Ministry of edukation and Sciences of Republic Kazakhstan
M.O.Auezov South-Kazakhstan state University Hight school “Information Technology and Electricity”
Departament “Computer Engineering and Software”

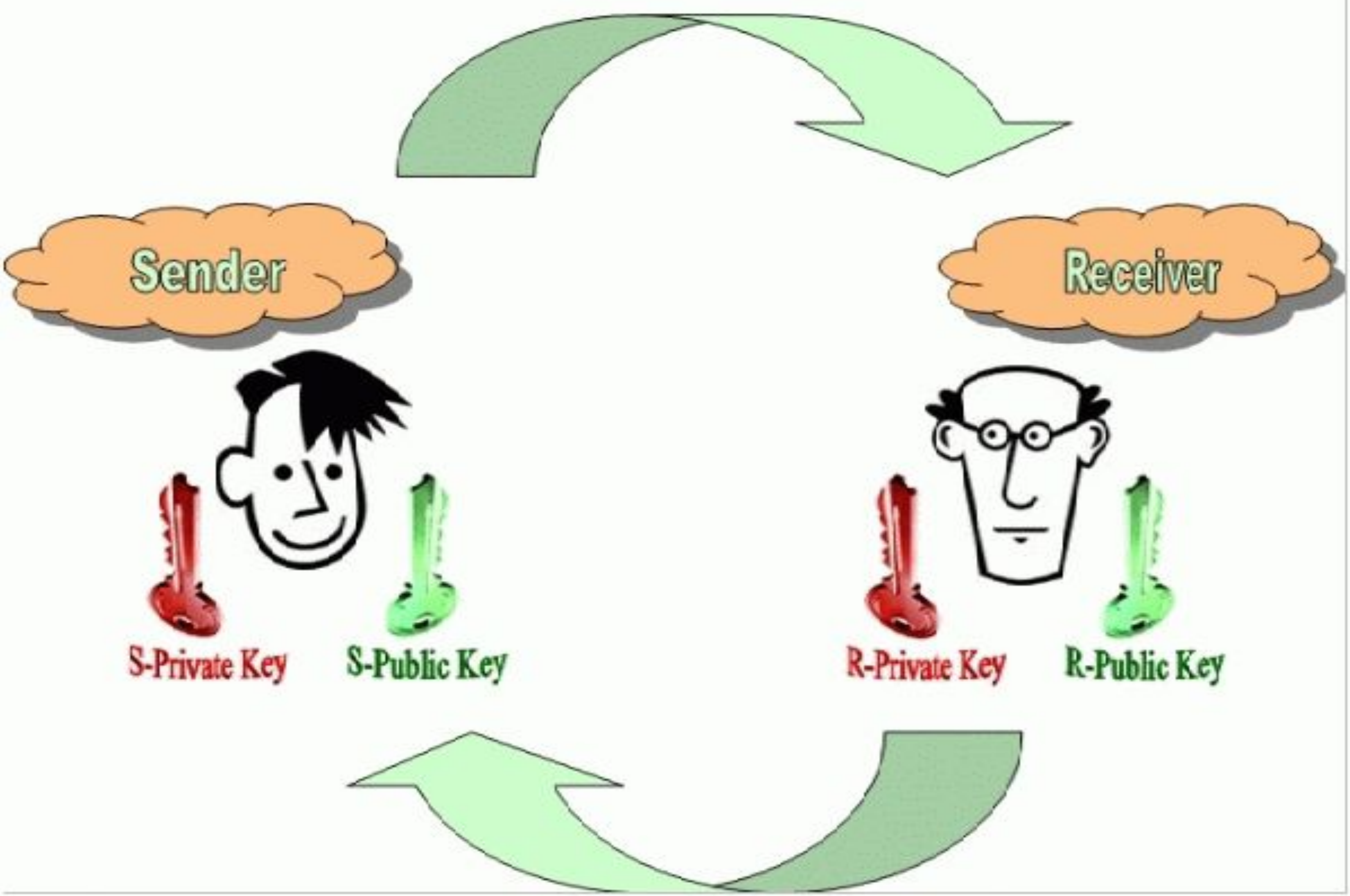
Diffie-Hellman Key Agreement Method

Prepared by:Tiles T.
The group:IP-13-6a2
Checked by :N.N.Dausheyeva

Encryption

- "All that is necessary for safety - a quality encryption".
- This assertion can be heard everywhere. If the information is protected by encryption, no one can read it or change it. Encryption can still be interpreted as authentication.
- Encryption - the most important means of ensuring security. The encryption mechanisms help protect the confidentiality and integrity of information, to identify the source of the information. However, the