THEORETICAL APPROACH OF CRYPTOGRAPHIC PROTOCOLS

Marian CREȚU

"Politehnica" University, Bucharest, Romania

Abstract: *This paper aims to make a brief foray into the field of information protection presenting a theoretical analysis of the most known and used cryptographic protocol types, necessary to change messages encryption and decryption keys, using computer networks as transmission channel. Under continuous development of new ways to exploit infrastructure and means of communications vulnerabilities, sensitive data encryption still remains a viable alternative.*

Keywords: *cryptography, protocol, symmetric key, public key, quantum*

1. INTRODUCTION

Cryptology is defined as the science of secret writing, of its unauthorized decryption, and of the rules which are in turn intended to make that unauthorized decryption more difficult (Bauer, 2006: 21-43). It appeared and developed following the need to protect information with greater sensitivity. The two sides of its, cryptography and cryptanalysis evolved together in the context of the emergence and development of computing machines. If in ancient times, when the first signs of using encryption techniques were hieroglyphic writing or transposition techniques (Scylla or Caesar's cipher), in the Middle Ages, polyalphabetic ciphers were developed by Vigenere and Battista's contributions.

The World War II had its contribution in the development of automatic machines for encryption (Enigma, Purple, Poem), and in implementing new cryptanalytic methods. Appearance of the first electronic computer in the 60' was at the start of explosive growth, both encryption algorithms (DES in the 70', IDEA, Locki, Skipjak) and cryptanalysis techniques (different test batteries, such as DIEHARD or NIST), leading nowadays to implementations of increasingly more complex algorithms (Rijndael, Twofish, Serpent, RC6).

2. CRYPTOGRAPHIC PROTOCOLS

By a protocol we mean a specific sequence of steps that are carried out in a particular application (Koblitz *et al.*, 2008).

A **cryptographic protocol** is a protocol that uses cryptography in order to transmit data. The parties can be friends and trust each other implicitly or they can be adversaries and not trust one another. A cryptographic protocol involves some cryptographic algorithm, but generally the goal of the protocol is something beyond simple secrecy. The parties participating in the protocol might want to share parts of their secrets to compute a value, jointly generate a random sequence, convince one another of their identity, or simultaneously sign a contract. The whole point of using cryptography in a protocol is to prevent or detect eavesdropping and cheating (Schneier, 1996).

To demonstrate the protocols functionality, we have to agree about several entities:

- A (Alice) is the initiator of the message;
- B (Bob) is the responder;
- E (Eve) is the eavesdropper;
- T (Trent) is the trusted third-party entity.

There are four main components of cryptographic protocols: confidentiality, data

integrity, authentication and non-repudiation (Salomon, 2005: 271-328).

1.*Confidentiality* is ensuring that information is not accessible for those who are not authorized to see it. A synonymous term for confidentiality is secret. There are many approaches to achieve confidentiality, from physical protection to mathematical algorithms that make data unintelligible (messages sent by *A* to *B* must not be readable by *E*) (Menezes, 1996; Paar *et al*., 2010).

2. *Data integrity* is ensuring that data are not altered in unauthorized manner. To ensure data integrity, we must have the ability to detect all modification of data by unauthorized entities. These modifications on transferred data, include insertion, deletion and data substitution (*B must* be able to detect when data sent by *A* has been altered by *E*) (Salomon, 2005; Paar *et al*.: 2010).

3. *Authentication* is closely linked to identification. They apply to entities and information in the same measure. Two entities involved in a protocol should be identified before making other exchanges messages (*B* should be convinced of the identity of the other communicating entity). Information transmitted through a channel should be identified in connection with the origin, date of creation, content and time it was sent. For these reasons this aspect of information security is divided into two major classes: entity authentication and data origin authentication, the last providing also data integrity (*B* should be able to verify that data purportedly sent by *A* indeed originated with *A*) (Salomon, 2005; Menezes, 1996).

