The Science of Cryptology

A section from the book *UMTS Security* by Valtteri Niemi and Kaisa Nyberg, to appear in November 2003, published by Wiley@Co.

Cryptographic systems

Cryptology is the science of information security and privacy. Mathematical techniques are investigated and developed to provide authenticity confidentiality, integrity and other security services for information that is communicated, stored or processed in an information system. Also the strength of cryptographic designs and protocols are evaluated from the point of view of mathematics, systems theory and complexity theory.

The design part of the science is called *cryptography*, while the security investigations and analysis is known as *cryptanalysis*. The naming convention reflects the two sides of the science of cryptology. This division is also apparent in the practical cryptographic development work, where the best practise has become to split the development resources into two teams. The team of cryptographers make proposals for cryptographic designs, which the team of cryptanalysts try to break.

A cryptographic system in its basic form is often depicted as a *communication system* involving three entities. Two of the entities are exchanging messages over an insecure communication channel. It has become customary to call these entities Alice and Bob. The third entity has access to the communication channel. She is called Carol, as the third letter to the alphabet, or Eve, as the *eavesdropper*. But Eve is allowed to perform all kind of malicious actions on the communicated messages, not just passive eavesdropping. All parties are also assumed to have certain computation resources. Different theoretical models vary a lot with respect to the amount computation resources the entities have and what kind of tampering Eve is performing on the communication channel.

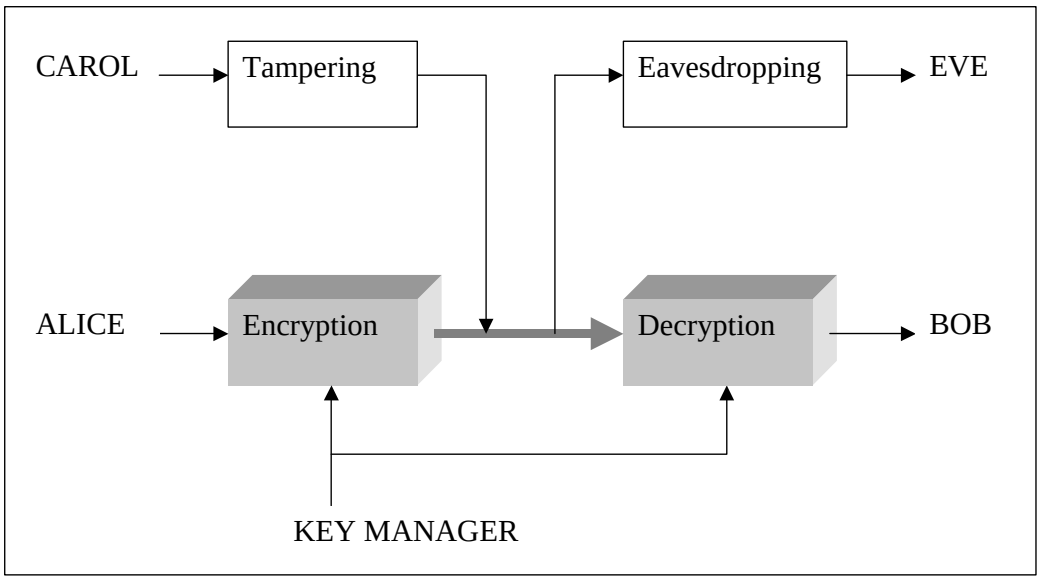

Figure 1 Cryptographic system

The goal of cryptography is to secure the communication of Alice and Bob over the insecure channel. A cryptographic system is typically given as a family of *cryptographic functions*, parameterised using a cryptographic value called the *key*. The functions may be *invertible* or *non-invertible*. Invertible functions are needed to protect the confidentiality of the messages. The cleartext message (*plaintext*) is encrypted by the sender entity Alice using the function. The encrypted message (*ciphertext*) is then sent over the channel to the receiving entity Bob. Bob decrypts the ciphertext using the inverse function. Non-invertible functions are only computed in one direction and are useful in protecting

integrity of the messages. Examples of cryptographic schemes using non-invertible functions are *message authentication codes*.

