UDC 004.056.55

ADVANCED DATA ENCRYPTION TECHNIQUES

© Tepechin R.I., Moiseev I.A., Lopyreva S.A.

Samara National Research University, Samara, Russian Federation

e-mail: volumejke@gmail.com

Today we are going to tell you about two advanced techniques which are widely used in modern encryption. Encryption is a process in which information is encrypted in such a way that only a certain number of people can view it. There are two main encryption methods, that are most effective nowadays – symmetric and asymmetric. Let’s start by looking at symmetric encryption to understand why asymmetric encryption was created.

Alice has an important document to send to Bob. She uses encryption software to protect this document with a password. Then she sends an encrypted document to Bob, but Bob is unable to open the document because he does not know the password that Alice used to encrypt the document. In simple terms, Bob doesn’t have the key to open the lock. And here comes the big problem: how can Alice safely transfer the password from the document to Bob? Sending a password via her email is risky enough, because intruders can intercept the password and use it to decrypt any messages between Alice and Bob [1].

Nowadays such modern symmetric encryption algorithms as Data Encryption Standard (DES), 3DES (or «triple DES») and International Data Encryption Algorithm (IDEA) are widely used. These algorithms encrypt messages in 64-bit blocks. If a message capacity exceeds 64 bits (as is usually the case), it must be split into 64-bit blocks each, and then somehow bring them together [2].

Triple DES (3DES) is a symmetric block cipher based on the DES algorithm, intended to eliminate the main disadvantage of the latter, namely the small length of the key (56 bits), which can be cracked with a full key search. The speed of 3DES is three times slower than that of DES, but the crypto-resistance is much better. The time required for 3DES cryptanalysis may be much longer than the time needed for DES autopsy [3].

The International Data Encryption Algorithm (IDEA), originally called Improved Proposed Encryption Standard (IPES), is a symmetric-key block cipher described in 1991. The algorithm was intended as a replacement for the Data Encryption Standard (DES).

Encryption with a private key is often used to support data confidentiality and is very effectively implemented with the help of invaded programs. This method can be used to authenticate and maintain data integrity [4].

The following problems are related to the symmetric encryption method:

Secret keys need to be changed very often as there is always a risk of their accidental disclosure (compromise); It is difficult to ensure the security of secret keys when they are generated, distributed and stored. This is precisely the problem that asymmetric encryption intends to solve, so let’s look at it in more detail.

Asymmetric encryption Is like a mailbox on the street. The mailbox is available to anyone who knows its address. You could say the location of the mailbox is entirely public. Anyone who knows the address of the box can put the letter there, but only the owner of the mailbox has a key to open it and read the letters. Using asymmetric encryption, Bob and Alice must generate a key pair on their computer. The most popular and safe method for key generation is RSA Algorithm. This algorithm generates a public key and a private key that are mathematically linked. The public key can be used to encrypt information. And only a certain private key can be used to decrypt it. Given that both keys are mathematically related, a private key cannot be derived from a public key. In other words – if you know someone’s public key, you can’t get his private key.

Now let’s look at how Alice and Bob will use asymmetric encryption to transmit information safely. They start by exchanging their public keys. Bob gives his public key to Alice, and Alice gives his public key to Bob. Now Alice can send an important document. She encrypts the document using Bob’s public key, then sends an encrypted file to Bob, who uses his private key to decrypt the document. In other words, using asymmetric encryption, only Bob can decrypt the encrypted document. Even Alice can't decrypt this document, because only Bob's private key is appropriate. The security of the asymmetric encryption now rests on Bob and Alice's shoulders: she must keep her private keys in a secure location so that Alice only has access to Alice's private key, and Bob only has access to Bob's. If the intruder takes possession of Alice's private key, he can decrypt all the incoming messages that were encrypted with her public key, but the intruder cannot decrypt the message from Alice, as it requires Bob's private key. Asymmetric encryption is used in many cases where security really matters. You may not have known, but every time you visit a site with HTTPS, you use asymmetric encryption. Asymmetric encryption is also used to protect electronic messages [1].

Lets have a look at most effective asymmetric algorithms:

Diffie-Hellman is one of the first recorded examples of asymmetric cryptography, where both sides must first exchange keys over some secure physical channel. Diffie-Hellman eliminated the need for secure exchange by creating an additional key, the public key.

The Rivest-Shammir-Adleman algorithm, better known as RSA, is currently the most widely used asymmetric cryptosystem on the Internet. RSA is a slow algorithm, so it is used to encrypt and decrypt symmetric keys, which in turn encrypt and decrypt messages. Symmetric keys do most of the work, and RSA creates a reliable and secure channel.

ECC stands for cryptography with elliptic curves, which is an approach to public-key cryptography based on elliptic curves over finite fields. Cryptographic algorithms typically use mathematical equations to decrypt keys [5].

In conclusion, symmetric encryption algorithms are much faster and require less computational power, but their main disadvantage is key distribution. Since the same key is used to encrypt and decrypt information, this key must be given to all who need access, which naturally creates certain risks (as described earlier). In turn, asymmetric encryption solves the key distribution problem by using public keys for encryption and private keys for decryption. The trade-off is that asymmetric systems are very slow compared to symmetric systems and require much more computational power [6].

References

1. URL: https://mpdblog.ru/chto-takoe-assimetrichnoe-shifrovanie-i-kak-eto-ispolzuetsya-v-kriptovalyutax.
2. URL: https://artemsannikov.ru/cisco/cisco-security/symmetric-encryption-csec.
3. URL: https://ru.wikipedia.org/wiki/Triple_DES.
4. URL: https://askwiki.ru/wiki/International_Data_Encryption_Algorithm.
5. URL: https://proverkassl.com/book_algoritm_glossary.html.
6. URL: https://academy.binance.com/ru/articles/symmetric-vs-asymmetric-encryption.