UDC 004.021

DEVELOPMENT OF A HYBRID CRYPTOSYSTEM FOR USER DATA PROTECTION

ARTYOM SUBBOTIN, YURY PASTUHOV
Polotsk State University, Belarus

The most important requirement for the encryption system is its durability. Unfortunately, increasing durability using any method usually leads to difficulties in encrypting data and decrypting it. Therefore, the formation of a deeply thought-out cryptosystem is a very important task.

Introduction. The level of knowledge in the field of data encryption is quite high. Every year a lot of programmes and literature, which are dedicated to cryptographic systems, are created. A cryptographic system is a family of cipher transformations and a keys collection. There are symmetric and asymmetric cryptosystems.

Main section. Symmetric cryptosystems (with a secret key) - cryptosystems, which are built on the basis of keeping the encryption key secret. The encryption and decryption processes use the same key. The secrecy of the key is a postulate.

Asymmetric cryptosystems (open encryption systems with public key) – the meaning of these cryptosystems is that different transformations are used for encryption and decryption. One of them – encryption - is absolutely open to all. The other, decoding, remains secret [1].

At the moment quite resistant systems are used more often, systems with a rather complex encryption algorithm. Because of the need for various objects to encrypt secret data and cryptographic systems do not stand still and are constantly being improved.

Selection of encryption algorithms. Based on the analysis of the most crypto-stable algorithms, the following conclusions were made:

– encrypting information using the symmetric algorithm AES: despite the shortcomings, to crack the information protected by this algorithm is almost impossible. The essence of AES is that any "frontal attack" on protected data – that is, the selection of all possible passwords — is very stretched out in the future. If we imagine that a hacker has vast resources, that is, a whole collection of supercomputers, then he could get access to encrypted data in decades.

– Encryption of the session key using the asymmetric RSA-OAEP algorithm: it is not only involution modulo a large number. It is also the addition of redundant data which allow additional protection of your information [2].

Flowchart of the communication protocol. Let the two subscribers agree to exchange data. The scheme, which is shown in Figure, assumes that each participant in the information exchange has two keys: a public PK and a private SK. Let's have a look on the process of sending a document M. The sender (subscriber A) generates a secret key – a random number, which is used only once and therefore called a one-time or session key. This key is used to encrypt the M document using a symmetric cryptoalgorithm. The session key is encrypted in the recipient's public key (subscriber B) and attached to a previously encrypted document. The generated message is sent to the recipient. This person, received the message, repeats the same procedure, but in reverse order. Using his private key, the recipient recovers the session key, and then decrypts the document with it.

Selection of the length of the session key. The second step is to select the session key length. The number of encryption rounds depends on the key size:

– 128 bits length – 10 rounds;
– 192 bits long – 12 rounds;
– 256 bits length – 14 rounds.

As an example, let's take a key length of 128 bits. Input data for encryption operations is an array of 16 bytes. Before encryption starts, the bytes of this array are placed sequentially in the matrix columns. Inside the algorithm, operations are performed on a byte matrix, called the state matrix. The final value of the state matrix is the output of the algorithm and is converted into a sequence of ciphertext bytes. Similarly, 16 bytes of the cipher key fall into the columns of the original matrix. The dimension of all matrices is 4 × 4. Four bytes in each column of the state matrix or key can be considered as one 32-bit word. Therefore, the state matrix is an array of 4 words. The matrix that arrives at the input of each round is called the input state matrix, and the output matrix of the output state is formed at the output of the round. [3]

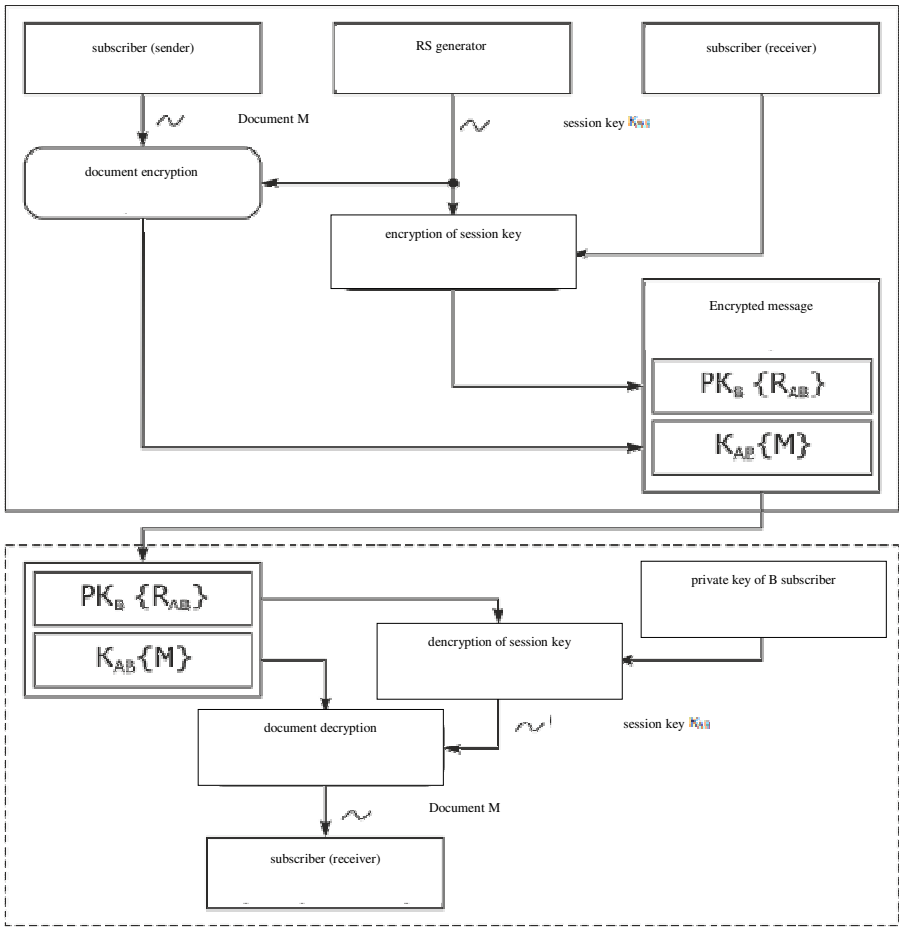

Figure. –Exchange scheme of 2 keys

Conclusion. After analysing what was said above, we can conclude that the encryption algorithm developed can successfully compete with analogues at the moment. At the same time, the developed scheme provides a great opportunity to implement additional functions and settings.

REFERENCES

1. Мао, Венбо. Современная криптография: теория и практика : [пер. с англ.] / Мао, Венбо. – М. : Вильямс, 2005.
2. Pointcheval, D. HD-RSA: hybrid dependent RSA, a new public-key encryption scheme. Submission to IEEE P1363: A symmetric Encription, 1999.
3. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты / А.А. Петров. – ДМК, 2000.