The description of the cryptographic system can be made public, and even known to Eve. The security of a cryptographic system shall not depend on the secrecy of the system. Hence cryptographic algorithms can be published, distributed and sold as commercial products. The users of the cryptographic system, Alice and Bob, are required to keep secret only the knowledge of the actual function they are using. They indicate their selection to the system by giving the system the key, the value of the cryptographic parameter. To the outsiders, to Eve and Carol, the selection of the shared secret of Alice and Bob must be unpredictable to provide full uncertainty of the function Alice and Bob are using. Hence there is no secrecy without uncertainty. Uncertainty is created by randomness. Cryptology investigates how randomness can be efficiently used to protect information. The main challenge of the management of cryptographic keys is to provide unpredictable keys to the users of the cryptosystem. The requirement of unpredictability has often been underestimated in practise, or has been traded off for other requirements. Cryptographic keys derived from human memorable poems or generated using pieces of literature at hand, have often turned out to be fatal. A lively description of various aspects of hardship "between silk and cyanide" involved in the generation, management, and use of cryptographic keys is given by Leo Marks in [5].

The science of cryptanalysis has identified a number of ways Eve or Carol can use to *attack* the cryptosystem. Also the goals of the attacks vary. Eve may just want to eavesdrop, while Carol may want to forge the messages and eventually create a triangle affair [1]. Eve is using *ciphertext only*, while Carol may be using *chosen ciphertext*. The ultimate goal is to find the secret key, since it would mean a total break to the cryptographic system of Alice and Bob. More precisely, an occasional compromise of one key used by Alice and Bob would not ruin the system. Alice and Bob need just change to a new key and take a better care of it. A cryptosystem is considered totally broken if there exists an efficient method using which the key can be systematically derived from the practically available information with non-negligible probability.

Security and vulnerability

Before the revolution in information technology caused by computers, that is, still at the time of the World War II, the professional research and development of cryptography was a privileged activity of military and intelligence agencies. Primer level textbooks were published explaining the basic principles of classical cryptosystems and their cryptanalysis. Such material is still often included as an introductory chapter in modern cryptographic textbooks [12]. More serious cryptology was a carefully protected proprietary knowledge. The first trustworthy and detailed accounts about the cryptanalysis of the German Enigma cipher were not published until late 1970's. The extensive British cryptanalytic activity during the World War II that took place in Bletchley Park, an unspectacular small village between the university towns of Oxford and Cambridge, remained a well-kept secret as long as thirty years after the activity was closed at the end of the war.

Cryptographic technology has not lost its importance as a means of national security. Neither have intelligence organisations lost their interest in cryptologic research. The cryptographic methods and the devices carrying such methods are considered as warfare, whence the use and export of cryptographic methods is controlled. Governments of 33 industrial countries participate in the Wassenaar Arrangement on export controls for conventional arms and dual-use goods and technologies [13]. The purpose of this arrangement is to prevent proliferation of strong arms technology to the governments of less stable countries. The strength of cryptographic systems is measured by their key sizes. There has been some more pressure to increase the control of the use of cryptography in the aftermath of September 11th, where it has been claimed that the attackers used encrypted email for their communication. The New York Times interviewed inventors of modern cryptography, among others the Stanford professor M. E. Hellman, asking the impossible question, whether they had refrained from publishing their inventions, most of which date back to the 1970s, if they knew then to which extent their inventions can be misused to serve malicious goals [3]. To this respect cryptography shares the dilemma of the modern technology, how to exploit the best part of it without creating new vulnerabilities.

Development of cryptology to a public science

The first modern scientific treatment of cryptology was published in 1949. It was a comprehensive paper by Claude Shannon, where he presented the theoretical framework of what he called the *secrecy systems* [11]. A previous paper on mathematical theory of communication [10], published the year before, was a seminal work that laid the foundations of modern information theory in the terms of bits, and started a growing and successful research activity in this field soon after it was published. The second paper did not result in any upsurge in open cryptologic research. Indeed, it took 27 years before anything significant happened. James Massey considered the reasons for this in his very readable survey paper on principles of contemporary cryptology [6] as follows:

> First, the theory of theoretical security of secrecy systems that it provided was virtually complete in itself, and showed conclusively that theoretically-secure secrecy systems demand the secure transfer of far more secret key than is generally practicable. Moreover, the insights that Shannon provided into the practical security of secrecy systems tended to reinforce accepted cryptographic approaches rather than to suggest new ones. But Shannon's observation that "The problem of good cipher design is essentially one of finding difficult problems, subject to certain other conditions…. We may construct our cipher in such a way that breaking it is equivalent to (or requires at some point in the process) the solution of some problems known to be laborious" took root in the fertile imaginations of the Stanford cryptologic researchers, W. Diffie and M.E. Hellman. The fruit was their 1976 paper "New Directions in Cryptography" that stunned the cryptologic world with the startling news that *practically-secure secrecy systems can be built that require no secure transfer of any secret key whatsoever*.

