EUROPEAN PARLIAMENT

SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT

STOA

DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION

Vol 3/5
Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues

Working document for the STOA Panel

Luxembourg,November 1999 PE 168.184/Vol 3/5/EN

Cataloguing data:

Title: **Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues**

Workplan Ref.: EP/IV/B/STOA/98/14/01

Publisher: European Parliament
Directorate General for Research
Directorate A
The STOA Programme

Author: Dr Franck Leprevost - Technische Universität Berlin

Editor: Mr Dick HOLDSWORTH,
Head of STOA Unit

Date: November 1999

PE number: **PE 168. 184 Vol 3/5**/EN

This document is part of a series published in five volumes.
(Vols. 1/5 - 5/5).
The original language of this publication is French.

Chiffrement, cryptosystèmes et surveillance électronique : un survol de la technologie
Résumé

Les objectifs de ce rapport sont :

- rappeler aux Membres du Parlement Européen les risques, concernant la surveillance électronique, inhérents à l'utilisation des moyens modernes de communication ;
- fournir aux Membres du Parlement Européen un document de référence concernant les technologies de cryptage, et les statuts actuels des démarches de standardisation de ces techniques ;
- décrire les directions futures possibles en ce qui concerne, tant les communications sécurisées, que les méthodes de surveillance électronique ;
- donner aux Membres du Parlement Européen une traduction, à la fois précise et claire pour les non-experts, et montrer les implications pratiques, de documents techniques relatifs à la sécurité de l'information, constituant des amendements récents à des organismes de contrôle internationaux ;
- proposer des options aux Membres du Parlement Européen permettant de préserver les intérêts des citoyens, entreprises et organisations européennes.

Le rapport contient six parties principales.
La première est une description succinte des moyens de communications modernes utilisés et de leurs risques ; la deuxième fournit un survol des techniques cryptographiques actuelles : cryptographie à clef secrète, cryptographie à clef publique, cryptographie quantique, qui sont détaillées dans les trois parties suivantes. La troisième partie donne une description précise de la cryptographie à clef secrète, un état de l'art concernant la situation en termes de sécurité informatique de protocoles très largement utilisés, et un point actuel sur les procédures de standardisation du futur standard fédéral américain, qui devrait s'imposer comme standard mondial. La quatrième partie donne une description très précise de la cryptographie à clef publique, un état de l'art concernant les procédures de standardisation au niveau mondial des protocoles à clef publique, une lecture technique d'un document de la DG XIII de la Commission Européenne. La mise en oeuvre pratique de la cryptanalyse et de la cryptographie quantique peuvent avoir des conséquences particulièrement importantes au niveau international sur le plan politique, diplomatique ou financier : la cinquième partie décrit l'état de l'art concernant ces deux directions. Le Wassenaar Arrangement concerne les contrôles sur les exportations d'armes conventionnelles et les produits technologiques sensibles, et regroupe 33 pays, dont ceux de la Communauté Européenne et les signataires de l’accord UKUSA. La sixieme partie est une lecture technique des amendements concernant la sécurité de l’information du 3/12/1998 au Wassenaar Arrangement. La derniere partie du document est une liste de suggestions de nature a protéger les citoyens européens, et à préserver les intérêts des entreprises et organisations européennes. Elle donne également des projets de recherches complémentaires, afin de mieux mesurer l'impact de certains accords internationaux sur le plan de la surveillance électronique en Europe. Le rapport inclu une bibliographie, donnant une liste des documents référencés.

Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues

FRANCK LEPREVOST

1. Introduction

Electronic surveillance is generally considered to be a weapon with which to fight organised crime or terrorism ([**32**], Foreword, p. iii). It can, however, have a darker side, namely that of industrial espionage, violation of privacy, or both.
The report [**35**] published by STOA in January 1998 refers to the role played by the ECHELON network in electronic surveillance (see [**8**] for a list of links to this subject). It is a global network which can intercept all telephone, fax or e-mail communications.
Although it is very difficult to quantify the losses caused by industrial espionage (many cases are not reported, either because the company fears losing face or simply because the damage goes undetected), the losses incurred by firms in the European Union can reasonably be put at several billion euros per year. The extent of the problem can be surmised from a study published by PricewaterhouseCoopers Investigation LLC ([**27**]) on 22 March 1999; the study shows that over 59% of all firms with a significant presence on the Internet were spied on in 1998. Furthermore, it is quite conceivable that information acquired by such means is exploited by the international stock markets. It is an issue which thus affects shareholders, companies and national economies alike.
The initial purpose of this report is to illustrate the main techniques whereby EU citizens, firms and institutions can protect themselves, to a certain extent, against what is now known as economic intelligence.
In Section 2, we outline the various means of communication generally used. We also describe some of the techniques, of varying degrees of sophistication, by means of which information can be unlawfully accessed, and some countermeasures which can be taken. Technological measures allowing data to be transmitted confidentially require the use of cryptosystems, which are briefly defined and illustrated in Section 3. In Sections 4, 5 and 6 we outline the latest developments in secret-key, public-key and quantum cryptographic protocols. As regards the first two, we give an update on standardisation procedures. In Section 7 we conduct a technical appraisal of the information security aspects of the Wassenaar Arrangement, which concerns export controls for conventional arms and sensitive technological products. We conclude the report by making recommendations to the European bodies.

This document does not necessarily represent the views of the European Parliament. Nevertheless, in this report commissioned by STOA, and particularly in Sections 2, 7 and 8, we systematically viewed things from a standpoint which we judged to be the most favourable vis-à-vis the defence of European interests.

2. Means of communication used and risks involved

In this section we look at relatively hi-tech methods of communication; direct oral transmission and traditional mail are therefore not dealt with. For the sake of clarity and in keeping with standard practice in this field, we have designated Alice and Bob as two hypothetical individuals wishing to communicate.

2.1 Standard telephones. Standard telephone systems can be tapped without any technical difficulties: a microphone can be placed inside the telephone set; alternatively, the wires of the telephone exchange of the building where the target is located can be tapped, as can those of the telephone company's central exchange. These techniques are largely undetectable by the target.