encryption itself is not a solution to all problems. It is only a delaying action. It is known that any encryption system can be hacked.

Public Key Cryptography



Basic encryption concepts

- Encryption is hiding information from unauthorized persons providing at the same time authorized users to access it. Members are called authorized, if they have the appropriate key to decrypt the information.
- The goal of any encryption system is to maximize the complexity of access to information by unauthorized persons even if they have the ciphertext and know the algorithm used to encrypt. While an unauthorized user does not have the key, privacy and integrity of the information is not broken.

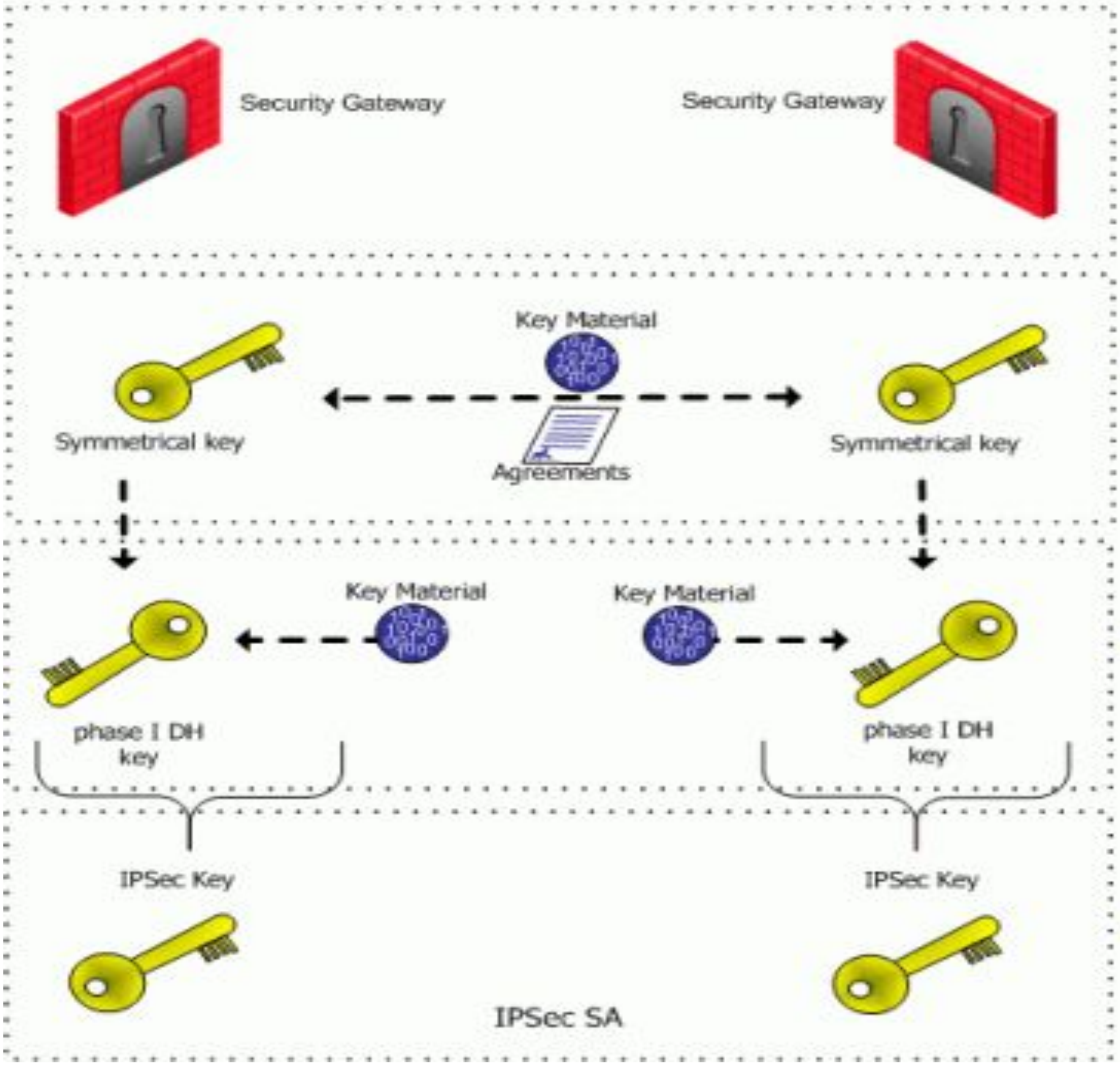
- Using encryption provides three security status information.