Hence there was no public research activity in about a quarter of a century, while within the closed organisations the research went on by experts developing encryption machinery and analysing wiretapped encrypted communication traffic. In most countries the use of cryptography and cryptographic equipment was subject to license, and was limited to securing internal communication of governments. During the cold war mathematicians developed encryption systems, but they were not presented in public. Results of mathematical research were withheld from publication if they were considered applicable to cryptography. For example, O. Rothaus discovered mathematical objects he named as bent functions in the 1960's, but the paper did not appear until 1976 [9]. In addition to encryption technology, where they are used in highly nonlinear constructions, bent functions found by Rothaus have applications in spread spectrum technology, which was developed first for military radio communication, and became later the radio technology of UMTS. The coding sequences that are used to effectively spread the radio channels over the spectrum are based on bent functions and similar mathematical constructions. Still in late 1970's researchers of the Massachusetts Institute of Technology (MIT) were forbidden to publish their results based on the export control of conventional arms [4].

In Shannon's secrecy systems the enemy, that is, the cryptanalyst, has access to the encrypted message. The enemy is also assumed to have detailed knowledge of the used cryptosystem, which defines the family of cryptographic functions that constitute the cryptosystem. This principle is named as Kerchoff's principle after a Dutch linguist A. Kerchoff (1835-1903). The secrecy of the system is based solely of the secrecy of the key. Kerchoff's principle does not imply that only a public cryptosystem can be secure. Keeping the details of a cryptographic system secret adds another hurdle to the malicious efforts of breaking the protection it is supposed to offer.

The requirement of publishing all details of cryptographic systems is justified in large public systems, such as contemporary digital computer and communication networks. The security features must be thoroughly scrutinised using well-founded scientific and engineering principles. Opening the details of cryptographic systems to public analysis proves that the designers have tried their best to make the system as robust as possible, in particular, that no secret trapdoors that purposefully weaken the security are hidden in the system.

The first design effort for a public cryptographic method was launched in 1973 in the United States when the National Bureau of Standards made an open call for an encryption algorithm suitable for data

protection in commercial and banking communication networks and data bases. It took four years before the Data Encryption Standard (DES) was published in January 1977. The DES is a conventional algorithm based on Shannon's principles and the cryptographic experience of IBM and NSA experts. The publication of the DES algorithm took place within a year from the publication of revolutionary paper of Diffie and Hellman. These two events became the starting points of modern cryptologic research. Ever since the DES algorithm has been an inextinguishable source of cryptologic research material in the field of symmetric, or conventional cryptography, while the work of Diffie and Hellman opened up to new and unconventional directions of public key cryptography.

While the scope of cryptologic research became wider, also the range of various security services provided by cryptographic applications started to grow rapidly from the traditional protection of message confidentiality to the authentication of communication entities as well as protection of data integrity. The formal concept of cryptographic one-way function was created. The first known examples of practical systems using one-way functions for authentication purposes date back to 1950's. These *Identification Friend or Foe* (IFF) methods were used for authentication between military aircrafts [2]. In early 1970's the first applications of one-way functions, although not yet called by that name, were made to protect password tables in computer servers [14]. Essentially the same paradigm is used by the GSM and UMTS specifications for subscriber authentication in modern mobile communication systems.

The scientific activity in cryptologic research is strong and successful. The *International Association of Cryptologic Research* (IACR), founded in 1982, organises three major conferences each year in the United States, Europe and Asia or Australia. In addition it supports organisation of smaller specialised workshops, such as the annual workshop on Fast Software Encryption and publishes a scientific journal, Journal of Cryptology. The conference and workshop proceedings and the journal published by the IACR constitute the main body of the scientific cryptologic literature.