4. *Non-repudiation* is an objective of information security that prevents an entity to deny its previous actions. When controversy arises in connection with certain actions, a trusted third entity is used to resolve the dispute (when *B* receives a message from *A*, not only is *B* convinced that the message originated with *A*, but *B* can convince a neutral third party (*T*) of this; *A* cannot deny having sent the message to *B*) (Koblitz *et al*., 2008; Hankerson, 2006).

One of the main problems in cryptography remains the key exchange protocol. It is used in all types of encryption techniques: symmetric key encryption, public-key encryption, one-way hash functions and quantum encryption.

2.1 Symetric key cryptosystems. Cryptographic systems using identical keys for encryption and decryption processes are also named secret key cryptosystems, because of the *K* key that must be kept secret, and transmitted on secured channels (fig. 1).

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

Encryption (E) and decryption (D) processes are very easy since the K key is known:

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

$$_K(C) = D_K(E_K(M)) = M \quad (3)$$

By the type of used algorithm, symmetric key cryptosystems are classified into two categories:

- **block ciphers**: ciphers acting on a division of clear text, blocks of input being independently computed, with the typical blocks length between 32 and 128 bits. Basic transformations used for encryption and decryption are substitutions and transpositions, iteratively repeated.

- **stream ciphers**: input message is considered as a sequence (string) of symbols. Encryption operates on plain text symbols, one at a time. The *K* key is generated by a shift register with response, having the initial state 0 and controlled by a compact key.

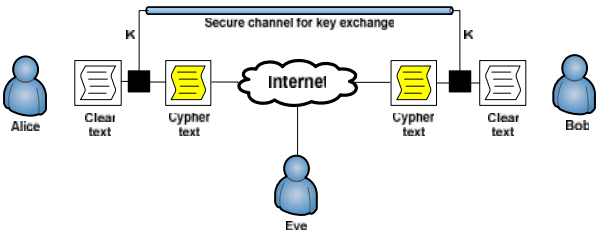

Fig. 1. Symmetric key cryptosystem.

Since the algorithm is valid in both directions, users must have mutual trust. Security of this type of algorithm depends on key length and how can it be kept secret. When communications between many users must be encrypted, there is a big problem of key management, so for *n* users are possible $n(n-1)/2$ bidirectional links, each link using a different encryption key. This generally

involves difficult problems in generation, distribution and key storage. Electronic computers 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, it becomes virtually impossible to break the cipher, even if encryption algorithm is well known.

There are some disadvantages using the symmetric key cryptography:

1. Key-distribution represents a problem even in the case where only two parties communicate. Within large organizations, where many individuals must have the same key, the use of a public-key cipher is recommended.

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

3. Symmetric-keys require large keys in digital signature algorithms.

2.2 Public-key cryptosystems. Instead of one secret key, asymmetric cryptography uses two different keys, one for encryption and the other one 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 wishing to send an encrypted message. Only the recipient, which holds the second key (private key), can decipher and use the message. In public key systems, protection and authentication are performed by distinct changes (fig. 2). Because keys are asymmetric, the encryption key is always different from decryption key:

$$K_e \neq K_d \tag{4}$$

Characteristic for these systems is that the encryption and decryption are performed very fast if K_e and K_d are known. For M as clear text and C as cipher text, a public key cryptosystem follows the relations:

$$\begin{cases} E_{K_e}(M) = C \\ D_{K_d}(C) = M \end{cases} \tag{5}$$

For known C and K_e, finding M is computationally unfeasible, making this cryptosystem more attractive than the symmetric one. One of the most famous applications of this type of cryptosystem is the digital signature.

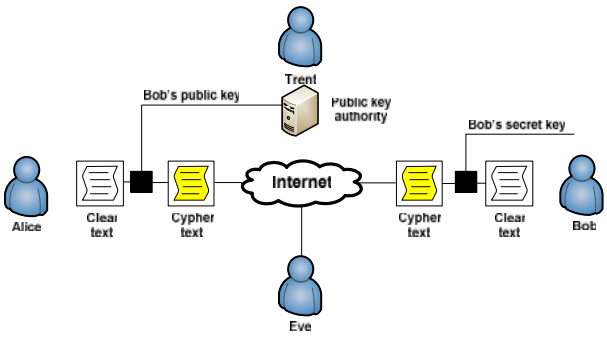

Fig. 2. Public key cryptosystem.