2.2 Voice-scrambling telephones. Secure telephones and fax machines are now available on the market. Their level of security may be very modest, depending on the legislation currently in force in their country of origin (see Section 7).

2.3 Fax machines. As things stand, fax machines should be considered as insecure as telephones. Fax-encrypting machines do exist, but their security level is contingent on legislation in their country of origin, as above.

2.4 Cordless telephones. Some older models transmit just above the AM broadcasting band and can thus be easily intercepted. Commercially-available scanners enable the more recent models to be tapped. Sometimes certain sound wave inversion techniques are recommended in order to combat tapping, but these solutions only provide a very low level of confidentiality. As regards cellular phones, the situation is more complex. Early models transmit in the same way as radios and so do not provide a high level of confidentiality, since conversations can be intercepted using inexpensive scanners (equally low-priced equipment can be purchased to increase the frequencies accessible to the scanners currently on the market). It is worth mentioning here the US Administration's attempt to impose the Clipper standard on all portable phones developed in the United States. This would have allowed government agencies to retain keys enabling them to eavesdrop on conversations. Moreover, details of the encryption algorithm 'Skipjack', developed by the NSA, have not been made public.

The GSM system, the international standard for digital cellular phones, was developed by the GSM MoU Association (which became the GSM Association on 30 November 1998) in collaboration with the European Telecommunications Standard Institute ([**13**]), an international umbrella organisation bringing together public authorities, operator networks, manufacturers, service providers and users. GSM uses cryptographic techniques at various levels. As regards identification, GSM uses several algorithms, although in practice most operators use a protocol named COMP128. However, in April 1998 the Smartcard Developer Association ([**28**]), in collaboration with David Wagner and Ian Goldberg, researchers at UC Berkeley (USA), announced that it had developed a system whereby phones using the GSM standard could be cloned . But on 27 April 1998, Charles Brookson, chairman of the security group of the GSM MoU Association, stated that this would not be of any practical use to fraudsters.

With regard to confidentiality, GSM uses a protocol known as A5. There are two versions of this system: A5/1 and A5/2, which meet different needs. According to some experts, A5/2 is less secure than A5/1, which we will now discuss. The A5/1 protocol in theory uses 64 bits. But Wagner told us that in practice ([**33**]), in every phone he had seen, 10 bits had been systematically replaced with zeros, thus reducing the theoretical security of the system to 54 bits. The system is therefore even less secure than the 56 bits offered by DES, which can now be cracked all too easily (see 4.4). Work conducted before this discovery ([**11**]) had already reduced the real security of the system to 40 bits. It is therefore quite possible that by using similar methods, i.e. assuming that 10 bits are equal to zero, the actual security level of A5/1 – and hence the confidentiality of conversations - can be reduced even further.

On 24 February 1999, at the GSM World Congress in Cannes (France), Charles Brookson announced that GSM security had been reviewed and in particular that COMP128 had been revised.

2.5 ISDN. It is technically possible to tap an ISDN telephone with the help of software that remotely activates the monitoring function via the D channel, obviously without physically lifting the receiver. It is therefore easy to eavesdrop on certain conversations in a given room.

2.6 Internet communications. In a nutshell, the traditional mail equivalent of an e-mail on the Internet is a postcard without an envelope. Basically, such messages can be read. If they are in plaintext, they can be understood and any 'secret reader' can take measures which are detrimental to the two parties wishing to communicate. For example, if Alice sends a message to Bob and if

Charles is a passive attacker, Charles knows what message has been sent but he cannot modify it. If, on the other hand, he is an active attacker, he can modify it. One way of circumventing this problem is by encrypting the messages (see Section 3). However, the solutions developed by Microsoft, Netscape and Lotus for encrypting e-mails are configured in such a way that the NSA can systematically read all e-mails thus exchanged outside the United States (although it is probably the only agency that is able to do so).

2.7 The TEMPEST effect. TEMPEST is the acronym for Temporary Emanation and Spurious Transmission, i.e. emissions from electronic components of electromagnetic radiation in the form of radio signals. These emissions can be picked up by AM/FM radio receivers within a range varying from a few dozen to a few hundred metres. Building on these data it is then possible to reconstruct the original information. Protective measures against such risks consist of placing the source of the emissions (central processors, monitors, but also cables) in a Faraday cage, or jamming the electromagnetic emissions. The NSA has published several documents on TEMPEST (see [**25**]).

All computers work by means of a micro-processor (chip). The PC chip market is dominated by Intel, which has a market share of over 80%. On 20 January 1999 Intel unveiled its new PSN-equipped Pentium III processor.

2.8 PSNs. Pentium III processors have a unique serial number called PSN (Processor Serial Number). Intel devised this technique in order to promote electronic commerce. The aim of the serial number is to enable anybody ordering goods via the Internet to be identified. Intel maintains that all users will be able to retain control over whether or not to allow their serial number to be read. However, software techniques enabling the number to be read have already been discovered (see [**26**]) . It is therefore possible to obtain the PSN secretly and to track the user without his or her knowledge.

The PSN is very different from the IP (Internet Protocol) address, even though a user's IP address can be revealed to any webpage he or she chooses to visit. IP addresses are not as permanent as PSNs: many users have no fixed IP address that can be used to track their movements, as they may use masks via the proxy servers of Internet service providers. ISPs normally assign a different IP number per session and per user. Users can also change ISP, use a service which guarantees their anonymity, etc.

As it stands, the PSN can therefore be used for electronic surveillance purposes. Moreover, it is still not known for sure whether PSNs can be cloned. If so, their use for identification purposes in electronic commerce would have to be ruled out.

3. An overview of cryptographic techniques

Cryptography is the study of the techniques used to ensure the confidentiality, authenticity and integrity of information and its origin. Cryptography can be broadly divided into three categories: private-key, public-key and quantum cryptography. Several of these techniques make extensive use of hash functions. Here we give a brief outline of the techniques, explaining them in more detail in Sections 4, 5 and 6. However, it should be stressed that a high degree of confidentiality can be attained only by combining these techniques with measures to counter TEMPEST effects. Basically, it is no use encrypting data if, for example, they can be read in plaintext while being transferred from the keyboard to the central processor. Assuming that the information to be processed is in binary code, the fundamental unit of information referred to in all sections of this report is the bit, apart from in Sections 3, 4 and 6, where its quantum equivalent, the qubit, is used.

