Basic Principles of Functioning of the Hybrid Cryptographic System

Olexander Belej

Lviv Polytechnic National University
tiger_oles@i.ua

For encryption of open text a special algorithm is used, the secrecy of the transformation of information is achieved through the use of a unique algorithm or key that provides each time original encryption of information. However, with the development of cryptography, the basic principle of modern encryption systems was the Kerckhoff rule, according to which the popularity of the opponent of the algorithm of transformation should not reduce the reliability of the encryption system, and its cryptostability is determined only by the secrecy and quality of the used cryptographic keys [1, 2]. Thus, without the knowledge of the secret key decryption should be practically impossible, even under a known encryption algorithm.

Symmetric cryptosystems can be implemented on a variety of secret key encryption algorithms (standards) that can be split into block and streaming. As a rule, modern symmetric cryptosystems are represented by such well-known standard as DES and Rijndael (USA), which is a block cipher [3].

In practice, hybrid cryptosystems are effectively used, combining elements of symmetric and asymmetric cryptosystems and, accordingly, inherent in their properties: for symmetric methods of encryption, high speed and short cryptographic keys; for asymmetric, the possibility of an open and secure distribution of encryption keys [4].

In the hybrid cryptosystem, public key encryption is used to encrypt, transmit and further decrypt only the secret key of symmetric encryption, which is directly used to encrypt transmitted messages (plaintext). Thus, the asymmetric cryptosystem harmoniously complements the symmetric cryptosystem, providing a simple and safe distribution (transmission) of secret key encryption. The generalized scheme of the hybrid cryptosystem is shown in Fig. 1

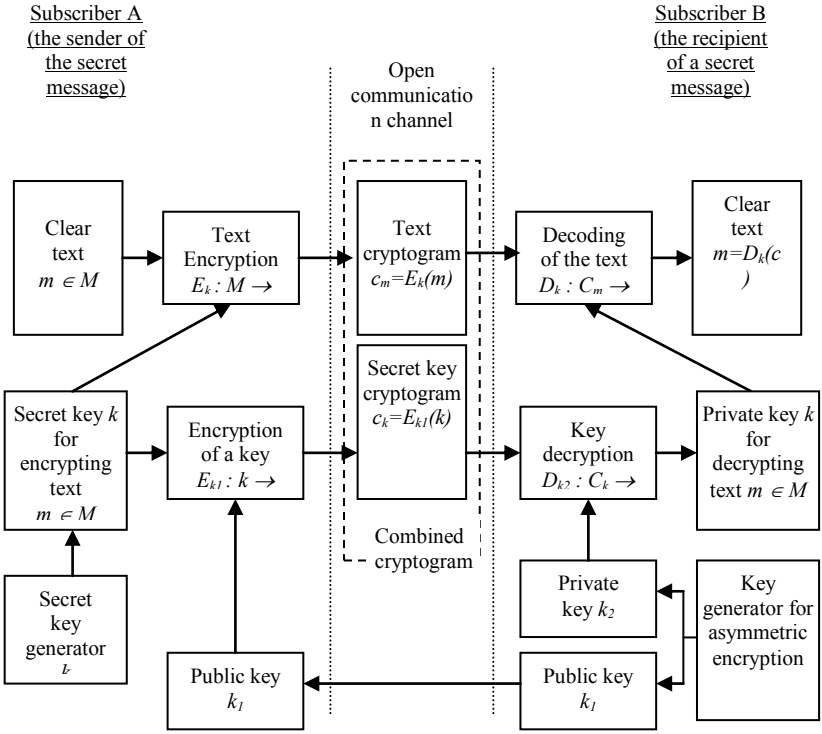

Fig.1 Scheme of the hybrid cryptographic system.

The secret communication protocol (transmission of a secret message) between subscriber A (sender) and subscriber B (receiver) may be as follows:

1. Subscriber B generates open (k1) and closed (k2) keys for asymmetric encryption, and transmits the public key k1 to an open (accessible, unprotected) communication channel of subscriber A.

