Systems Comunicazioni srl
ITALY	TELSY Elettronica e Telecomunicazioni S.p.A.
ITALY	Telvox s.a.s.
IVORY COAST	Software Marketing Consultancy
JAPAN	ADVANCE Co., Ltd.
JAPAN	Compal Inc.
JAPAN	Fujitsu Labs Ltd.

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

JAPAN	Jade Corporation Ltd
JAPAN	Mitsubishi Electric Corporation
JAPAN	Mitsubishi Electric Engineering Company Ltd
JAPAN	Netscape Communications KK Japan
JAPAN	Nihon RSA
JAPAN	Nipon Telephone & Telegraph
JAPAN	Open Software Foundation / Pacific
JAPAN	Paradyne Japan, KK
JAPAN	Toshiba Information Systems (Japan)
JAPAN	Yokohama National University
KENYA	Memory Masters
KUWAIT	LBI International
LUXEMBOURG	Data Alert International Elfhoven BV
MADAGASCAR	Megabyte Computers
MALAYSIA	Digitus Computer Systems
MALTA	LBI International, Inc.
MALTA	Panta Computer Co Ltd.
MALTA	Shireburn Co. Ltd.
MAURITIUS	Megabyte Computers Ltd.
MEXICO	Computer Security Corporation
MEXICO	Ontrack Computer Systems, Inc.
MEXICO	Seguridata Privada S.A. de C.V.
MEXICO	The King of Hearts
NEPAL	Quantum System Software
NETHERLANDS	Ad Infinitum Programs (AIP-NL)
NETHERLANDS	Alco Blom Software
NETHERLANDS	Ascit B.V.
NETHERLANDS	Atlantis Nederland BV
NETHERLANDS	Concord Eramcom Nederland BV
NETHERLANDS	CRYPSSYS Data Security
NETHERLANDS	Cryptech Nederland
NETHERLANDS	Data Alert International Elfhoven BV
NETHERLANDS	DigiCash
NETHERLANDS	DSP International
NETHERLANDS	Elfhoven Automatisering
NETHERLANDS	Eliashim Europe B.V.
NETHERLANDS	Geveke Electronics BV
NETHERLANDS	Incaa Datacom BV
NETHERLANDS	Incaa Nederland B.V.
NETHERLANDS	Philips Crypto B.V.
NETHERLANDS	Pijnenburg
NETHERLANDS	PTT
NETHERLANDS	Symantec, Netherlands
NETHERLANDS	Tulip Computers BV
NETHERLANDS	Verspeck & Soeters b.v.
NEW ZEALAND	CES Communications Ltd.
NEW ZEALAND	John Gilmore
NEW ZEALAND	Loadplan Australasia Pty Ltd
NEW ZEALAND	LUC Encryption Technology, Ltd. (LUCENT)
NEW ZEALAND	Microsoft New Zealand
NEW ZEALAND	Peter Gutmann
NEW ZEALAND	RPK New Zealand Ltd
NIGERIA	Software Marketing Consultancy
NORWAY	Alladin Software
NORWAY	BDC Bergen Data Consulting A/S
NORWAY	Bergen Data Consulting A.S.
NORWAY	Columbi Micro a.s.
NORWAY	Ericsson Semafor
NORWAY	InfoMedica AS
NORWAY	Informasjonskontroll A/S
NORWAY	Informatikk A/S
NORWAY	Kirkedam Elektronikk EDB
NORWAY	Notis A.S.
NORWAY	PDI
NORWAY	Scand PC Sys/Sectra
NORWAY	Siemens Nixdorf, Informasjonssystemer A/S
NORWAY	Skanditek A/S
NORWAY	Sterling Software Scandinavia A/S
NORWAY	Swanholm Distribution A/S
NORWAY	Telepartner as
NORWAY	Voicetech A.S.
OMAN	LBI International
PHILIPPINES	Digitus Computer Systems
POLAND	Dagma sp z o o
POLAND	Enigma Information Security Systems
POLAND	SOFT-u.1.
PORTUGAL	Infornova
PORTUGAL	Redislogar SA
PORTUGAL	RSVP Consultores Associados Lda
QATAR	LBI International
REUNION	Megabyte Computers
ROMANIA	Interscope s.r.l.
RUSSIA	<UNKNOWN>
RUSSIA	Ancort
RUSSIA	Askri
RUSSIA	Elias Ltd.
RUSSIA	INFORM - RTG
RUSSIA	LAN Crypto
RUSSIA	RESCrypto
RUSSIA	ScanTech
RUSSIA	TELECRYPT, Ltd.
SAUDI ARABIA	Info Guard Saudi Arabia
SAUDI ARABIA	LBI International Ltd