3.1 Hash functions. These are tools which have multiple applications; amongst other things, they can be used to create secret keys and electronic signatures. Their basic function is to rapidly map a file (of any size) to a fixed-size value, such as 160 bits, as in the European hash function RIPEMD-160. If the

value is known it should be impossible to reconstruct an initial text that would match the hash value. Essentially, it is very hard to invert. A hash function should also avoid collisions. In other words, it should not be possible to construct two distinct files giving the same hash values.

3.2 Secret-key cryptography. With this method, a single key is used both for encrypting and decrypting. This key should be known only to Alice and Bob. It can be of varying length. Secret-key cryptography can be divided into two categories: Stream Ciphers and Block Ciphers. With Stream Ciphers the length of the key is the same as that of the message to be transmitted. The 'right' size, i.e. that which can be used as a basis for recreating a key the same size as the message, can be reduced to a fixed size with the help of cryptographically secure pseudorandom bit generators. These generators have to pass very stringent statistical tests. As regards Block Ciphers, the size of the key is fixed (56 bits for DES, 128 bits for AES, see 4.3, 4.4). The main problems with this technique lie in the management and distribution of the keys.

3.3 Public-key cryptography. Unlike the secret-key algorithms, public-key algorithms require two keys per user. Alice (and Bob respectively) chooses a secret key, X_A (respectively X_B) and publishes (e.g. in a directory) a public key Y_A (respectively Y_B). Bob encodes his message with Y_A and sends it to Alice. Only Alice, with her secret key X_A, can decode the message. The security of public-key algorithms has a mathematical basis (see Section 5).
See [**21**] and [**23**] for details of a report (updated to 31 December 1998) on the standardisation procedures for AES secret-key protocols (see 4.5) and IEEE-P1363 public-key protocols (see 5.3).

3.4 Quantum cryptography. This method is dealt with in 6.2.

3.5 Cryptanalysis. Cryptanalysis is the perfection of techniques or attacks to reduce the theoretical security of cryptographic algorithms. This should not be confused with the hackers' approach, since they, as a rule, exploit weaknesses not in the algorithms themselves, but in the security architecture. In 4.4 we describe a number of attacks on secret-key cryptosystems and in 5.1 and 6.1 on public-key cryptosystems.

3.6 Security quantification. In general security is evolutive, as it often depends on the scientific knowledge of a given period. It may be absolute. For example, the only known form of attack for breaking various Block Ciphers is that of trying out all possible keys (Brute-Force Attack). Hence, if such a system uses a 56-bit key, security equals 2^{56} operations. It can also be relative: theoretically, a cryptosystem is considered to be insecure if it can be cryptanalysed in polynomial time according to the size of the data. Its degree of security can be considered satisfactory if it takes a sub-exponential, or better still, exponential period of time to cryptanalyse. More precise measurements can be provided in terms of MIPS/year. This unit of measurement is equivalent to a computer's computational capacity, carrying out a million instructions per second over a year (approximately 3.10^{13} instructions in all).

4. Secret-key cryptography

Secret-key cryptography can be divided into two categories: Stream Ciphers and Block Ciphers.

4.1 Stream Ciphers. These technologies are only rarely published. Where Block Ciphers encrypt in blocks, Stream Ciphers encrypt on a bit-by-bit basis. The most well-known of these, and the most cryptographically secure, is the One-Time Pad, which requires a key of the same length as the message to be transmitted. This key must also be created randomly. For practical purposes, the One-Time Pad is often simulated by means of cyptographically secure pseudorandom bit generators, often abbreviated to CSPRBG (Cryptographically Strong Pseudo-Random Bit Generator). Starting with an initial data item X_0 (seed), CSPRBG is used to create deterministically bits which appear to be random. This is then double-checked by subjecting the CSPRBG candidate to extremely stringent statistical

tests.

4.2 Block Ciphers. With Block Ciphers a message is cut into fixed-length blocks. With the aid of an algorithm and secret key K of fixed length, but possibly of a different length to the blocks, each block is encrypted and sent. The recipient decrypts each block with the same key K. All he or she then has to do is to 'stick' the blocks back together to recover the original message. The *de facto* standard for algorithms in the Block Cipher category is DES (see 4.4).

4.3 Problems. At least two problems may arise with these methods (Stream Ciphers and Block Ciphers):

> (a) How do Alice and Bob communicate the secret key K to each other?
> (b) In a network with *n* users where n(n – 1))/2 secret keys are needed (e.g. 499 500 secret keys in a network of 1 000 users), obvious problems of storage and security need to be addressed.

Public-key (see 5, particularly 5.2) and quantum (see 6.2) cryptography techniques provide partial solutions to these problems.

4.4 DES: state of the art. The symmetric algorithm most widely used at present is undoubtedly DES (Data Encryption Standard). In 1997 it was recognised as an FIPS (Federal Information Processing Standard) and registered as FIPS 46-2. DES uses a 56-bit key. There are therefore 2^{56} possible keys. The block length is 64 bits.
DES has enjoyed the political backing of the United States for a very long time. As recently as 17 March 1998, for example, Robert S. Litt (Principal Associate Deputy Attorney-General) maintained that the FBI did not have the technological and financial capacity to decrypt a message encrypted with a symmetric 56-bit secret-key algorithm. He concluded by stating that 14 000 Pentium PCs would need to be used for four months in order to achieve such a feat (see also statements by Louis J. Freeh (Director of the FBI) and William P. Crowell (Deputy Director of the NSA, [**10**], p. 1-2).
Nevertheless, the Electronic Frontier Foundation built a DES cracker and presented it at an informal (Rump) session of the Crypto '98 conference in Santa Barbara. The machine (worth USD 250 000, including the design) is described in [**10**]. Better still, the book explains how to scan the plans in order to reproduce the machine for a maximum outlay of USD 200 000 (basically there is no need to pay over again for the design). This machine is capable of finding a secret DES key in an average of four days. In January 1999 a team led by the Electronic Frontier Foundation won the RSA Laboratories' Challenge (pocketing USD 10 000 for their efforts) by managing, with the aid of a large computer network, to break a 56-bit key in 23 hours 15 minutes. This has both political and diplomatic implications: it appears that it is now financially feasible for all nations to decode all DES-encoded records that may have been built up over the years. From now on all DES-based systems should therefore be considered insecure. In practice, it is now advisable to use Triple-DES at the very least (though even here caution is needed). The NIST (National Institute for Standards and Technology), mindful of the risks relating to DES, has called on the cryptographic community to work on its successor – AES (Advanced Encryption Standard [**24**]).