2. Subscriber A generates a session-secret cryptographic key for symmetric encryption and encrypts for it the secret message (open text) m to be transmitted.

3. Subscriber A encrypts the session secret cryptographic key on the public key k1.

4. Subscriber A transmits an open communication channel to the user's address in an encrypted message (encrypted message) cryptogram with a cryptogram of the secret cryptographic key k used to encrypt this message.

5. Subscriber B decrypts the closed secret key k2 session secret cryptographic key, which decrypts the cryptogram of the message m.

To increase cryptographic stability in the hybrid cryptographic system, each secret link session (encryption of a new message) generates its own secret key for symmetric encryption called sessional.

The choice of the size of cryptographic keys for symmetric and asymmetric encryption is carried out in such a way that their potential cryptantability to the attack by the method of full overview of possible options was comparable.

If the open and closed asymmetric encryption keys are used repeatedly (for a long time), then their cryptographic stability should be substantially higher than that of the session secret key of symmetric encryption, since when they are disclosed (discredited), the opponent will have the opportunity to decrypt the secret keys transmitted to the session and, accordingly, , encrypted messages on them.

In tabl. 1 shows the lengths of the keys of symmetric cryptosystems that have difficulty disclosing by the method of full-fledging, which can be compared with the difficulty of factorizing the corresponding modules of asymmetric cryptosystems.

TABLE 1

LENGTH OF KEYS OF SYMMETRIC CRYPTOSYSTEMS

Key length symmetric cryptosystem, bit	Module of an asymmetric cryptosystem, bit
56	384
64	512
80	768
112	1792
128	2304
192	5184
256	9216

Most hybrid systems work this way. For a symmetric algorithm (3DES, IDEA, AES, or any other), an occasional session key is generated. This key usually has a size from 128 to 512 bits (depending on the algorithm). Then a symmetric algorithm is used to encrypt the message. In the case of block encryption, you must use an encryption mode, which will allow you to encrypt messages with lengths that exceed the length of the block. Regarding the most accidental key, it should be encrypted using the public key of the recipient of the message, and it is at this stage that an open-source cryptosystem is used (RSA or Diffie-Hellman algorithm). Because the session key is short, its encryption takes a bit of time.

Encrypting a message set using an asymmetric algorithm is a computationally more complex task, so it is preferable to use symmetric encryption here. Then it's enough to send a message encrypted by a symmetric algorithm, as well as a corresponding key in an encrypted form. The recipient first decrypts the key using his secret key, and then, with the help of the received key, receives all messages.

Extended hybrid encryption uses two pairs of asymmetric keys and a pair of symmetric ones. By passing one key one by one in an encrypted form, the overall stability of the cryptosystem increases.

Step 1. The first asymmetric key sends through the Internet in unencrypted form.

Step 2. Send second asymmetric key encrypted with key in step 1.

Step 3. Sending a symmetric key encrypted with the key in step 2.

Step 4. Use the symmetric key in step 3 to encrypt and decrypt the information.

All these actions are done with only one purpose - to make the evil cipher impossible or inappropriate.

REFERENCES

[1] Th.Beth, M.Frisch, G.J. Simmons (eds.) “Public-Key Cryptography: State of the Art and Future Directions”. *E.I.S.S. Workshop - Oberwolfach*, Germany, July 1991 - Final Report. Lecture Notes in Computer Science, V.578.

[2] W.Diffie, M.Hellman. “New Directions in Cryptography”. *IEEE Trans. Inform.* Theory, IT-22, No.6 (1976), pp.644-654

[3] R.L.Rivest, A.Shamir, L.Adleman. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”. *CACM*, V.21 (1978), No.2, pp.120-126.

[4] B.Schneier. “Applied Cryptography: Protocols, Algorithms and Source Code in C”. *John Wiley & Sons, Inc*., 1994.