A SHORT REVIEW OF DATA ENCRYPTION SYSTEMS

Raicea Gabriela, *Roşia de Amaradia* Technological High School, ROMANIA

SUMMARY: The present article proposes a short review of data encryption systems, of their history and basic elements, and also presents a comparison between symmetrical and asymmetrical encryption systems used to secure data transfer over networks of computers or the Internet.

KEYWORDS: encryption, decryption, cryptology, DES, AES, digital signature

1. INTRODUCTION

The name of cipher comes from the Arab word sifr, and nowadays 9th century Arab scientist al-Kindi is credited with the first book on cryptology **[1]**. Even before, there were primitive ciphers used by the ancient Egyptians; the Greeks were using transposition in 5th century B.C. and Julius Caesar used a substitution cipher (Caesar cipher).

Leon Battista Alberti described a cipher disk in his 15th century De cifris, using a polyalphabetic substitution, a machine complicated for that time **[2]**.

Giovan Battista Bellaso's cipher (1553), erroneously attributed later to Blaise de Vigenère, a simpler form of the polyalphabetic ciper, resisted breaking for three centuries, earning the title of *"*le chiffre indéchiffrable*"*, the unbreakable cipher.

Maybe some of the most famous cipher machines – and attempts to break them – were used in the Second World War by the Germans. They became known as the Enigma machines. The first Enigma machine was invented by Arthur Scherbius at the end of the First World War. At the outbreak of the second world conflagration, the Enigma machines were in use and providing an extremely strong defense of the German military information system. Brilliant Polish cryptologists (Rejewski, Zygalski, Rozicki), first managed to break the Enigma, using inside information. Subsequent work in breaking the frequently changed codes is attributed to renowned scientists Alan Turing and Gordon Welchman, at Bletchley Park.

Modern cryptography arose with Claude Shannon, in his article, "Communication Theory of Secrecy Systems" (1949) in which he proposed that for the best encryption, a key needed to be as long as the message [**3**].

Decades later, the computer age began. The encryption needed to resist information theft attempts. In 1977, the first Data Encryption Standard (DES) was developed at IBM and published by the Federal Bureau of Standards (USA). The NSA played a part in developing the data system encryption, reducing the key length from 128 bits to 56 bits. The DES 56-bit key was broken in 1998, when computers became more powerful and easily available to everyone.

In 2000, the National Institute of Standards and Technology confirms the AES (Advanced Encryption Standard), replacing the DES.

2. BASIC THEORY

Cryptography presents itself in two variants, both meant to ensure its goals of authentication, privacy, integrity, non-repudiation, service reliability and availability [**4**].

In the conventional (symmetrical) cryptography, the key is kept secret and used to code and decode the information. In the non-conventional (asymmetrical, public keys-) cryptology, a (public) key is used to crypt the data, and a private key is used to decrypt it for the user.

The process of encrypting data has a few basic elements. The encryption can be done using software or hardware. The encryption algorithm needs to be strong, hard or impossible to break. The speed of the encryption process is most important. The system should be easy to use. The key is a string of bits used in the encryption and the decrypting of the data. In order to recover the data, the user needs to possess a valid key. Longer keys are more secure, but one-time use keys are very strong.

Key management is one of the challenges in data encryption: how to create, transfer, stock, archive and destroy keys.

3. DES and AES

DES is a symmetrical encryption system. DES uses a 56 bit key in order to encrypt a 64-bit input block of plain text. The 8 bit difference becomes additional parity bits.

Each 64 bit input is first permuted and then taken as an input for a process that carries out 16 rounds of Feistel's Scheme, each of which takes the 64 bit output of the previous round and a 48 bit per-round key. The result of each round is again a 64 bit output. The per-round keys differ for each round and have a length of 48 bit. Each per-round key is a derivate of the initial 56 bit key. After the last round, the 64 bit output needs to go through the inverse initial permutation. The decryption is basically just the inverse of this process.[**5**]

DES is used to encrypt ATM systems and UNIX systems passwords. In 1998, the DES was broken using a "Deep Crack" – the EFF DES cracker. Brute force was used to crack the 56-bit encryption, in order to prove that the level of encryption was insufficient. As a result, AES was developed.

AES is a symmetrical encryption system developed through a competition by NIST in order to strengthen the security of data systems. It uses input blocks and keys of different sizes, and the number of ciphering rounds depends on those sizes. The winners were cryptanalysts Joan Daemen and Vincent Rijmen, with the Rijndael cipher, which does not use a Feistel network. Rijndael uses a variable number of rounds, depending on key/block sizes, as follows: 9 rounds if the key/block size is 128 bits; 11 rounds if the key/block size is 192 bits and 13 rounds if the key/block size is 256 bits. [**6**]

DES received multiple adaptations, to improve security, like the Triple-DES (also known as an EDE – encrypt, decrypt, encrypt – standard.) The 56-bit key is encrypted with another key (K1), then decrypted with a K2, and again encrypted with a K3. If K3 is the same as K1, then the encryption is similar to a simple DES.