4.5 AES. The required features for AES are: a) the algorithm should be a secret-key Block Cipher type algorithm, and (b) it should support the following combinations of cryptographic key-block sizes: 128-128, 192-128 and 256-128 bits. The algorithms used in AES will be royalty-free worldwide. The algorithm should also be sufficiently flexible, for example, to allow other combinations (64-bit block lengths); it should be efficient on various platforms and in various applications (8-bit processors, ATM networks, satellite communications, HDTV, B-ISDN, etc.) and it should be usable as a Stream Cipher, MAC (Message Authentication Code) generator, Pseudo-Random Number Generator, etc.
The first AES conference was held on 20 August 1998 (just before the Crypto '98 conference). During the conference, presentations were given of the 15 (out of 21) candidates that had been

accepted: CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOK197, MAGENTA, MARS, RC6, RIJNDAEL, SAFER+, SERPENT and TWOFISH.
At present, it seems that the DEAL, LOK197, FROG, MAGENTA and MARS (in the extra-long key version) proposals are subject to attacks of varying intensity.
The second AES conference will be held in Rome on 22-23 March 1999, after which five algorithms will be chosen out of the 15 candidates. The debate on the 15 candidates has already begun ([**3**]). A third AES conference will be held from six to nine months later, when the winner will be announced. Following a final examination period of another six to nine months, the winning algorithm will be put forward as an FIPS. It is likely that AES will become an FIPS in around 2001.

5. Public-key cryptography

5.1 A description of public-key cryptography. The security of public-key algorithms has a mathematical basis:

- Factoring of large integers: RSA (Rivest-Shamir-Adleman) and Rabin-Williams.
- Discrete Log Problem: DSA (Digital Signature Algorithm), Diffie-Hellman key exchange, El Gamal cryptosystem and electronic signature and Schnorr and Nyberg-Rueppel electronic signatures.
- Discrete Log Problem for elliptic curves: the above algorithm equivalents also apply to elliptic curves. Given an elliptic curve E defined over a finite field Fp or $F2^n$, it is essential to be able to rapidly calculate the number of rational points on the elliptic curve over the finite field in question. The Schoof-Elkies-Atkin method (now known as SEA) is normally used for this purpose. In some cases (Koblitz curves or complex multiplication curves) this number is very easy to calculate.

Public-key cryptosystems are prone to attacks:

- Factoring of large integers: the ECM (Elliptic Curve Factoring Method) is used to find small factors. At present QFS (Quadratic Field Sieve) or NFS (Number Field Sieve) are used to find large factors. There is a limit to the numbers that can be considered. Very recently, Professor Shamir of the Weizmann Institute perfected an approach known as the 'Twinkle Attack' which enables 512-bit numbers to be factored with great rapidity. The cost of the attack is also very modest. At present, therefore, RSA-512 bits should no longer be considered secure.
- Discrete Log Problem: to solve this problem, the index-calculus method or the NFS method can be used. There is a limit to the numbers that can be considered.
- Discrete Log Problem for elliptic curves: a well-known attack is Pollard's rho method (which can also be parallelised). Here too, only certain curves can be considered: the so-called supersingular or anomalous elliptic curves should be avoided (a very rapid practical test can show whether a given elliptic curve is suitable).

The techniques based on the problem of factoring, on the one hand, and the discrete logarithm, on the other, are fundamentally different. For the former, large prime numbers have to be secretly produced and stored. As it is not humanly possible to remember large prime numbers, they have to be stored on a physical medium, which could give rise to security problems.
The approach to the discrete logarithm problem is different. For example, the user can freely choose a text that is easy to memorise (e.g. a poem). The text is then translated into binary code and hashed with a tried-and-tested hash function, such as the European proposal RIPEMD160, which has an output of 160 bits (see. 3.1). These 160 bits, being impossible to memorise, form the user's secret key. This approach has the advantage of limiting storage problems.
These two approaches solve different problems, according to the parameters involved. Elliptic curve-based techniques are now the focus of attention, since unlike other proposals, no subexponential algorithm has as yet been discovered to resolve the discrete logarithm problem for these groups. Consequently, elliptic curves over fixed-size fields provide the same degree of security as other algorithms for fields or modules of a larger size. For example, the security provided by elliptic curves for a 163-bit module is equivalent to that provided by RSA for 1024 bits.

5.2 Symmetric or public-key cryptography? Symmetric and public-key cryptosystems are not mutually exclusive . On the contrary, for the secure transmission of a document through an open channel (e.g. Internet), they are most useful if combined.
For example, Alice lives in Paris and wishes to send a 15-page report by e-mail to Bob, who lives in Brussels. It is out of the question for Alice to go to Brussels to give a secret AES key to Bob. If she were to choose this expensive method, she might just as well deliver the document in person! Naturally, Alice and Bob could choose to communicate using public-key cryptographic techniques, as described above, the only problem being that encryption with these techniques is about 1000 times slower than encryption using secret-key cryptosystems.
The most practical solution could be the following:

- Alice sends a 128-bit message K to Bob using public-key cryptography. The use of public-key techniques is warranted, as the message is very short (128 bits). Alice and Bob thus share the secret K.
- As agreed between them according to standard practice, K is the secret key to a secret-key algorithm, AES.
- Alice and Bob forget the public-key technology. To continue communicating they use AES with the K key. Alice can now send her 15-page document to Bob for the price of a phone call.