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

SINGAPORE	Communications Systems Engineering Pty. Ltd.
SINGAPORE	Diethelm Singapore Pte, Ltd
SINGAPORE	Digitus Computer Systems
SINGAPORE	Digitus Computer Systems
SINGAPORE	Microsoft Singapore Pte, Ltd.
SLOVAK REPUBLIC	Lynx sro
SLOVAK REPUBLIC	PCS Bratislava sro
SOUTH AFRICA	BSS (Pty) Ltd.
SOUTH AFRICA	BSS (Pty) Ltd.
SOUTH AFRICA	Citadel Data Security
SOUTH AFRICA	Computer Security Associates
SOUTH AFRICA	Denel Informatics
SOUTH AFRICA	EFT
SOUTH AFRICA	Intelligent
SOUTH AFRICA	Nanoteq
SOUTH AFRICA	Net One
SOUTH AFRICA	NetSec
SOUTH AFRICA	Sentera
SOUTH AFRICA	Siemens Ltd. So. Africa -Pretoria
SOUTH AFRICA	Siemens Ltd.-So Africa
SOUTH AFRICA	Spescom
SOUTH AFRICA	Thawte Consulting
SOUTH AFRICA	Digitus Computer Systems
SOUTH KOREA	Future Systems, Inc.
SOUTH KOREA	JiranSoft
SOUTH KOREA	Penta Security Systems Inc.
SOUTH KOREA	Senex Technologies Inc. Ltd
SOUTH KOREA	SoftForum
SPAIN	Asociacion Espanola de Empresas de Informatica
SPAIN	Asociacion Nacional de Industrias Electronicas
SPAIN	Atlantis Iberica
SPAIN	Economic Data al
SPAIN	SECARTYS
SPAIN	Sinutec
SWEDEN	Ardy Elektronics
SWEDEN	AU-System Communication AB
SWEDEN	AU-System Infocard AB
SWEDEN	AV System Infocard
SWEDEN	Business Security AB
SWEDEN	COST Computer Security Technologies International
SWEDEN	DynaSoft
SWEDEN	Glenn Larsson
SWEDEN	Henry Padilla
SWEDEN	QA Informatik AB
SWEDEN	SECTRA AB
SWEDEN	SONNOR Crypto AB
SWEDEN	Stig Ostholm
SWITZERLAND	ASCOM Tech AG
SWITZERLAND	Brown-Boveri
SWITZERLAND	Crypto AG
SWITZERLAND	Ete-Hager AG
SWITZERLAND	ETH Zurich
SWITZERLAND	ETH Zurich
SWITZERLAND	Gretacoder Data Systems AG
SWITZERLAND	Incaa Datacom AG
SWITZERLAND	Lightning Instrumentation SA
SWITZERLAND	Markt & Technik Vertriebs AG
SWITZERLAND	Omnisec AG
SWITZERLAND	Organa
SWITZERLAND	Safeware AG
SWITZERLAND	Theissen Security Systems Ltd.
TAIWAN	Digitus Computer Systems
THAILAND	Digitus Computer Systems
TURKEY	ASELSAN Inc.
TURKEY	Logosoft Yazlim San Tie Ltd
UAE	LBI International
UK	<UNKNOWN>
UK	Adam Back
UK	Andrew Brown
UK	Apricot Computers, Ltd.
UK	Atlantic Coast plc.
UK	Avant Guardian Ltd.
UK	Baltimore Technologies plc.
UK	Ben Laurie
UK	British Telecom
UK	Business Simulations
UK	Cambridge Electric Industries
UK	Codepoint Systems Ltd.
UK	Computer Security Ltd.
UK	Cray Electronics Holding, PLC
UK	Cylink Ltd.
UK	Data Innovation Ltd.
UK	Datamedia Corporation, Ltd.
UK	DataSoft International Ltd.
UK	Digital Crypto
UK	Dynatech Communications Ltd. (Northern office)
UK	Dynatech Communications Ltd.
UK	Emergent Technologies, Ltd.
UK	EngRus
UK	Ewen Associates Limited
UK	Fauzan Mirza
UK	Finansa
UK	Fulcrum Communications

