A SECURITY ANALYSIS OF PUBLIC KEY CRYPTOGRAPHIC SYSTEMS USED FOR ELECTRONIC SIGNATURE

Eugen NEACȘU[1], Paul ȘCHIOPU[2]

Information security is manifested depending on situation and requirements. People involved in a transaction must have confidence that the objectives of information security are met. To this end, over time, increasingly complex security protocols and techniques have been developed. For a good result in terms of information security - in addition to mathematical algorithms and cryptographic protocols - it is necessary to comply with rules and procedural techniques. This study presents a detailed analysis of cryptographic systems with public keys used in digital signature, presenting methods to secure and manage the systems handled.

Keywords: cryptography, information, security, digital signature

1. Introduction

Paper has long served as a writing tool, due to its features: relatively small size, easy accessibility, durability. It was a cheap and convenient instrument for storing information, as long as the communication needs of the documents were met. Today, the problem of transmitting documents on paper has become expensive compared to the communication of documents in electronic form through computer networks.

The development of electronic devices and computer networks has had a special contribution both in the evolution of cryptographic means and in cryptanalytic methods, by permanently increasing the computing power of microprocessors and the volume of data that can transit networks.

An information security method is the electronic signature, a method that ensures the authenticity, identification and non-repudiation of sent messages. The signature serves to identify, authorize and validate, is assigned to a single individual and is considered unique. In the current technological and

[1] Security Engineer, Advanced Technologies Institute, Bucharest, Romania, e-mail: neacsu.eugen@yahoo.com

[2] Professor, University POLITEHNICA of Bucharest, Romania, e-mail: schiopu.paul@yahoo.com

informational context we can not guarantee that we can achieve all objectives necessary for information security, but the technical means are based on cryptographic mechanisms.[1]

The possibility of transmitting, electronically, signed documents is the first step towards the new technological world, based on the reaction speed of those involved in the exchange of information, disregarding the geographical distance. The electronic signature is a personal attribute, being used to recognize the identity of a person in certain operations. This element solves the problem of the person's identity and the authenticity of the document better than the holographic signature.

A cryptographic protocol is a protocol that uses cryptographic techniques to transmit data. In this case, the corresponding parties may be allies, benefiting from mutual trust, or they may be adversaries. A cryptographic protocol involves certain cryptographic algorithms, but in general, the purpose of a protocol goes beyond this aspect of information secrecy. The parties involved in the protocol may jointly use information sequences to calculate values or generate random sequences, convince each other of the identity of the correspondent, or sign a contract at the same time. The use of cryptography in protocols has the role of preventing or detecting the interception or illegitimate misappropriation of an identity.[1]

In order to demonstrate the operation of the protocols, we establish the entities involved in the transmission of messages:

- ✓ E (Sender) - the one who initiates and transmits the message;
- ✓ R (Receiver) - the legitimate correspondent of the sender;
- ✓ I (Intruder) - the one who wants to intercept the message;
- ✓ A (Authority) - the trusted entity.

There are four major components of cryptographic protocols: confidentiality, data integrity, authentication and non-repudiation.[2]

- Confidentiality ensures that the information is not accessible to unauthorized persons. Another term used for confidentiality is secrecy. There are multiple approaches to obtaining confidentiality, from physical protection to mathematical algorithms that make the data unintelligible (messages sent by E to R must not be readable by I);

- Data integrity ensures that data is not altered or accessed unauthorized. To ensure data integrity, the ability to detect changes in data by unauthorized entities is required. Changes to transmitted data consist of data insertions, deletions or substitutions (R must be able to detect whether data sent by E has been intercepted and modified by I);
- Authentication is closely linked to identification. It is applied to both entities and information. The entities involved in the protocol must be identified before the exchange of messages (R must be convinced of the real identity of the entity with which it communicates). The information transmitted through a communication channel must be identifiable in terms of origin, creation date, content and transmission time. For this reason, the aspect of information security is divided into two major classes: authenticity of entities and authenticity of data origin, the second also ensuring data integrity (R must be able to verify that the data intended to be sent by E, is indeed sent by E);
- Non-repudiation is an objective of information security that prevents an entity from denying its actions. When controversies arise over certain actions, a trusted entity is used to resolve the dispute (when R receives a message from E, not only is R convinced that the message comes from E, but he can convince a third party, neutral A, the fact that the message comes from E; E cannot deny that he sent the message to R).