Alice's and Bob's systems must, however, be compatible: indeed, the aim of the standardisation drive described below is to harmonise communications.

5.3 IEEE-P1363 and other standards. The P1363 project began in 1993 under the auspices of the IEEE (Institute of Electrical and Electronics Engineers) Standardisation Committee. Its aim is to improve communications between several families of public-key cryptosystems: RSA, El Gamal, Diffie-Hellman and elliptic curves. Since the end of 1996, the techniques considered by P1363 have changed little and have been summarised in ([**16**]). The P1363A project contains additional techniques.
The standard project (draft version 9) is now ready to be revised by a group of experts from the IEEE Standards Association. The group started its work in February 1999 and will deliver its initial conclusions on 2 April 1999. According to the most optimistic estimate, the draft will be approved as a standard on 25 June 1999.
The IEEE-P1363 standard will have a huge influence on other standards, such as ANSI X9.42, ANSI X9.62 and ANSI X9.63 in the banking industry. It will also be the cornerstone of the X.509 ([**17**]) and S-MIME ([**18**]) protocols. These multiple protocols are essential for
electronic commerce.

5.4 A technical interpretation of the Commission (DG XIII) document COM(97) 503. This document [**12**] sets out Community-wide requirements with regard to secure electronic communications. It focuses on both electronic signatures and confidential methods of electronic communication. Below we suggest a few updates to Technical Annexes I (Digital Signature) and II (Symmetric and asymmetric encryption) to this document.

Annex I. It would be preferable to avoid citing MD2 and MD5 as examples, since cases of collision in the former and pseudo-collision in the latter have been brought to light. It would also be advisable to replace SHA by SHA-1 (based on [**14**]) and to write RIPEMD-160 (based on [**7**]) instead of RIPEM 160. It is currently recommended that one of these two hash functions be used to replace the MD2, MD4 and MD5 functions wherever possible.
Annex II. Symmetric encryption systems. It would be preferable to avoid citing DES and SAFER as examples. We suggest that IDEA, which so far has shown no serious flaws, be retained and that the candidates that passed the first AES round be mentioned.
Annex II. Asymmetric encryption systems. Once again, as regards the examples provided, it would be advisable to be more specific, e.g. by taking up the approach described at the start of 5.1, which is currently being standardised.
Annexe II. Systems security. We suggest deleting the last sentence of the second paragraph: 'In a symmetric system like DES or IDEA, keys of 56 to 128 bits provide similar protection as a 1024-bit public key'. This assertion is totally

false.

6. Quantum cryptanalysis and quantum cryptography

Quantum cryptanalysis and quantum cryptography may have a considerable impact in the political, diplomatic and financial terms.

6.1 Quantum cryptanalysis. The term quantum cryptanalysis refers to the set of techniques whereby the secret keys of cryptographic protocols can be found by means of quantum computers. It is an area in which research is thriving, as in August 1998 one of the system's founders, Peter Shor of AT & T Bell Labs, won the Nevanlinna Prize, which was awarded to him at the International Congress of Mathematicians in Berlin. He has developed methods based on quantum physics to factor large numbers in polynomial time ([**29**], [**30**]) or to solve the Discrete Log Problem even when formulated within the general context of Abelian varieties ([**31**], see [**32**] for a summary of these results).

Consequence: if these results were to be put into practice, the immediate consequence would be that the security of the public-key cryptographic protocols described in Section 5 would be permanently undermined. In addition, cryptosystems based on Abelian varieties would then be cryptanalysed via quantum computing. A parallel can be drawn between these consequences and the comments in 7.3 relating to the Wassenaar Arrangement.

Despite this, IEEE-P1363 is still valid: the Shor algorithms require a powerful quantum computer, whose existence is still hypothetical. Various experimental proposals have been made (qubits are the quantum equivalent of bits and are basically dual-state quantum systems):

- To use the electronic states of ions as qubits in an electromagnetic ion trap and to manipulate them with lasers (see [**4**]).
- To use nuclear atom spins in a complex molecule as qubits, and to manipulate them using nuclear magnetic resonance (see [**6**] and [**9**]).
- To use the nuclear spins of silicon chip impurities as qubits and to manipulate them using the chip's electronics (see [**19**]).

None of these proposals has been tested for anything other than small numbers of qubits.

This field of research is particularly well-regarded in the United States and is funded by the DARPA, the Pentagon's research department. A similar project has been set up in Europe: nine research groups have joined together to form the Quantum Information European Research Network. Nonetheless, according to Shor ([**31**]) it would be unreasonable to expect a quantum coprocessor to be developed within the next few years.

Should such a quantum computer ever exist, the public-key cryptography described in Section 5 would become obsolete. Nevertheless, there is a theory of quantum cryptography, more specifically of quantum key-sharing ([**1**], see [**2**] for a bibliography on the subject), which offers an alternative to public-key cryptography.

6.2 Quantum cryptography. The problems are similar to those described in 5.2: Alice and Bob once again wish to share a secret, which they can then use as a secret key for a symmetric protocol (such as AES). If they use only a telephone line, they have no choice but to employ public-key cryptography. If an attacker with a powerful quantum computer eavesdrops on their conversation, they are open to the attacks described earlier. However, if they can use an optical fibre to transmit quantum states, they can employ quantum cryptography. It can be designed in such a way that an attacker listening in on the conversation can capture only one 'bit' of the conversation at the most. Furthermore, any information that he does manage to capture will disturb the states, so Alice and

Bob will immediately know what is happening. All they would then have to do then is reject the states in question.

Although the theory dates back to 1982-84 ([**1**]), it was not put into practice until the 1990s. In 1990-92 IBM began an initial free-space experiment over a 30 cm length. In 1993-95 British Telecom conducted an experiment on optical fibres over a 10-30 km length. In 1996 Swiss Telekom conducted similar experiments on a 23 km fibre under Lake Leman. In 1997 Los Alamos National Lab successfully conducted the same experiments on a 48 km optical fibre, and in 1998 it conducted an experiment through free space over 1 km.