- Confidentiality. Encryption is used to hide information from unauthorized users during transmission or storage.
- Integrity. Encryption is used to prevent change of information in transit or storage.
- Identifiability. Encryption is used to authenticate the source of information and the prevention of failure information from the sender to the fact that data has been sent to them.

Terms related to encryption

- Plain Text - information in its original form, also known as plaintext.
- ciphertext - information, expose the encryption algorithm.
- algorithm - a method used to convert plaintext into ciphertext.
- key - the input data by using the algorithm which is a transformation of plaintext into ciphertext, or vice versa.
- Encryption - the process of converting plaintext into a cipher.
- decryption - the process of converting plain text into cipher.

IKE Phase II



- Peers exchange more key material and agree on encryption and integrity methods for IPSec
- DH key is combined with the key material to produce the symmetrical IPSec key
- Symmetrical IPSec keys used in bulk data transfer

There are four terms that you need to know:

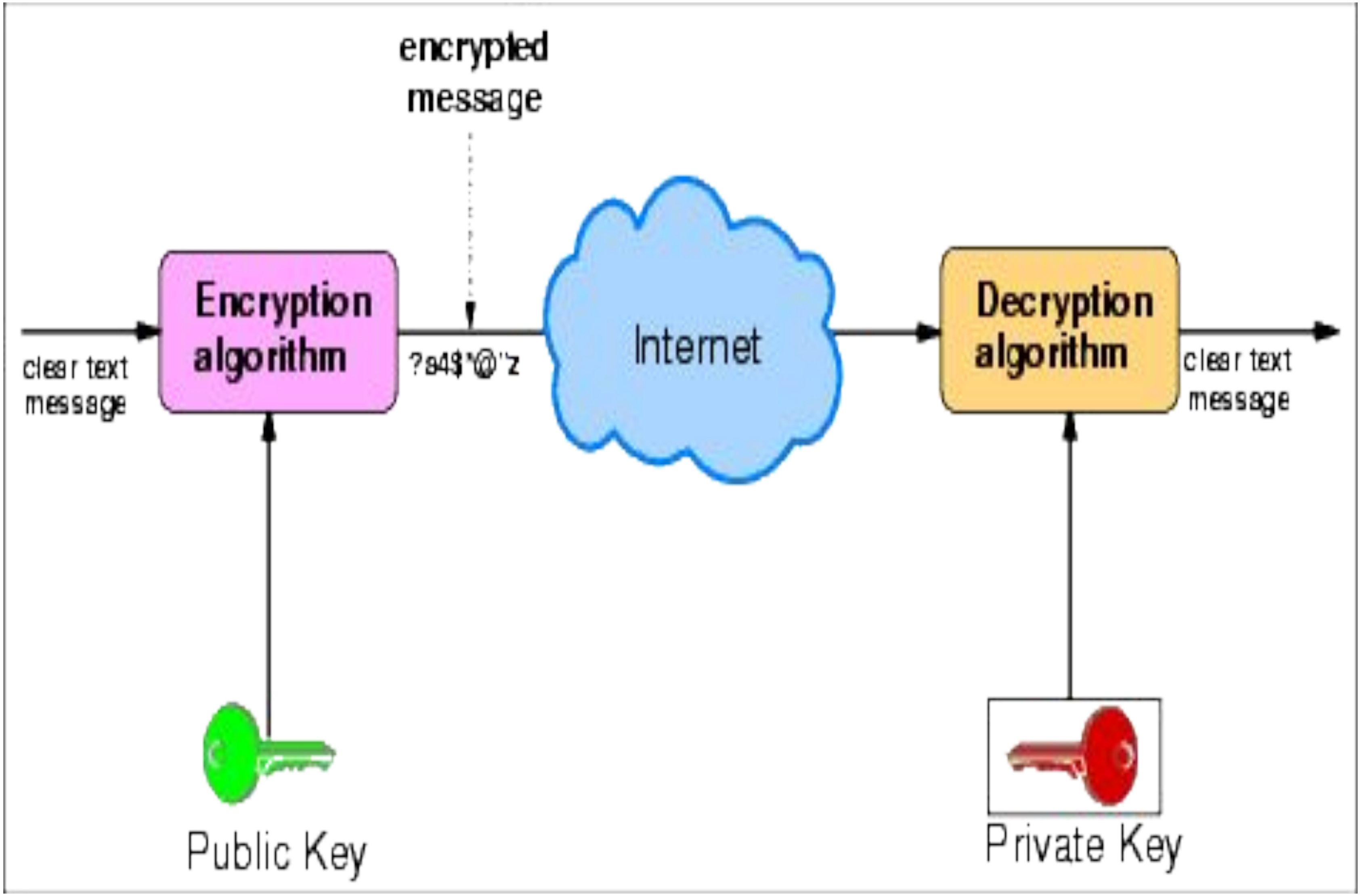
- cryptography - the science of hiding information by using encryption.
- cryptographer - a person engaged in cryptography.
- cryptanalysis - the analysis of the art of cryptographic algorithms for vulnerabilities.
- cryptanalyst - person who uses cryptanalysis to identify and use vulnerabilities in the cryptographic algorithms.

Attacks on the encryption system

- encryption systems can be subject to attacks in three ways:
- by weaknesses in the algorithm;
- attack by "brute force" in relation to the key;
- through a vulnerability in the system environment.
- Carrying out an attack on an algorithm cryptanalyst shows vulnerability in the method of converting plaintext into cipher to reveal the plaintext without using the key.