One of the major cryptographic problems remains the change protocol of cryptographic keys. This protocol is used in all encryption techniques: symmetric key encryption, public key encryption, unidirectional hash functions and quantum cryptography.[3]

The transformation of information from clear text to encrypted text, following its passage through the encryption algorithm must be sufficiently complex to withstand a cryptanalytic attack. Changes in the encrypted text as a result of changing one or more characters in the plain text should not allow a cryptanalyst to predict their effect. This feature of a cryptographic algorithm on a message is called *confusion* and represents a complex functional relationship between the three elements: clear text, encryption key and encrypted text. The distribution of clear text information throughout the encrypted text, so that a change made to the plain text causes changes in as many portions of the encrypted text as possible, is called *diffusion*. In this case, a cryptanalyst needs a large amount of encrypted text in order to determine the encryption algorithm.

2. Encryption key management and security policies

Key management plays a fundamental role in cryptography, underlying the provision of cryptographic techniques for obtaining confidentiality, authentication of the entities involved and the origin and integrity of data. The purpose of a good cryptosystem is to reduce the complex problem of the correct and safe management of cryptographic keys, by using hardware or software solutions, correlated with procedural controls. The problem of physical and procedural security (secure rooms with isolated equipment), protected hardware devices and trust in a large number of people is minimized by concentrating on a small number of reliable elements, easy to monitor and control.

Financial and government institutions recognize the need to maintain a high level of data confidentiality. To avoid the high costs that can arise in the event of information compromise, these institutions frequently use cryptographic techniques in their data protection strategies. For the encryption process to be efficient, the encryption keys, as well as the data they protect, are treated with the same care and are just as important.[4]

Key management is usually performed in the context of a specific security policy that explicitly or implicitly defines the threats to which a system is exposed. These policies may influence cryptographic requirements depending on the susceptibility of the environment in question to different types of attack. Such policies also specify:

- ✓ the practices and procedures to be followed in carrying out the technical and administrative aspects of key management;
- ✓ the responsibilities of each party involved;
- ✓ the types of information related to the events that took place in the system, necessary for a security audit.

Encryption keys must be protected against unauthorized disclosure, abuse, alteration or loss. Although complex encryption techniques verified and accepted by standardization frames (ISO, ANSI, NIST) are currently used, the management of cryptographic keys can be considered a permanent challenge. Using inappropriate techniques for storing, distributing, archiving and retrieving keys can expose the keys, giving access to the encrypted data, to unauthorized persons. Automating these processes by implementing a key management system (KMS) can be a viable solution (Fig. 1).

