Laboratory work № 8.

The subscriber station secure e-mail.

Topics:

¬ Software and hardware for generating key information
¬ The use of electronic signature and encryption when exchanging messages via E-mail Objectives:
Installing Software Center key generation. Generation of the key information. Installation email program. The exchange of public keys. Message exchange.

Stages:
1. Install and work with Crypton emulator v1.4.
2. Installing and Using DiKey
3. Installing and Using DiPost

Crypton emulator v1.4 - a driver that emulates the work of devices of cryptographic protection of data series "Krypton" in the operating environments Windows NT 4.0 and Windows 95/98. Before installing the driver on your computer should be set Crypton API version 2.25 or higher.

DiKey Program - Center for key generation (STG) - performs the generation of the file with the key information required for program operation DiPost if cryptographic information protection is implemented in DiPost.
Dipost program - a client program email subscriber

Cryptography today

Modern cryptography conventionally includes four major sections:

- Symmetric cryptosystem

- Public-key cryptosystems

- Electronic signature system

- Key management

Moreover, the electronic signature systems are built on the basis of, or with the use of public-key cryptosystems. Key management is necessary to ensure the efficiency of the above cryptosystems.

Imagine that you need to pass a certain message (email, file, or something else) sent through open communication (eg over the Internet), and you do not want anyone but him [the recipient] could read and understand the meaning of this message. Since the information will be transmitted over public communications, it may intercept or distort during shipment ... How is it possible to fight?

Encryption

In cryptographic terminology, the original message is called plaintext (cleartext). Changing the source code so that others hide from its contents, called encryption or encoding (encryption). The encrypted message is called ciphertext (ciphertext). The process by which the ciphertext is extracted from the plaintext is called decipherment (decryption). Typically, in the process of encryption and decryption using a key (key), or a pair of keys - public and private (public, private key), and the algorithm ensures that decryption can be done only by knowing the key.

Algorithms using keys are divided into two classes: symmetric (or algorithms, secret key) and asymmetric (or public key algorithms). The difference is that symmetric algorithms use the same key for encryption and decryption (or the decryption key simply calculated by encryption key). While Asymmetric algorithms use different keys, and the decryption key can not be calculated from the encryption key.

Symmetric algorithms are divided into stream ciphers and block ciphers. Streaming allows you to encrypt the information bit-wise, while the block work with a certain set of data bits (usually the block size is 64 bits) and cipher this set as a whole.

Asymmetric ciphers (also called public-key algorithms, or - more generally - of public key cryptography) permit a public key is accessible to all (for example, published in the newspaper). It allows anyone to encrypt a message. However decipher this message can only owner of the private key. The key for encryption is called the public key, and the key for decryption - the private key or secret key

Electronic digital signature

Some asymmetric algorithms may be used to generate an electronic signature (digital signature or electronic signature, an electronic signature or - all three terms are used in the literature in Russian). The digital signature is called a data block generated by using some secret key. Thus with the public key can verify that the data was actually generated using this secret key, that is, to confirm the original author of a message or document and, in addition, check the integrity of the sent message (if it is not corrupted during transmission). generating a digital signature algorithm must ensure that it was not possible without the private key to create a signature which at check will be accurate (by spoofing protection).

Digital signatures are used to verify that the message came from the sender does not corrupted (assuming that only the sender - author has the secret key corresponding to its public key). Also, signatures are used to time the stamp (timestamp) on documents: the party to whom we trust, signs the document with the timestamp using its private key and thus confirms that the document already existed at the time, declared in time stamps.

Digital signatures can also be used to certify (certification) that the document belongs to a certain person. This is done as follows: the public key and information about who it belongs to, signed by the parties, which we trust. This trusted signer side we can, on the grounds that her key has been signed by a third party. Thus there is a hierarchy of trust. It is clear that a key must be the root of the hierarchy (that is, we trust him, not because he is someone signed, but because we believe a priori that he can be trusted). there is a very small amount of network root keys in a centralized key infrastructure (for example, authorized government agencies, also known as certification agencies or centers). In a distributed infrastructure, there is no need to have a universal for all root keys, each of the parties can trust their set root key (say, your own key and keys, it signed). This concept is called a web of trust (web of trust).

The digital signature of a document is usually created so: from a document generated by the so-called digest (message digest), and added to it information about who signs the document, time stamp, and so on. The resulting string is further encrypted with the private key signing using a particular algorithm. The resulting set of encrypted bits and represents the signature. It is usually applied signature public key of the signer. Recipient first decides for itself whether it trusts the fact that it belongs to the public key, to whom should belong (with the help of a network of trust or a priori knowledge), and then decrypts the signature using the public key. If the signature is properly decrypted and its contents corresponds to the document (the digest, etc..), The message is confirmed.

Available are several methods for creating and verifying digital signatures. The best known is the RSA algorithm (by the way, is also used for data encryption).