7. A technical interpretation of Category 5 of the Wassenaar Arrangement

7.1 The Wassenaar Arrangement. Acknowledging the end of the Cold War, on 16 November 1993 in The Hague representatives of the 17 member states of COCOM decided to abolish the committee and replace it with a body which reflected the new political developments. The decision to wind up COCOM was confirmed in Wassenaar (Netherlands) on 29-30 March 1994 and came into effect on 31 March 1994.

The foundations of the agreement on COCOM's successor were laid on 19 December 1995, once again in Wassenaar, and the inaugural meeting was held on 2-3 April 1996 in Vienna, which since then has become the site of the Permanent Representation of the Wassenaar Agreements.

The Arrangement concerns export controls for conventional arms and sensitive technological products. Participating countries are: Germany, Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Denmark, United States, Russian Federation, Finland, France, Spain, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Norway, New Zealand, the Netherlands, Poland, Portugal, Republic of Korea, Slovak Republic, Czech Republic, Romania, United Kingdom, Sweden, Switzerland, Turkey and Ukraine.

This list of 33 countries includes, in particular, those of the European Community and the signatories to the UKUSA agreement.

The Arrangement is open to those countries which fulfil certain criteria (see [**34**] for a full description) and decisions are based on consensus. Observers are not admitted.

As regards the security of information, some important amendments were made during the last meeting of the representatives of the signatory countries to the Arrangement on 2-3 December 1998 in Vienna ([**34**]). These amendments, of which we give a technical interpretation below, concern Category 5, part 2, entitled *Information Security.*

7.2 Category 5, part 2: Information Security. Part 5.A.2 stipulates in particular that controls are to be imposed on systems, equipment and components using the following (either directly or after modification):

1. a symmetric algorithm using a key longer than 56 bits; or
2. a public-key algorithm, in which the security of the algorithm is based on one of the following:
   (a) the factorisation of integers higher than 512 bits (e.g. RSA);
   (b) discrete log computations in the multiplicative group of a finite field larger than 512 bits;
   (c) discrete log computations in a group other than those mentioned above, and which is larger than 112 bits.

However (Note 5.A.2.d), cryptographic equipment specially designed and intended solely for use in machines for banking or money transactions is not subject to controls.

7.3 Comments. The gist of Point (1) is that unrestricted exports are authorised

only for those techniques which offer the same degree of security as DES. As explained in 4.3, this type of system offers a very limited degree of security. The techniques referred to in Point (2) were illustrated in 5.1. The main groups targeted in (2c) are those associated with elliptic curves. However, in actual fact (2c) covers a far vaster area, as it concerns all groups. It thus includes, *inter alia,* rational points of Abelian varieties over a fnite field (in particular elliptic curves, which are Abelian varieties of dimension 1), which are known (see 6.1) to be open to quantum cryptanalysis.
As stated in 5.1, according to current know-how elliptic curves over fixed-size fields offer equivalent security to that provided by RSA with far larger modules or with the discrete logarithm over a far larger finite field. In other words, (2a), (2b) and (2c) offer equivalent degrees of security, in that, on average, more or less the same effort is required to recover the secret data from the different algorithms. This explains the slight difference in size between (2a, 2b) and (2c). Moreover, as seen in 5.2, these public-key techniques are generally combined with secret-key cryptosystems.

7.4 Note. Watermark techniques are not included in the systems subject to controls. Such techniques, which are also known as data hiding or steganography, enable one piece of information to be hidden in another, e.g. a fax, photo, video or sound files. The hidden information generally protects the intellectual ownership of the data (see [**20**]), but nothing prevents users from hiding other things, such as a 128-bit key for a symmetric system, which the two correspondents have agreed on in advance (possibly via information that has been embedded in another document using a stenographic method). The state of the art is that documents which contain information hidden using steganographic techniques cannot – without special software - be distinguished from the original; moreover, the information can withstand numerous compressions/decompressions (necessary for the rapid transmission of such documents over the Internet) and can only be recovered by means of a special software product and a password. This technique is also very cheap. It seems that it is not therefore subject to export restrictions, but in practice it does allow confidential data to be exchanged. Likewise, the approach entitled 'Chaffing and Winnowing: Confidentiality without Encryption', developed by Professor Rivest, also enables a high degree of confidentiality to be achieved, whilst avoiding any entanglement with the Wassenaar Arrangement.

7.5 Impact on criminal organisations. It would be naïve to imagine that criminal or terrorist organisations conduct their business in compliance with international import/export rules, or that they do not have not the means to perfect highly confidential methods of communication. Algorithms do not stop at borders. Moreover, numerous algorithms are freely accessible. It is also difficult to see how the authorities could prove that a suspect binary sequence was created using an unauthorised system if, for example, it was actually created with a public-key cryptosystem using a 4096-bit module. Just because an intercepted binary sequence does not make sense, even if it has hypothetically used a 'lawful' cryptographic system (which can be ascertained, but at considerable cost), this does not mean that it has been created 'unlawfully' (which, above a certain level of sophistication, cannot be ascertained). Lastly, even if cryptographic products are subject to tight export controls, the fact remains that they are still freely used in many countries, including the United States. However, it does not appear that criminal or terrorist organisations operate only outside these countries; but neither do the authorities of these countries appear to lack effective means of investigation on their national territory.

7.6 Impact on the European Union. From a Community point of view, the consequences of the Wassenaar amendments are manifold.
Prior to the amendments, EU firms were free to conquer the data security market as long as the laws of their country of origin authorised them to do so. In particular, European firms in this sector could export solutions with a very high degree of security, the only restrictions being those imposed by national legislation (which could nevertheless be extremely tight, as in the case of France until recently).