E represents a non-inverting trap-door function. K_d is the necessary trap-door to compute the inverse function D. RSA, Diffie-Hellman, Markle-Hellman are well known algorithms using this type of functions (Salomon, 2005; Menezes, 1996).

Public-key cryptography is not perfect. Here are some of its problems:

1. Time for encryption for this type of algorithm is normally much bigger than the time needed in symmetric-key ciphers.

2. The keys used for encryption and decryption are much longer (about 1000 bits) than those in symmetric-key cryptography (usually in the range 32-128). The increased length is useful to prevent an easy key factorization.

3. The difficulty of factoring large numbers ensures the security, but this difficulty may be temporary once an efficient factoring algorithm will be discovered (Zeng, 2010).

2.3 Quantum cryptosystems. Quantum private communication is an alternative for the classic private communication, and it is able to ensure the four goals of cryptographic protocols Even more, it is able to detect the eavesdropper operations. Currently, quantum physical laws cannot be broken, making them perfect for a more secure communication channel. Security requirements are satisfied by quantum cryptosystems authentication protocol (fig. 3).

In order to understand how quantum private communication is working, we will consider a communication model where two entities, Alice and Bob, using a communication network want to send a

message using a quantum private communication system. Authentication and confidentiality are two important factors for a strong security via a quantum private communication system (Biham *et al*., 2000: 715- 724).

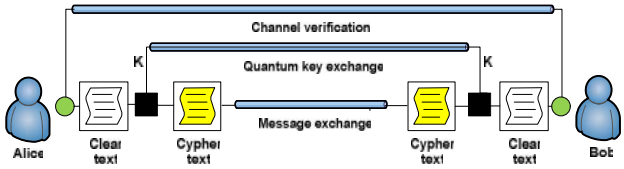

Fig.3. Quantum key cryptosystem.

While the smallest classical information unit is the bit, quantum information unit uses the qubit (a quantum system that lies in a two-dimensional Hilbert space (*dim H* = 2)) (van Assche, 2000: 49-52).

Any two-level quantum system can be represented by states, for phase encoding, photon polarization, or spin ½ systems. The first two linear states corresponds to horizontally (→) and vertically (↑) polarized photons, while the last two to polarization angles - 45° (↖) and + 45° (↗) relative to vertical axis. Bit value '0' is represented by the states $|0\rangle$ and $|+\rangle$, while the pair of states $|1\rangle$ and $|-\rangle$ stands for bit value '1'. Orthonormal and conjugate bases are formed by the pairs $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$. They are rectilinear (⊕) and diagonal basis respectively (⊗) (Zeng, 2010: 135-137).

Bennett and Brassard defined in 1984 the first known protocol, BB84 (table 1), based on four quantum states:

$$\left\{|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{a}}\left(|0\rangle + |1\rangle\right), |-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right\} (6)$$

Table 1. The BB84 protocol

Alice			**Bob**		Bases announcement	Shifted key
Random bit sequence	Random basis	Photon polarization	Random measuring basis	Measured polarization		
1	⊗	↗	⊗	↗	Confirmed	1
1	⊕	→	⊗	↖	-	-
0	⊕	→	⊕	→	Confirmed	0
1	⊗	↖	⊕	↗	-	-
0	⊗	↗	⊕	→	-	-
1	⊕	↖	⊕	↖	Confirmed	1
1	⊕	→	⊗	↗	-	-
0	⊗	→	⊗	→	Confirmed	0

B92 is another quantum protocol that can be implemented using a single non-orthogonal basis, or two non-orthogonal states (Bennet, 1992). Bob and Eve are unable to decode all the bits on the quantum channel due to the non-orthogonal states. Bob will use the suitable quantum projection operators in order to perform two separate measurements. Bob's measurements detects if Alice's transmitted bit sequence is correct. The protocol has 3 major phases:

Phase 1: **Quantum transmission.** Alice generates a random bit string that she wants to transmit. For each bit she chooses a random encoding basis and prepares the states that will be sent to Bob using the quantum channel. For each received qubit, Bob chooses his measurement basis randomly and independently of Alice. Bob records both measurement bases and the results of measurements.