Public cryptographic development efforts

In addition to the scientific research the public international development and research efforts contribute significantly to the general knowledge and understanding of the security and performance requirements of modern cryptographic systems. The development and analysis of cryptographic algorithms for the 3GPP UMTS benefited significantly from two such projects: the *Advanced Encryption Standard* (AES) programme by NIST and the European NESSIE (*New European Schemes for Signatures, Integrity, and Encryption*) project.

The overall goal of the AES programme was to develop a *Federal Information Processing Standard* (FIPS) that specifies an encryption algorithm capable of protecting sensitive government information well into the twenty-first century. The algorithm was expected to be used by the U.S. Government and, on a voluntary basis, by the private sector. The initial announcement of the open AES competition was published on January 2nd 1997. The AES development and evaluation process took four years. The documentation is available at the AES home page [8]. After the first round, five candidates were selected to the second round, from which the Rijndael cipher by two Belgian cryptographers and with 128-bit block and three different key sizes was selected as the winner of the competition in September 2000. The 3GPP MILENAGE algorithm makes use of the AES algorithm as its "cryptographic engine".

The NESSIE project was a three- year 2000–2003 project within the Fifth Framework of the European IST Programme [7]:

> The main objective of the project is to put forward a portfolio of strong cryptographic primitives that has been obtained after an open call and been evaluated using a transparent and open process. The project intends to contribute to the final phase of the AES block cipher standardisation process (organised by NIST, US), but will also launch an independent open call for a broad set of primitives providing confidentiality, data integrity, and authentication. These primitives include block ciphers, stream ciphers, hash functions, MAC algorithms, digital signature schemes, and public-key encryption schemes. The project will develop an evaluation methodology (both for security and performance evaluation) and a software

toolbox to support the evaluation. The project goal is to widely disseminate the project results and to build consensus based on these results by using the appropriate fora (a project industry board, 5th Framework programme, and various standardisation bodies). A final objective is to maintain the strong position of European research while strengthening the position of European industry in cryptography.

The block cipher algorithm MISTY1 is one of the NESSIE candidates, and has been extensively evaluated by the NESSIE project. Since many attacks of MISTY1 may also be relevant to 3GPP KASUMI, and the other way round, the extensive analysis performed by the NESSIE project on MISTY1 has also consolidated the position of KASUMI as a secure cryptographic primitive.

References

[1] M. Burmester, On the risk of opening distributed keys. In: Y. Desmedt (Ed.) *Advances in Cryptology – Crypto'94*, Lecture Notes in Computer Science 839, Springer-Verlag 1994, 308-317.

[2] Whitfield Diffie, The First Ten Years of Public Key Cryptology. *Proceedings of the IEEE,*76 (1988), 560-577.

[3] Gina Kolata, When science inadvertently aids an enemy, *New York Times*, September 25, 2001.

[4] Susan Landau, Communications Security for the Twenty-first Century: The Advanced Encryption Standard. *Notices of the AMS*, 47 (2000), 450-459.

[5] Leo Marks, *Between Silk and Cyanide.* Harper Collins Publisher, 2000.

[6] James Massey, An Introduction to Contemporary Cryptology. *Proceedings of the IEEE,* 76 (1988), 533-549.

[7] NESSIE, Project Home page: https://www.cosic.esat.kuleuven.ac.be/nessie/

[8] NIST AES Home page: http://csrc.nist.gov/CryptoToolkit/aes/

[9] O. S. Rothaus, On "bent" functions. *Journal of Combinatorial Theory,* Series A, Vol. 20, 1976, 300-305.

[10] Claude Shannon, A Mathematical Theory of Communication. *Bell Syst. Tech. J.*, 27 (1948), 379-423, 623-656.

[11] Claude Shannon, Communication Theory of Secrecy Systems. *Bell Syst. Tech. J.*, 28 (1949), 656-715.

[12] D. Stinson, *Cryptography, Theory and Practise*. Second Edition, Chapman&Hall/CRC, 2002

[13] Wassenaar Arrangement, December 2002, http://www.wassenaar.org/

[14] M. V. Wilkes, *Time-Sharing Computer Systems*. Second edition, American Elsevier, New York, 1972.