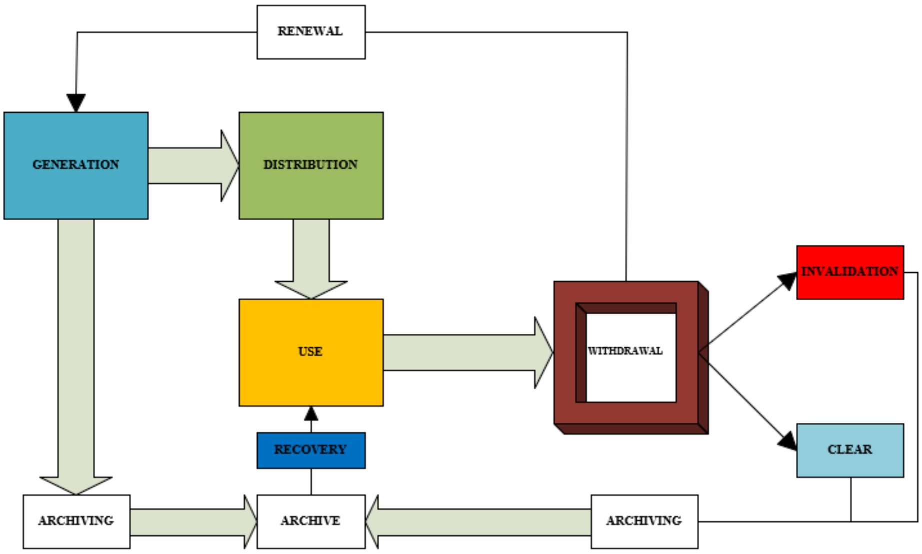

Fig. 1. Proposed KMS

The proposed KMS is an efficient one and it can be extremely complex, setting the lifetime of each managed encryption key. The basic processes of a KMS are: key generation, key distribution, use keys, key storage, key recovery, cancellation of keys, removal and destruction of keys. Depending on the security policies implemented, a KMS can only run some of these processes.

3. Key exchange in cryptosystems

One of the main problems in cryptography remains the key exchange protocol. These protocols are required, regardless of the type of encryption technique used: symmetric, public or quantum encryption.[5]

In symmetric cryptographic systems, since the same K key is used for both encryption and decryption of the message, it must be transmitted in maximum security, using secure channels (Fig. 2).

$$K_e = K_d = K \qquad (1)$$

The encryption (E) and decryption (D) processes are easy to perform for a known K key:

$$E_K(M)=C \qquad (2)$$

$$_{K}(C)= D_{K}(E_{K}(M)) = M \qquad (3)$$

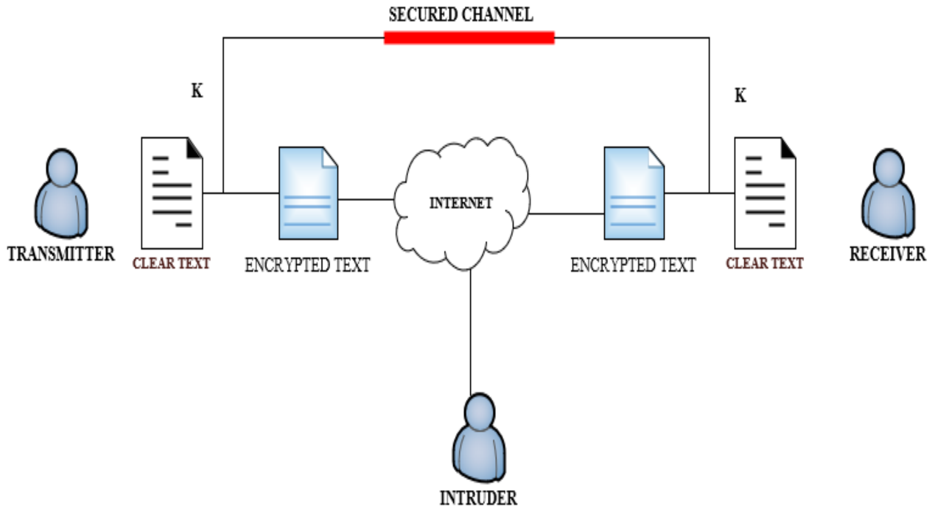

Fig. 2. Transmission of encryption keys (symmetric cryptosystem)

Because the algorithm is valid in both directions, users must trust each other. The security of this type of algorithm depends on the length of the key and how it is sent and kept secret. When communications between *n* users need to be encrypted, there is a major problem with key management, so *n(n-1)/2* bidirectional links are possible for users, each link using a different encryption key. This generally involves difficult problems in generating, distributing and storing the key. Electronic computers have allowed the use of larger keys, thus increasing resistance to cryptanalytic attacks. When the secret key has a convenient size and is changed frequently enough, the cipher becomes virtually impossible to break, even if the encryption algorithm is well known.

Disadvantages in the proposed Key Exchange:

a. Key distribution can be a problem, even if there are only two entities involved in the key exchange. In large organizations, where many people need to use the same key, it is recommended to use a cipher based on public keys;

b. Even if the number of participants is small, the cryptographic key must be replaced very often;

c. Very large keys are required in digital signature algorithms.