- Attacks "brute force" - the selection of any possible attempts to convert the cipher key in plain text. In this case, the longer the key, the more the total number of keys, and the more keys should an attacker to try it finds the correct key. If you have the required amount of time and resources, the attack ends successfully. Hence the conclusion algorithms must be evaluated over a period of time during which the information is protected during this attack. The algorithm is regarded as safe if the cost of obtaining key using the attack "brute force" exceed the cost of the protected information.
- Using the computer system vulnerabilities tend to be discussed in the context encryption. However, in practice very easy to attack a computer system than the encryption algorithm.
- Conclusion: The system is just as much impact on the overall security of encryption than the encryption algorithm and key.

Encryption with a secret key

- There are two basic types of encryption: a secret key and a public key.
- Secret-key cryptography requires that all parties have the right to read the information, have the same key. It will be necessary only to protect the key.
- Public key encryption - the most widely used encryption method, because he shall ensure the confidentiality of information and ensure that information remains unchanged in the course of transmission.


encrypted message
Encryption algorithm
clear text message
?a4$'@'z
Internet
Decryption algorithm
clear text message
Public Key
Private Key

The essence of a secret encryption key

- The essence of a secret encryption key
- Encryption secret key is also called symmetric encryption because it uses the same key to encrypt and decrypt data, ie, the sender and receiver of information must have the same key.
- Secret-key cryptography provides confidentiality of the information in an encrypted state. Decrypt message Only those who know the key. Encryption private key quickly and easily implemented using hardware or software.