Phase 2: **Bases announcement.** Bob send his bases (not the results) to Alice using the public channel. This information will not help Eve to affect Bob's state. Alice and Bob have a previous agree to discard the bits where they used opposite bases. The sequence of bits remaining after bases announcement forms the shifted key.

Phase 3: **Error estimation.** In this phase, Alice and Bob hold a string which will help them to determine if there was an

eavesdropper connected. The difference between Alice's and Bob's keys can be determined by the error rate. For a calculated error rate higher than admitted threshold value, message sending is stopped. For accepted threshold values, they perform the error correction and privacy amplification in order to generate the final key.

3. KEY EXCHANGE PROTOCOL FOR STORED KEYS USING DATABASES

In order to use a fast and secure algorithm, there are several issues to be solved in a convenient manner. Fast algorithm means symmetric key algorithm, and secure means public key exchange protocol. Thus, we obtain a hybrid algorithm, using both well known techniques.

Practice revealed that an increased number of users in a network, contribute to a low level of network security. Another problem is that every encryption process need a new encryption / decryption key, meaning that there is a large number of keys that must be stored. A good idea is to use a secured database for storage. This database must be installed on every trusted entity computer and it can be transmitted from one trusted entity to another using a quantum channel, a classic encrypted channel, or by storage devices (CD, Memory Stick, Mobile HDD, etc.). We presume that computers in the network use security policies and data stored on their HDD are secured. The algorithm will use a PRNG (Pseudo Random Number Generator) to choose a key ID from those stored in database. The plaintext will be encrypted using the encryption key with that ID.

The decryption process will use the key ID received on a secure channel to access the database and select the proper key.

4. CONCLUSIONS

Symmetric and public key cryptosystems both have strong and weak elements. Their combined use (by sending the secret key using asymmetric protocols and encrypting message using symmetric algorithms) results in hybrid cryptosystems, able to properly respond to cyber attacks, increasing the level of data protection.

Quantum mechanics, although it is an area that has its origins in the 60', by its applications in the field of cryptography and correlated with current technology, has a decisive role on communication channels checking.

Use of databases instead of sending the encryption key over a common network and changing the key on every encryption / decryption process, will increase the diffusion factor, making cryptanalysis process more difficult.

BIBLIOGRAPHY

1. Bauer, F.L. (2006). *Decrypted Secrets - Methods and Maxims of Cryptology* (4th edition). New York: Springer-Verlag. 21-43.
2. Bennet, H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*.
3. Biham, E., Boyer, M., Boykin, P.O., Mor, T., Roychowdhary, V. (2000). *A proof of the security of quantum key distribution. STOC'00: Proceedings of the thirty-second annual ACM symposium on theory of computing*. New York: ACM Press. 715-724
4. Hankerson, D., Menezes, A., Vanstone, S. (2004). *Guide to Elliptic Curve Cryptography.* New York: Springer-Verlag.
5. Koblitz, H., Koblitz, N., Menezes, A. (2008). *Elliptic curve cryptography, the serpentine course of a paradigm shift*. [online]. URL: eprint.iacr.org/2008/390
6. Menezes, A., van Oorschot, P., Vanstone, S. (1996). *Handbook of Applied Cryptography*. New York: ACM Press.
7. Paar, C., Pelzl, J. (2010). *Understanding Cryptography. A Textbook for Students and Practitioners.* Berlin, Heidelberg, New York: Springer-Verlag.
8. Salomon, D. (2005). *Coding for Data and Computer Communications Publisher.* PhD New York: Springer-Verlag. 271-328.

9. van Assche, G. (2006). *Quantum Cryptography And Secret-Key Distillation*. Cambridge: Cambridge University Press. 49-52.

10. Zeng, G. (2010). *Quantum Private Communication*. Beijing: Higher Education Press. Berlin, Heidelberg, New York: Springer-Verlag. 135-137.