Instead of a secret key, asymmetric cryptography uses two different keys, one for encryption and the other for decryption. Since it is impossible to deduce one key from the other, one of the keys (public key) is made public and is available to anyone who wants to send an encrypted message. Only the recipient, who holds the second key (private key), can decrypt the message. In public key systems, protection and authentication are performed separately (Fig. 3).

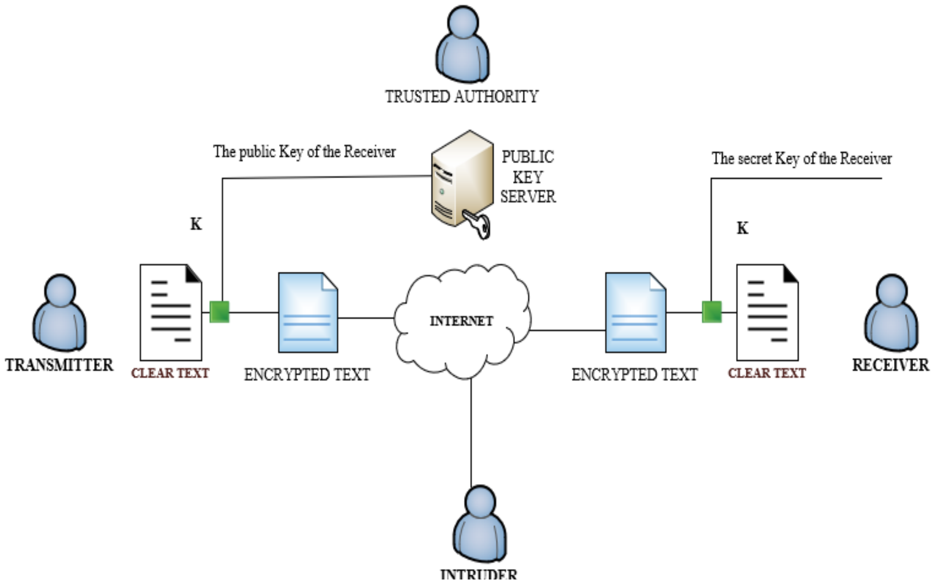

Fig. 3. Transmission of encryption keys (cryptosystem with public keys)

$$Ke \neq Kd \tag{4}$$

Characteristic for these systems is the fact that the encryption and decryption processes are performed quickly. For clear text and encrypted text C, a public key cryptosystem follows the relationships:

$$E_{Ke}(M) = C \tag{5}$$

$$D_{Kd}(C) = M \tag{6}$$

For unknown C's and K's, finding M is computationally impossible, making the public key cryptosystem more attractive than the symmetric key cryptosystem. One of the most popular applications for this type of cryptosystem is the digital signature.

It is an irreversible trap-door function. K_d is the trap-door needed to calculate the inverse of the function (D). RSA, Diffie-Hellman, Markle-Hellman are well known algorithms that use this type of function.

Public key cryptography is not perfect. Some of its problems are: [6]

- the encryption time for this type of algorithm is normally much longer than the time required in symmetric key algorithms;
- the keys used for encryption and decryption are much longer (usually 1024 bits) than those used in symmetric key cryptography (usually in the range of 32-128 bits). The increased key length is useful to prevent easy key factorization; The high factorization difficulty of large numbers ensures security, but this difficulty may disappear with the discovery of an efficient factorization algorithm.

The security analysis shows the difficulty of high factorization of large numbers ensures security, but this difficulty may disappear with the discovery of an efficient factorization algorithm.

4. Security issues in public key cryptographic systems

Any attempt to obtain clear text from the encrypted text without holding the secret key is considered a cryptanalytic attack. Cryptographic analysis studies attack methods based on minimal information about encryption keys, algorithms used, authentication protocols, clear text segments and corresponding segments in the encrypted text, or only based on one or a set of encrypted texts using the same algorithm.