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

UK	GEC-Marconi Secure Systems
UK	Gelosia
UK	Gretag Ltd.
UK	Honeywell
UK	ICL Secure Systems
UK	Incaa UK
UK	InfoShare
UK	Instant Access
UK	Interconnections
UK	International Data Security, Ltd.
UK	International Software Management
UK	IQ International
UK	IT Security International
UK	ITV
UK	J.R.Ward Computers Ltd.
UK	J.S.A. Kapp
UK	Jaguar Communications Ltd.
UK	Janus Sovereign
UK	JCP Computer Services
UK	JPY Associates Ltd.
UK	Loadplan
UK	Logica
UK	Microft Technology Ltd.
UK	Microsoft Ltd.
UK	NEST Ltd.
UK	Network Systems Corporation (UK)
UK	Newbridge Networks Ltd
UK	News Datacom
UK	Northern Telecom Europe Ltd.
UK	Novell, Ltd. (UK)
UK	Paradyne European Headquarters
UK	PC Security Ltd.
UK	Plessy Crypto
UK	Plus 5 Engineering Ltd.
UK	Portcullis Computer Security Ltd.
UK	PSCP
UK	Premenos UK Limited
UK	Prosoft Ltd.
UK	Protection Systems Ltd.
UK	Racal Air Tech
UK	Racal Airtech Ltd.
UK	Radius
UK	Reflex Magnetics Ltd.
UK	S&S International PLC
UK	Sapher Servers Ltd.
UK	Securicor 3net Ltd.
UK	Sington Associates
UK	SmartDisk Security Corp. UK (SDSC)
UK	Smith's Associates
UK	Soft Concepts
UK	Softdiskette
UK	Sophos Ltd.
UK	Stralfors Data
UK	Sygnus Data Communications
UK	Time & Data Systems
UK	Tricom
UK	University College London
UK	Widney Ash
UK	Zeta Communications Ltd.
VENEZUELA	GDV Sistemas
WEST INDIES	Global Traders Inc Ltd
WEST INDIES	Global Traders Inc Ltd
YUGOSLAVIA	Sophos Yu d.o.o.
ZIMBABWE	RyVal Computer (Private) Ltd

**D. REPORT OF THE PRESIDENT'S EXPORT COUNCIL SUBCOMMITTEE ON
ENCRYPTION, WORKING GROUP ON INTERNATIONAL ISSUES**

September 18, 1998

The following findings have been adopted by the PECSENC as a reflection of conditions of international competition prior to the U.S. Government's liberalization of encryption export controls announced on September 16, 1998. The liberalization may affect many of these findings, and the findings will be used as a baseline for a review of the effects of the liberalization in future sessions of the PECSENC.

1. The difference between U.S. encryption controls and those of other nations is a serious -- but not the only -- factor determining success in the computer security market. With or without controls, both U.S. and foreign products are likely to continue to coexist, and other factors are likely to continue to slow deployment of security products. Many foreign companies, for example, especially those influenced by governments, will continue to favor domestic security solutions, and many computer users will not deploy serious security technology until there have been major incidents with losses that can be attributed to lack of encryption.

2. Nonetheless, the adverse impact of controls on U.S. industry is palpable. For many software applications, business customers simply demand security and encryption; it is a checklist item, and its absence is a deal breaker. While simply counting the number of foreign encryption software products in the market is not an accurate measure of the impact of controls, one particularly serious risk is that non-U.S. companies will use their ability to export stronger encryption as "leverage" to dominate particular applications.

This has happened in at least one field - Internet banking - and may occur in other areas of electronic commerce. Brokat, a German company that scarcely existed four years ago, now has 250 employees and offices in several countries including the United States. Brokat's specialty is Internet banking and electronic commerce, but it broke into that business on the strength of being able to offer stronger encryption than German banks could obtain in Netscape or Microsoft browsers. It is now a major player in this niche, with 50% of the European Internet banking market and enough U.S. customers to justify a 20-person U.S. branch office. Meanwhile, encryption constitutes 10% or less of Brokat's revenue, and it has expanded its initial Internet banking offerings to include support for other forms of electronic commerce. Loss of U.S. competitiveness in the electronic commerce software market obviously raises concerns not just about encryption software but other software opportunities. Indeed, it foreshadows a weakening of the U.S. position as a leader in electronic commerce generally.

3. The persistent emphasis in U.S. export control policy over the past two years on key recovery, or "lawful access," has also taken a toll on the

credibility of U.S. security products. Key recovery continues to find a market. Business wants to ensure that data are available for corporate purposes, including litigation. Key recovery is seen as an important feature for stored business data (though not for communicated data in transit).