Now, however, the only products that European data security firms are allowed to export without restriction are of a far lower quality.
By virtue of these amendments, at the time of publication of the agreement European data security firms, unlike their US counterparts, could not automatically realise economies of scale and target large markets. Even if, from the viewpoint of the Wassenaar Arrangement, they were on an equal footing with US firms, this apparent equality was deceptive and overall they were at a disadvantage.
Fortunately, bilateral agreements reached in Europe now allow European firms to sell high-quality solutions freely throughout the continent. However, this freedom ends abruptly at Europe's external borders.
But even if the use of cryptography is such as to prevent industrial espionage by bodies with limited financial clout, the Wassenaar Arrangement resolutions do not protect firms from all risks. In the light of the existence of the DES Cracker, it is not unreasonable to estimate that an institution with a USD 300 million budget could recover a 56-bit key within a few seconds. With the same budget, it would take a few tenthousandths of a second (see 2.4, where this is the maximum level of security provided by several GSM cellphones) to find a secret 40-bit key. Hence those firms, bodies or individuals that equip themselves with a cryptosystem which fulfils the criteria set out in 7.2 should be fully aware that the Echelon network is in all likelihood still able to intercept and decode their information.

8. Recommendations

It is our view that the recommendations (Section 4.5, p. 21-22) contained in the previous report [**35**] are still valid. Here, however, we seek to provide the European Parliament with some alternative solutions.

A.- Experts should be commissioned to provide updates on a regular basis, or as required, to the technical documents published by Community bodies. For example, it would be advisable to examine whether and to what extent the comments made in 5.4 (which are by no means exhaustive) have been taken into consideration; it would also be advisable to monitor the conferences on AES, IEEE-P1363 and P1363A concerning secret-key and public-key cryptography and the experimental developments with regard to quantum processors.

B. – Bearing in mind the legal risks run by European telephone industries (groups of users could be roused to action by the fact that the level of security provided does not systematically correspond to the level claimed), European bodies should encourage European telephone operators to:

- update their implementation of the COMP128 authentication algorithm;
- clearly specify the actual level of security of their implementation of the encryption algorithm A5.

C – In view of the fact that the NSA has managed to bring about a considerable reduction in the degree of security offered to non-US users of solutions developed by Microsoft, Netscape and Lotus for encrypting electronic messages, with the express intention of being systematically able to read the messages exchanged by these users (and probably being the only agency in the world able to do so), the European Parliament should actively promote the use, amongst European organisations, firms and citizens, of e-mail encrypting solutions that actually provide the confidentiality promised. At the same time, Proposal 5 of the 'Policy issues for the European Parliament' contained in the STOA IC 2000 report by Duncan Campbell should be taken into consideration.

D. – In view of:

- the launch of the worldwide advertising campaign for the PSN*-equipped Pentium III by the market leader (80%+) for PC chips,
- the risks of the PSN being used for electronic surveillance purposes,
- the concern shown by the highest US authorities with regard to this precise subject (see the declaration [**15**] made on 25 January 1999 by Mr Al Gore, Vice-President of the United States),
- the risk that PSNs may be cloned and be unsuitable for e-commerce, hence the risk that this new industry may be held back, particularly in Europe,

the relevant committees of the European Parliament should:

- call on American government agencies, including the NSA and FBI, to provide information on their role in the creation of the PSN developed by Intel,
- at the same time commission a group of independent technical experts to conduct a precise assessment of the risks connected to this product: electronic surveillance, PSN falsification, etc. The group should issue its report as soon as possible.

Building on the initial results of the above, if appropriate, the relevant committees of the European Parliament, should be asked to consider legal measures to prevent PSN-equipped (or PSN-equivalent) chips from being installed in the computers of European citizens, firms and organisations. We wish to underline most strongly that the above suggestions have no connection whatsoever with any particular firm, but are motivated purely by the characteristics of a product which, unless rapid action is taken at Community level, may become a de facto industrial standard in Europe within the next few months.

E. – As regards Category 5, Part 2 of the Wassenaar Arrangement, dealt with in Section 7 of this report, the following should be noted:

- Since high-security secret-key and public-key algorithms are freely accessible, for example via the Internet, and in view of Note 7.4 and the implications of such accessibility (see 7.5), it appears that export restrictions in no way constitute a serious impediment for criminal and terrorist organisations. Nevertheless, by following the example of the United States the police can take effective action, even when top-quality cryptographic products are freely used.
- However, in the light of 7.6, such export restrictions pose a serious obstacle to European data security firms and hinder the development of the international
e-commerce industry.
- On 19 January 1999, following the inter-ministerial committee meeting on the information society ([**5**]), the French Government, in agreement with President Chirac, pledged to liberalise the use of cryptography by raising from 40 bits to 128 bits the security threshold which may be freely used. This latest development is apparently only the first step towards a total deregulation of the use of cryptography on French territory. Until then, French rules on cryptography had been among the most stringent in the world.
- The Echelon network is most probably able to intercept, decode and process the information transmitted with products on the market that fulfil the criteria mentioned in 7.2.

In order to strengthen Community cohesion, the European Parliament should strive initially to persuade EU countries to adopt a common position at the meetings organised under the Wassenaar Arrangement. Subsequently, in view of the aforementioned points, and in order to boost electronic commerce on a worldwide scale, it should suggest that the Community simply with from Category 5, Part 2 of the list of products subject to controls under the Wassenaar Arrangement.

F. – The committee should commission a more detailed report on the implications

* Processor Serial Number

of the risks in terms of electronic surveillance that the Wassenaar Arrangement brings with it. For example, under Item 5.B.1.b.1 (Part 1, on Telecommunications) certain equipment using ATM (Asynchronous Transfer Mode) digital techniques is subject to controls. This data transfer technology is far more difficult (but not impossible, see [**32**], part 2, and the aforementioned STOA report by Duncan Campbell) to monitor electronically than conventional TCP/IP systems. It would also be very useful to ascertain whether products that are authorised for export provide effective responses to TEMPEST (see 2.7 and introduction to point 3), since the usefulness of cryptosystems is somewhat limited if the data can be read in plaintext before encryption or after decryption, with the aid of electromagnetic radiation.

Bibliographie

1 *C. H. Bennett, G. Brassard :* Quantum cryptography: public key distribution and coin tossing. In Proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (1984).