Substitution cipher

- Substitution cipher processes at one time a single letter of the plaintext. The message can be read both by subscribers using the same permutation scheme. Key in the code number of the substitution is a shift of letters, either completely reordered alphabet.
- Disadvantage: constant frequency of letters in the alphabet of the source, ie, any letter, repeated very often. With enough ciphertext, you can find a sequence of characters and crack any code.

Disposable pads

- Disposable pads (One-time Pad, OTP)
- The only theoretically uncrackable encryption system, which is a list of numbers in a random order, used to encode the message. OTP only be used once.
- Disposable pads are used in IT environments with a very high level of security (but only for short messages).

- Disadvantage: the generation of truly random and the problem of the proliferation of notebooks notebooks. In other words, if the notebook is detected, it is disclosed and that the information he is protecting. If the pads are not random - can be identified schemes that can be used to analyze the frequency of occurrences of.

The operation of one-time pad

Message	S	E	N	D	H	E	L	P
Letters, replaced by the corresponding numbers	19	5	14	4	8	5	12	16
A one-time pad	7	9	5	2	12	1	0	6
Adding plaintext into OTP	26	14	19	6	20	6	12	22
The cipher text	Z	N	S	F	T	F	L	V

Data Encryption Standard (DES)

- Data Encryption Standard algorithm (DES) was developed by IBM in the early 1970s. National Institute of Standards and Technology (NIST) has adopted the algorithm (FIPS Publication 46) for the DES in 1977 after studying, modification and approval of the algorithm in the NSA. The algorithm was further modified in 1983, 1988, 1993 and 1999.

- DES uses a key length of 56 bits. Uses 7 bits of a byte, eight bits of each byte is used for parity. DES is a block encryption algorithm, the processing at the same time a 64-bit block of plaintext. The DES algorithm encryption performed 16 cycles with a different subkey in each of the cycles. The key is exposed to its own algorithm for the formation of 16 subkeys.