In essence, an attempt is made to determine a vulnerability of the algorithm, which can be exploited using methods for which the search time is considerably less than the time required to verify all possible key combinations (brute force attack). There is not yet a cryptographic system that can be said to be fully secure, but those cryptosystems for which known attacks take too long to be considered practical can be considered secure. Below are briefly described the most popular attacks, demonstrated and verified by mathematicians, computer scientists and cryptanalysts. [7]

✓ *Encrypted text attack* - is based on information about encrypted text sequences and is one of the most difficult cryptographic methods because of the summary information on which information about clear text or keys must be deduced;

- ✓ *Adaptive attack with ciphertext* - is an interactive form of ciphertext attack in which several clear text sequences are sent to be decrypted, then the obtained sequences are used to choose those parts of clear text and encrypted text that give information relevant about the ciphertext or the keys used for decryption;
- ✓ *Clearly chosen text attack* - this attack assumes that we have the ability to choose clear texts to be encrypted and we can obtain the corresponding encrypted texts to determine additional information, usually on the encryption keys;
- ✓ *Attack with selected keys* - in which the attacker does not have complete information about the keys but only some disparate information about the relationships between some keys; it is a very little used and almost impractical attack;
- ✓ *Brute force attack* - if the cryptographic system does not have vulnerabilities known to the attacker, the only way remains an attack that consists in trying all possible decryption keys;
- ✓ *Dictionary type attack* - is a cryptanalytic method in which the attacker prepares and stores a table with clear text-encrypted correspondences of the type of pairs ($P_iC_i=E_{Ki}(P),K_i$) sorted by C_i; Subsequently, the attacker monitors the communication and when it finds an encrypted text C_j that is found in its table, it will immediately find the encryption key K_j ;
- ✓ *Birthday Attack* - is based on the well-known paradox of "birthday" and its variants. The problem can be generalized as follows: if a function $f : A \to B$ can take any of the n values from the set B with equal probabilities, then after calculating the function for $\sqrt{n}$ different values it is very possible to find a pair of values x_1 and x_2 so that $f\,(x_1) = f\,(x_2)$. The event is a collision, and for functions with odd distribution, the collision may occur even earlier. The digital signature is susceptible to such an attack;
- ✓ *Attack of the man in the middle* - describes the situation when an attacker has the opportunity to read and modify messages exchanged between two correspondents without the two parties noticing that the method of communication between them has been compromised. The possibility of such an attack remains a serious problem for public key systems;

- ✓ *Mid-encounter attack* - is similar to the birthday attack, except that in this case the analyst has greater flexibility. Instead of waiting for two values to coincide in a single set of data, the analyst can look for an intersection of two sets. Assuming that the attacker knows a lot of clear *P* texts and *C* encrypted texts with the keys k_1 and k_2; then it can calculate $E_K(P)$ for all possible keys *K* and store the results; then can calculate $\mathrm{D_K(C)}$ for each *K* and compare with the stored results; if it finds a match it's like finding the two keys and can check directly on the plain and encrypted text. If the key size is *n*, the attack will use only 2^{n+1} encryption in contrast to a classic attack, which would require 2^{2n} encryption; [8]
- ✓ *Repeat attack* - is an attack in which the attacker memorizes a communication session in both directions (messages exchanged by both correspondents) or pieces of the session. The idea of the attack is not to decrypt a communication session, but to create confusion and false messages;
- ✓ *Attack with related keys* - in this case the attacker discovers a relationship between a set of keys and has access to encryption functions with such related keys. The stated goal is to find even the encryption keys. Algorithms such as IDEA, GOST, RC2 and TEA showed weaknesses when attacked; [9]
- ✓ *Sliding attack* - can be seen as a variant of the attack with related keys in which the relationships are defined on the same key; the attack is effective in the case of iterative or recursive processes (symmetric string or block type algorithms) that present degrees of similarity between successive cycles of the iterative process. The complexity of the attack is independent of the number of cycles of the algorithm. Weaknesses in this attack were found in the Feistel algorithm and even in the case of SHA-1;
- ✓ *Correlation attack* - is performed on the filter generator from string digits based on LFSR (Linear Feedback Shift Register) type generators, in two phases: first a function is determined between the generated key bit string and the shift register bits, after which the key string is interpreted as a noise-affected version of the string generated by the LFSR;[10]
- ✓ *Boomerang attack* - uses the flexibility of differential cryptography and allows the use of two uncorrelated features to attack the two halves of a block cipher. The method increases the potential of differential cryptanalysis, by using features that do not propagate through the entire cryptographic algorithm. The

results occur only in the presence of both characteristics, as the method cannot work independently for each characteristic.[10]

5. Conclusions

Depending on the situation and requirements, information security methods need to be constantly adapted to respond effectively to needs. In order for transactions to be secure and information security objectives to be met, increasingly complex cryptographic protocols and techniques have been developed. These, corroborated with the observance of some procedural techniques, can ensure the desired level of security.