2 *G. Brassard :* Quantum cryptography: a bibliography. SIGACT News 24:3 (1993). Une version plus récente est accessible online à http://www.iro.umontreal.ca/crepeau/Biblio-QC.html

3 *cAESar Project :* http://www.dice.ucl.ac.be/crypto/CAESAR/caesar.html

4 *J. I. Ciriac, P. Zoller :* Quantum computations with cold trapped ions. Phys. Rev. Lett. **74**, p. 4091-4094 (1995)

5 *Comité interministériel pour la société de l'information, conférence de presse de Mr. Lionel Jospin, Premier Ministre :* http://www.premier-ministre.gouv.fr/PM/D190199.HTM
Voir les decrets No. 99-199, 99-200 du 17 mars 1999, ainsi que l'arrete du 17 mars 1999 (Journal Officiel Numero 66 du 19 mars 1999)

6 *D. G. Cory, A. F. Fahmy, T. F. Havel :* Ensemble quantum computing by nuclear magnetic resonance spectroscopy. Proc. Nat. Acad. Sci. **94**, p. 1634-1639 (1997)

7 *H. Dobbertin, A. Bosselaers, B. Preneel* : RIPEMD-160: a strengthened version of RIPEMD. D. Gollmann, editor, Fast Software Encryption, Third International Workshop, Lecture Notes in Computer Science **1039** (1996). Une version corrigee et acutalisee est accessible online: http://www.esat.kuleuven.ac.be/bosselae/ripemd160.html

8 *Echelon : une liste de liens :* http://www.saar.de/bong/archiv/echelon.html, http://serendipity.nofadz.com/hermetic/crypto/echelon/echelon.htm, http://serendipity.nofadz.com/hermetic/crypto/echelon/nzh1.htm, http://www.telegraph.co.uk/et?ac=000602131144806&rtmo=0sksx2bq&atmo=0sksx2bq&pg=/et/97/12/16/ecspy16.html, http://www.freecongress.org/ctp/echelon.html, http://www.disinfo.com/ci/dirty/cidirtyprojectechelon.html, http://www.dis.org/erehwon/spookwords.html (spookwords)

9 *N. A. Gershenfeld, I. L. Chuang :* Bulk spin resonance quantum computation, Science **275**, p. 350-356

(1997)

10 *Electronic Frontier Foundation :* Cracking DES, Secrets of Encryption Research. Wiretap Politics & Chip Design, O'Reilly (1998)

11 *J. Dj. Goli● :* Cryptanalysis of alleged A5 stream cipher. In Advances in Cryptology, Eurocrypt'97, Lecture Notes in Computer Science **1233**, Springer-Verlag Berlin Heidelberg New York, p. 239-256 (1997)

12 *European Commission - Directorate General XIII :* Communication from the commission to the European Parliament, the council, the economic and social committee and the committee of the regions ensuring security and trust in electronic communication (COM 97-503). Egalement accessible online : http://www.ispo.cec.be/eif/policy/97503toc.html

13 *European Telecommunications Standards Institute (ETSI) :* http://www.etsi.fr/

14:*FIPS PUB 180-1* : Secure Hash Standard, Federal Information Processing Standards Publication 186, US Department of Commerce, National Institute of Standards and Technology, National Technical Information Service, Springfield, Virginia (1994). Accessible online sous: http://www.itl.nist.gov/div897/pubs/fips180-1.htm

15 *A. Gore, Vice-Président des Etats-Unis :* Interview au San Jose Mercury News (25/1/1999)

16 *IEEE-P1363 :* http://grouper.ieee.org/groups/1363/index.html

17 *IETF-PKIX, Public-Key Infrastructure (X.509) :* http://www.ietf.org/html.charters/pkix-charter.html

18 *IETF-S/MIME, Mail Security (smime) :* http://www.ietf.org/html.charters/smime-charter.html

19 *B. E. Kane :* A silicon-based nuclear spin quantum computer. Nature **393**, p. 133-137 (1998)

20 *M. Kutter, F. Leprévost :* Symbiose von Kryptographie und digitalen Wasserzeichen: effizienter Schutz des Urheberrechtes digitaler Medien. A paraître in Tagungsband des 6. Deutschen IT-Sicherheitskongresses des BSI (1999)

21 *F. Leprévost :* Les standards cryptographiques du XXI-eme siecle : AES et IEEE-P1363. A paraitre in *La Gazette des Mathématiciens* (1999)

22 *F. Leprévost :* Peter W. Shor, prix Nevanlinna 1998. A paraitre in *La Gazette des Mathématiciens* (1999).

23 *F. Leprévost :* AES und IEEE-P1363, die kryptographischen Standards des 21. Jahrhunderts. A paraitre in Tagungsband des 6. Deutschen IT-Sicherheitskongresses des BSI (1999)

24 *NIST AES Home Page :* http://csrc.nist.gov/encryption/aes/aes_home.htm

25 *NSA Tempest Documents :* NACSIM 5000, 5004, 5100A, 5201, 5203

26 *Ch. Persson :* Pentium III serial number is soft switchable after all. In c't Magazin für Computer Technik (1999)

27 *PricewaterhouseCoopers Investigations LLC :* The Corporate Netspionnage Crisis. Informations accessibles online : http://www.pricewaterhousecoopers.fm/extweb/ncpressrelease.nsf/DocID/B81092772821633B8525673C006AFA91

28 *Smartcard Developper Association :* http://www.scard.org/

29 *P. W. Shor :* Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal of Computing **26**, p. 1484-1509 (1997)

30 *P. W. Shor :* Quantum Computing. Proceedings of the International Congress of Mathematicians, Berlin, Documenta Mathematica, Journal der Deutschen Mathematiker-Vereinigung (1998)

31 *P. W. Shor :* Communication personnelle (1998)

32 *U.S. Congress, Office of Technology Assessment :* Electronic Surveillance in a Digital Age. OTA-BP-ITC-149, Washington, DC: U.S. Government Printing Office (July 1995)

33 *D. Wagner :* Communication personnelle (1999)

34 *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies :* http://www.wassenaar.org/

35 *S. Wright :* An appraisal of technologies of political control. Interim Study for the STOA (19/1/1998)