What is going on in the world of cryptography?

Jaroslav Pinkava, AEC Ltd. Brno, Czech Republic

Introduction

The importance of cryptography in today's digital communications is no doubt growing. The role of cryptography is unreplaceable. Cryptography is fulfilling a set of basic objectives (goals): secrecy, authentication, data integrity, non-repudiation etc. For this purposes there exists a whole array of corresponding security tools: cryptographic algorithms, digital signatures, cryptographic protocols, time stamping and other.

The contours of cryptography are nowadays formed mostly through the development of many standards and common recommendations. The present objective of cryptography is not only some method of ciphering, digital signing or confidential communication. In the privacy game are now participating whole large networks with an enormous number of individual users (the influence of Internet is not to be overlooked). It is necessary to build up the means for private communication in such environments, where it is in principle inevitable for any two participants to establish a secure private link. To allow this, the means of secure data transport, the means of authentication must be in some way unified. This is the basic aim of creating various cryptographic standards and recommen-dations. Currently, there exist quite a lot of such standards. Why are there so many and what are they describing?

The basic cryptographic standards are of course about ciphering algorithms as such, both symmetric and public key algorithms. The concept of digital certificate is now startingto be commonly deployed and its precisation is a part of the adequate standards (X.509). The Digital Signature Law is accepted, or being prepared for (depends on individual countries). It is necessary to develop the corresponding means providing the actual security to the functionality of a secure electronic commerce – there exists a whole assemble of respective initiatives in this area. The architecture of the Internet alone (OSI Reference Model - seven layers) leads to different concepts of secure data transmission on various layers. Financial institutions are developing own standards (ANSI, ISO). There exists a nice overview of such standards for example in [4].

Symmetric cryptography

The era of DES is over, a new standard called FIPS-46-3 was issued at the beginning of this year (1999). In this standard DES was replaced by the 3-DES algorithm (in fact this algorithm had already been in use). Entrust published the CAST algorithm (with 128-bit key) and gave a permission for its free use.

The American government institution for standards (NIST) is continuing the preparation of a completely new standard for symmetric ciphering algorithm – Advanced Encryption Standard (AES). This algorithm (maybe algorithms) has a different block size (compared to today's block cipher algorithms), it works with keys in the length of 128 bits. The reason for this action is obvious – the mankind computing power is beginning to get near the number of all possible 2^{64} input blocks and in some situations it would be possible to constitute a complete vocabulary (all pairs open text + cipher text for the unknown key).

The AES algorithm is mandatory designed for the three lengths of key (128, 192 and 256 bits). In August 1998 the names of 15 candidates to participate in the AES activity were announced. The second AES conference in Rome in March of 1999 was dedicated to analysing the cryptographic and implementation properties of this algorithm. On the basis of this conference analysis and received recommendations NIST has chosen five finalists. Their names were announced in August 1999.

There was: **MARS** (IBM), **RC6** (RSA Laboratories), **Rijndael** (Belgian cryptographers Daemen, Rijmen), **Serpent** (Anderson, Biham, Knudsen), **Twofish** (Bruce Schneier).

A third AES conference will be held in April 2000. The aim of this conference is to analyse these five finalist algorithms. Based on the results of this conference, one (or more) algorithm will be chosen, which then will be processed as the proposed NIST standard. It is expected that the new standard will be known in the summer of 2001.

Asymmetric Cryptography

Also the effort of the IEEE P1363 group got in the final phase. This group did a lot of work preparing the asymmetric cryptography standards. Thorough description and utilisation methods were elaborated for the following public key systems: RSA, Rabin-Williams, cryptosystems based on the problem of a discrete logarithm and cryptosystems exploiting elliptic curves. At present, there is a common consensus on understanding asymmetric cryptography as the system for:

a) key exchange (for secret keys of symmetric cryptography),

b) digital signature,

c) encryption (most of all for short messages mainly of service character).

In particular, the elliptic curve cryptosystems are considered to be a very perspective variety of public key cryptography. The relatively short key length of these cryptosystems is their main advantage. There exist a rich variability of the selection of a particular set of parameters. This is, in principle, an advantage, but for implementation it is necessary to follow the unified principles (individual users must have an access to a common cryptosystem with defined parameters, the only variables are the private and public keys). This is one of the reasons for the establishment of the SECG workgroup. The basic objective of this workgroup is to create a unified platform for an „effective“ elliptic cryptography. This is reached by specifying public key cryptography schemes and by introducing recommended elliptic curve parameters. And the US government is following: in May 1999 a document was issued specifying selected sets of parameters for elliptic curves. These parameters are recommended for use in US governmental institutions.

And what about cryptanalysis?

In the last one or two years, several results in the field of the cryptanalysis was of course also obtained. With the exception of DES and A5 (GSM) algorithms, these results are related not only to encryption algorithms, but mainly to the ways in which the algorithms are implemented (cryptographic protocols, the physical characteristics of algorithms implementations).