Current methods seek to ensure the authenticity, identification and non-repudiation of sent messages, and in the context of ongoing technological development and the determination of new methods of attack, the most effective technical means are based on the use of cryptographic mechanisms.[11]

In order to ensure the confidentiality of the data transmitted using cryptographic processes, the study pointed up methods of protecting the data traffic, presenting a proposed pattern to secure key management systems and highlighting an important segment of modern cryptography – the integrity of the information disseminated.

Cryptographic solutions based on symmetric block algorithms are a special category, characterized in particular by a very good encryption speed. Their design (and not only of this type of algorithms) must meet two essential conditions: to be "safe" and to be "fast". In recent years, great efforts have been made in the Academic and commercial world, to design algorithms that best meet the two stated conditions: speed and security.[12]

This paper exposes the security needs of users, the speed with which the processes of encryption and decryption of files are performed but also the permanent evolution of cryptanalytic methods. Depending on the security demands and the environment in which it is implemented, cryptographic systems can be modeled so as to obtain the desired product.

REFERENCES

[1]. *Amiel F., Villegas K., Feix B., Marcel L.,* Passive and Active Combined Attacks: Combining Fault Attacks and Side Channel Analysis. Workshop on Fault Diagnosis and Tolerance in Cryptography, pp. 92-102. IEEE Computer Society, Washington, DC, USA, 2007;

[2]. *Anderson R*., Security Engineering: A Guide to Building Dependable Distributed Systems. Second Edition, Wiley Publishing Inc., Indianapolis, Indiana, 2008;

[3]. *Baptista M. S*., Cryptography with chaos. Physics Letters A, March 1998;

[4]. *Biham E., Shamir A.,* Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, 1993;

[5]. *Biryukov A., Wagner D*., Slide Attacks. Proceedings of Fast Software Encryption - FSE'99, no. 1636, Lecture Notes in Computer Science, pp. 245-259, Springer-Verlag, 1999;

[6]. *Björkqvist M., Cachin C., Haas R., Hu X-Y., Kurmus A., Pawlitzek R., Vukolić M*., Design and Implementation of a Key-Lifecycle Management System, Financial Cryptography and Data Security, Lecture Notes in Computer Science, Volume 6052. Springer-Verlag Berlin / Heidelberg, 2010;

[7]. *Bleichenbacher D*., Chosen Ciphertext Attacks Against Protocols Based on RSA Encryption Standard PKCS#1. Advances in Cryptology Proceedings - CRYPTO'98, 1998;

[8]. *Brier E., Clavier C., Olivier F*., Correlation Power Analysis with a Leakage Model. Cryptographic Hardware and Embedded Systems - CHES 2004, Lecture Notes in Computer Science, vol. 3156, pp. 135-152. Springer Berlin / Heidelberg, 2004;

[9]. *Canvel B., Hiltgen A., Vaudenay S., Vuagnoux M*., Password Interception in a SSL/TLS Channel. Advances in Cryptology - CRYPTO '03, Lectures Notes in Computer Science, vol. 2729, Springer-Verlag, 2003;

[10]. *Marghescu, A., Svasta, P., Simion, E.,* Randomness extraction techniques for jittery oscillators. In: 38th International Spring Seminar on Electronics Technology (ISSE), pp. 161-166 (2015);

[11]. *Simion, E.,* The relevance of statistical tests in cryptography. IEEE Secur. Priv. 13(1), 66-70 (2015);

[12]. Data Breach Investigations Report (DBIR). https://www.verizonenterprise.com/DIBR/2015.