But the use of export controls to drive the key recovery market further than it would go by itself is hurting U.S. industry. Foreign governments and competitors, particularly in Europe, have misinterpreted this U.S. policy, perhaps deliberately. In essence, foreign customers are told often by their governments as well as local security companies that all U.S. encryption products come with a back door allowing the U.S. government to read the contents. In part this is the result of outmoded "Recovery" supplements to U.S. export rules that demand an unrealistic level of U.S. government access to key recovery products. In part it reflects the hostility of many foreign governments toward U.S. key recovery and access policies. It also reflects the fact that some countries will simply never rely on security products that are not home-grown, and misunderstanding U.S. key recovery policies may simply be a handy stick to beat U.S. products with. But it is unfortunate that the U.S. government has provided such a large and easily wielded stick.

4. U.S. controls are driving many U.S. companies into "cooperative arrangements" with foreign encryption suppliers. These cooperative arrangements allow U.S. companies to provide complete security solutions by encouraging their foreign partners to marry foreign-made crypto with U.S. commercial applications. These cooperative arrangements are highly risky under U.S. law, but they are not unlawful per se. Given the stakes, many companies have been prepared to take risks under U.S. law, and it is expected that more will do the same. The result is that U.S. policy has fostered the development of cryptographic software and hardware skills outside the United States. German, Swiss, Canadian, Russian, and Israeli cryptography companies have all benefited from this unintended consequence of U.S. encryption policy.

5. The U.S. government has made efforts to "level the field" of disparate export controls for encryption through negotiations under the Wassenaar Agreement. The U.S. proposal that 56-bit encryption become a new "floor" for encryption exports under Wassenaar, while certainly better than current policy, is likely to be implemented at least a year and perhaps several years too late. In response to the U.S. KMI initiative, which conditionally decontrolled 56-bit encryption in December 1996, other countries also decontrolled 56-bit DES but more or less unconditionally. The countries include Canada and apparently the United Kingdom. And by 1996, other countries, such as Germany, already were approving the export of 56-bit DES to virtually any country for virtually any purpose. Most recently, the exhaustion of a 56-bit DES key using a machine built for a quarter million dollars has entirely discredited DES as a serious security tool for valuable secrets. Single DES remains a useful tool for assuring privacy against a wide variety of potential adversaries and snoops, but decontrolling 56-bit encryption will not provide a significant boost to the competitiveness of U.S. technology for serious security applications.

6. Process and timing: In 1995, the State Department approved routine

GROWING DEVELOPMENT OF FOREIGN ENCRYPTION PRODUCTS
IN THE FACE OF U. S. EXPORT REGULATIONS

license applications for the export of encryption in less than a week on average. This was when the State Department had jurisdiction over encryption and NSA staffed the State Department's office and handled all encryption license applications.

This is no longer the case. The Commerce Department has staffed up heavily in the encryption field, but its processes now include parallel reviews by the FBI and NSA under a 30-day deadline that can be extended further with a simple "no" vote by either agency. For whatever reason, these agencies are now taking the full 30 days -- and often 90 days. Against a backdrop of continued export liberalization over the past four years, this degradation in export control performance strikes a jarring note.

The Commerce Department's performance in this area is not necessarily out of line with the performance of other countries. The German government often takes two to three months to approve a license for a new product and six weeks to approve a license for routine shipments. The difference is that German companies know with certainty that a license will be issued at the end of the process; and the German government imposes no key recovery requirement on exporters. Therefore, they can make commitments to deliver products that require a license even before they get the license. In the United States, both the FBI and NSA have at times cast votes intended to roll back existing policies, and they have at a minimum managed to stall licenses that seemed to fit existing policy. A key recovery policy, for example, has been applied sporadically to U.S. multinationals and with some inconsistency to other exports. For this reason, it is not prudent for exporters to assume that a license will be issued or to make commitments on the assumption that the license will be issued - even when existing policy makes it seem likely that a license will eventually be granted. Because an RFP by a foreign company may provide only 30 days for responsive proposals, and the proposals often must include an assurance that an export license will be obtained, some U.S. companies lose bidding opportunities simply because the U.S. government does not process licenses quickly enough.

In other respects, of course, Commerce Department practice is a large improvement over State's performance. This is particularly true for controversial licenses, on which Commerce typically forces a decision over a course of months. In contrast, State Department licenses could be held up for months without any explanation and there were no deadlines for resolving interagency disputes. Nonetheless, it seems clear that the Commerce Department and the other participants in the encryption licensing process should adopt additional procedures to speed the granting of relatively non-controversial licenses.