PKCS 1

The PKCS standards developed by the RSA Laboratories are well-known and frequently used specifications for particular cryptography solutions. In these standards there is described, for example, a syntaxis of cryptographic message, ways for implementing some public key cryptosystems, formation and elaboration of digital certificates, manipulating with keys, passwords etc. In August 1998 on the CRYPTO conference in Santa Barbara Daniel Bleichenbacher (Bell Laboratories) introduced a new attack on PKCS 1 (this standard describes encryption and digital signature generated by the RSA algorithm). The attack essence is in the possibility of sending a huge amount of messages (for example to an automatically responding server) with the goal to get the open text for the one defined ciphertext encrypted by RSA algorithm. Analysis of the responses to these messages then allow with mathematical techniques to get a considered open text. In the given situation the attacker can get only one defined open text, not the RSA algorithm key. But when this open text is the secret key for symmetric cryptography, then the described process results in extracting all the messages encrypted with this secret key. For the functionality of such a kind of an attack there must exist a possibility to get same information from the designed victim (an answer that the sent message is/is not valid is sufficient). Some of used cryptographic protocols allow this. This is, for example, the case of most of the SSL protocol variants, which were originated before publication of this attack. Smart Cards, if the attacker can use his own equipment, are also vulnerable by these means.

At present, a new variant of PKCS 1 is valid, in which the described possibilities for the attacker are eliminated. But what is performed for the common standards (the correction of holes) may not be corrected in the existing version in praxis. The users of the SSL should know what is the version of SSL used.

Remark: On the last Crypto conference (August 1999) was presented a new attack on the RSA signature, at the rump session Shai Halevi give a succesful signature forgery attack on ISO/IEC 9796-1. The attack is estimated to take 3000 chosen messages for a 1024-bit modulus, and results in a forged signature.

DES – Cracker

The cryptographers had been warning about this for a long time and latterly it was realised. The DES algorithm is not secure for the reason of an unsatisfactory key length (56 bits is not enough for today’s computers). On 17. July 1998 the Electronic Frontier Foundation announced the construction of a hardware unit, which is designed for breaking DES. The equipment worth 220 thousand of US dollars can determine the key of DES algorithm in 100 hours in average.

Then finally followed (and here the word finally is reasonable) the reaction of American official institutions. After twenty one years of its existence (1977), the DES standard was replaced by an algorithm with a substantially longer key (at minimum twice so long). The solution is evidently provisional (waiting for AES), but the revised 3-DES algorithm is undoubtedly a more secure way to data protection.

The Side-channels

There has been an enhanced attention in the last years to the so called side-channel attacks. For example Paul Kocher has demonstrated the possibilities of a timing attack introduced by him. By exact measurement of the length of time intervals, when varied cryptographic operations are executed, there exists a possibility of breaking some implementations of cryptographic algorithms. Basically this does not depend on the type of the algorithm. Analogue results were achieved by the same author with power consumption analysis. With these methods it is possible to extract a hidden key for example from a Smart Card.

The radiation characteristics are a similar leaking channel (the Smart Cards are by this method vulnerable too). If the used methods are accompanied with forced faults (so called fault-analysis), then for the potential attacker there exist many ways to get the access to confidential information.

When seeking an adequate defence from the above-described attacks, it is more effective to think about the construction of a whole security system rather than to improve partial physical characteristics of the system. This way can be at least very expensive and the effect may be minimal. The change of a security conception may lead to a more complex security system, but the target system security characteristics can be much better.

Why a good cryptography is needed?

Let's look first at one of the current very perspective area – electronic commerce. Automation of operations – this is the main reason for a principally higher effectiveness of electronic commerce systems when compared the classical „paper" systems. On the other hand, this is also the purpose of existence of new vulnerabilities. The attacker can now be at a long distance from the designated victim of his attack, and when he is succeeded then there exists no reason to think that he will not succeed next time.

A large hole in a security system can then lead to a bankrupt of a whole company during only one day. If an unsatisfactory security system is used for several years without any problems, it does not mean that the next day this will be enough. A more clever attacker can come and the company is over. A favourable electronic security system must be constructed with respect to a future attacker, it must be reasonable secure with respect to the attackers more skilful then the today's ones are.

What can we tell about the contemporary cryptographic systems existing on the market? Very often these systems are constructed by engineers (maybe very well educated engineers), but without co-operation with cryptographers. Cryptography is reduced to only one of the system components. Naturally, cryptology is primarily the science about vulnerability. And this is often forgotten. A whole system is as secure as its most fragile part. An encryption algorithm of a super quality cannot save us, if the key generation and management techniques are not of a satisfactory level.

Well-known is for example the following security hole during network login: Passwords used for individual user login are on the network in an open form. Minimally equipped hacker can get these passwords and no other means (authentication, encryption) can then block the attacker's access to all local network resources.

At the present we have possibilities to construct very good cryptographic algorithms. However, the practical cryptography needs more. It is the secure implementation of this algorithms, it is the consideration of many related problems, as key management with all its aspects (key exchange protocols, digital certificate elaboration, digital signatures, etc.), as all authentication means and protocols and the global system security overview. The use and support of the existing array of security standards is in current data protection systems unavoidable.

Literature

[1] C. Hall, I. Goldberg, and B. Schneier, Reaction Attacks Against Several Public-Key Cryptosystems, Counterpane Systems Report, 1998.

[2] Paul Kocher: Cryptanalysis of Diffie-Hellman, RSA, DSS, and Other Systems Using Timing Attack, December 1995, 6 pp.

[3] Paul Kocher: Differential Power Analysis, http://www.cryptography.com/dpa/index.html

[4] Alfred J. Menezes, Paul C. van Oorschoot, Scott A. Vanstone: Handbook of Applied Cryptography, CRC Press 1997, 780 pp.

[5] Bruce Schneier: Crypto-Gram, http://www.counterpane.com/

[6] Richard E. Smith: Internet Cryptography, Addison-Wesley 1998, 356 pp.