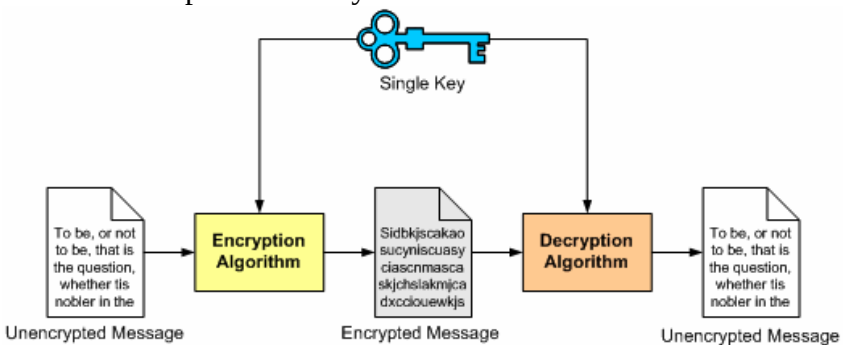

Figure 1: Symmetrical encryption systems

4. PUBLIC KEY ENCRYPTION

In 1976, Whitfield Diffie, Martin Hellman and Ralph Merkle created public key cryptography at Stanford University. Asymmetrical encryption is used, with a public (free) key used to encrypt, widely available, and a private key used to decrypt the data. Each key performs a unique function.

Public keys have to be shared but are too big to be easily remembered; they are stored on digital certificates for secure transport and sharing. The private keys are meant only for the individual who will use them, therefore can be saved on the computer using the system or on any other type of hardware the user prefers. Digital certificates are issued by entities known as Certificate Authorities (CAs).

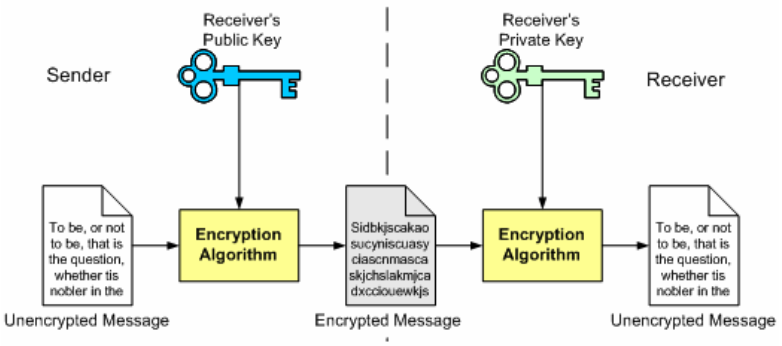

Figure 2: The public key encryption system

The main advantage of employing public key encryption is the use of digital signatures and data encryption. A certificate is an electronic document used to identify an individual, a server, a company, or some other entity and to associate that identity with a public key. A certificate provides generally recognized proof of a person's identity. Public-key cryptography uses certificates to address the problem of impersonation. It is also used because digital signatures ensure authentication, non-repudiation and integrity of the data [7].

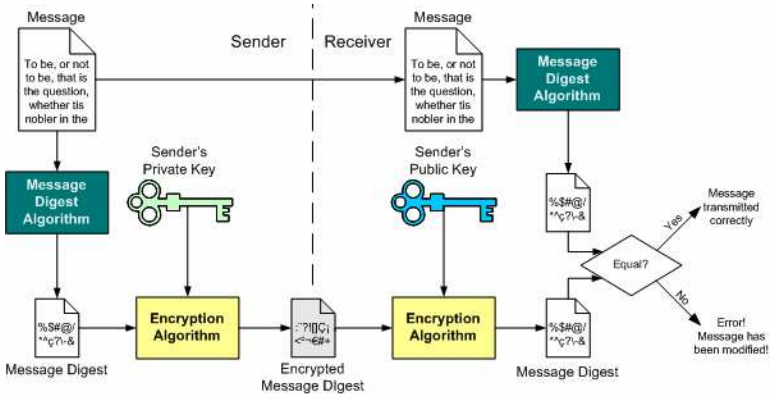

Figure 3: How digital signature works

Unlike digital signatures, the relationship between public key cryptography and message encryption is generally more straightforward, because encryption is a core function of public key cryptography. The key pair is used in message

encryption, but not for the entire message, because the encryption-decryption process using a key pair is expensive, due to the lengths of the keys' algorithms used. It is more economical to use a key pair on as little information as possible and use a faster, symmetric key on as much information as possible while ensuring that the information cannot be used until the private key is presented.

5. CONCLUSIONS

The article presents a short history of data encryption and cryptography. The elements of symmetrical and asymmetrical encryption systems are reviewed, with past and present applications.

While symmetric encryption is best-known and relatively fast and less expensive, it is also more exposed to brute-force attacks. Measures were taken in order to strengthen DES and AES. The asymmetrical encryption is more reliable and less exposed to attacks, but it can be slower and costly. A combination of both encryption methods is acceptable, with no loss in security levels and better end-user access time.

BIBLIOGRAPHY

[1]Al-Kadit, Ibrahim. "Origins of Cryptology. The Arab contributions". Cryptologia, vol. 16, issue 2, 1992.

[2]Alberti, Leon Battista, "A Treatise on Ciphers", trans. A. Zaccagnini. Foreword by David Kahn, Galimberti, Torino 1997.

[3]Shannon, Claude. "Communication Theory of Secrecy Systems", Bell System Technical Journal, vol. 28(**4**), page 656–715, 1949.

[4] Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." International journal of emerging technology and advanced engineering 1.2 (2011).

[5]Praeger, Cheril, Course Text, 2001. http://staffhome.ecm.uwa.edu.au/~00007092/teaching/3CC/WWW/chapter5.html

[6]http://www.eng.tau.ac.il/~yash/crypto-netsec/rijndael.htm

[7] Dooley, John F. "A brief history of cryptology and cryptographic algorithms". New York: Springer International Publishing, 2013.