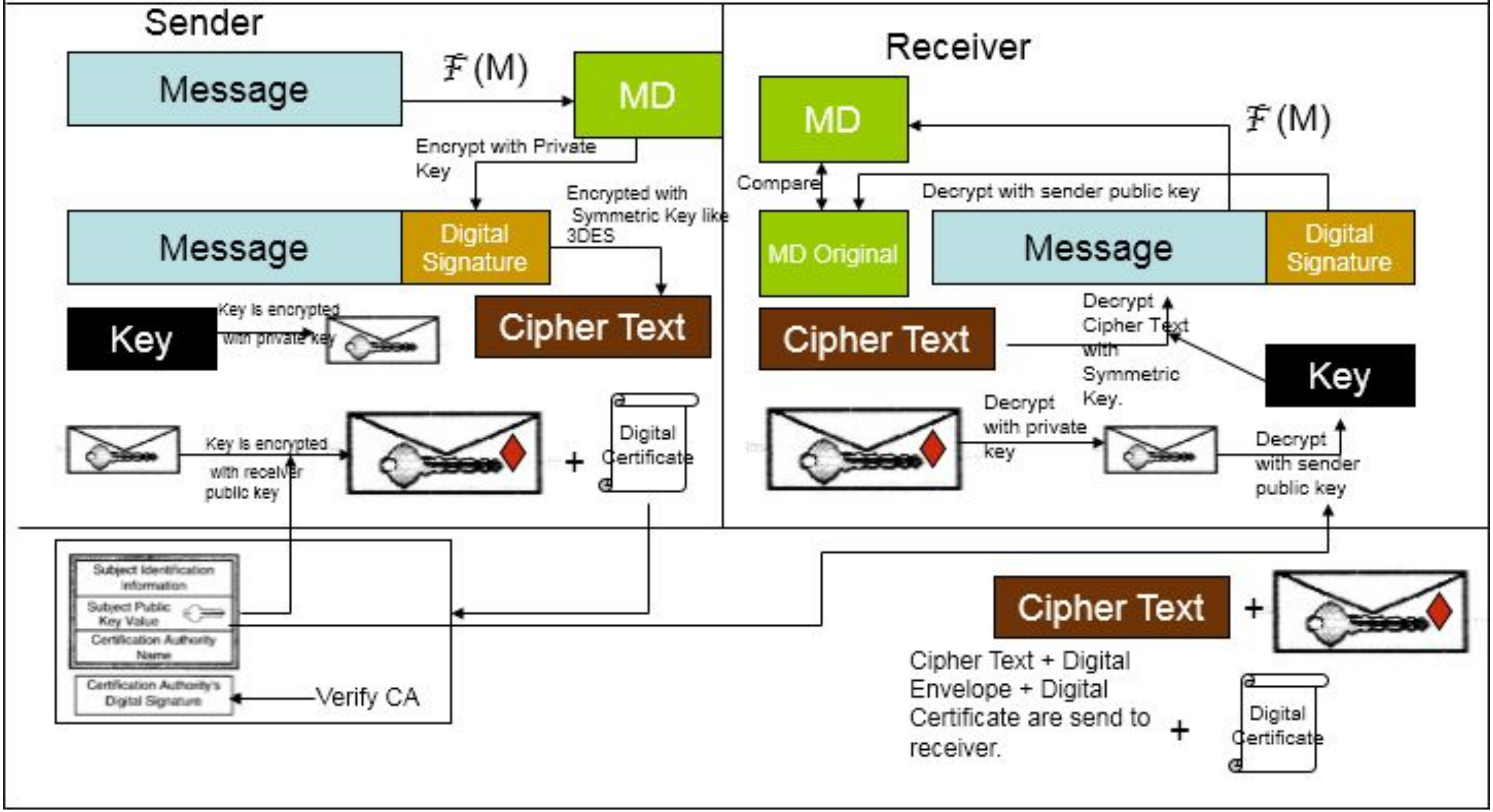
DES algorithm can operate in four modes

- Electronic codebook - a basic block encryption algorithm, in which the text and the key are combined to form a ciphertext. This mode is identical to the input form is identical to the output;
- The chain blocks. Encrypting each block occurs in electronic shifrbloknote, but with the addition of a third component derived from the previous output. Identical input (plaintext) is not substantially identical to the output;
- Feedback on the cipher text. As input data previously generated using DES cipher text. After that, the output data are combined with the plaintext and ciphertext new form;
- Feedback on the door. similar to the feedback mode over an encrypted text, but here we use the output of the DES, and there is no chaining of ciphertext.
- DES key can be determined by the attack "brute force" in 35 minutes.

Encrypt passwords

- Each user has his own password. The algorithm uses the first eight characters of the password. When a password length of eight characters, it is truncated, if shorter, it is padded. The first 7 bits of each character in a password is converted 56-bit number, using the first seven bits of each symbol. Thereafter, the system selects 12.bitnoe number based on the system time. This element is called "grain of salt" or extension. Expansion and password are used as input in the password encryption function. Extension is used to change one of the table in the permutation algorithm DES (permutation E) any of 4096 different ways, depending on the number of units in twelve bits. Basic plain text contains 56 zero bits, and 56 bits key is derived from the password. The algorithm is performed 25 times, and the input of each stage is the output of the previous stage. The final output data are converted into 11 symbols, and the expansion is converted into two symbol and placed before the final output data.
- The vulnerability is based on choosing a password, since most computer users use passwords, the number of possible combinations which is equal to 268, which is less than 255 possible DES keys.

How does PKI Work?



Sender

Message

Ƒ(M)

MD

Encrypt with Private Key

Message

Digital Signature

Encrypted with Symmetric Key like 3DES

Key

Key is encrypted with private key

Cipher Text

Key is encrypted with receiver public key

+

Digital Certificate

Subject Identification Information

Subject Public Key Value

Certification Authority Name

Certification Authority's Digital Signature

Verify CA

Receiver

MD

Ƒ(M)

Compare

Decrypt with sender public key

MD Original

Message

Digital Signature

Cipher Text

Decrypt Cipher Text with Symmetric Key.

Key

Decrypt with private key

Decrypt with sender public key

Cipher Text

+

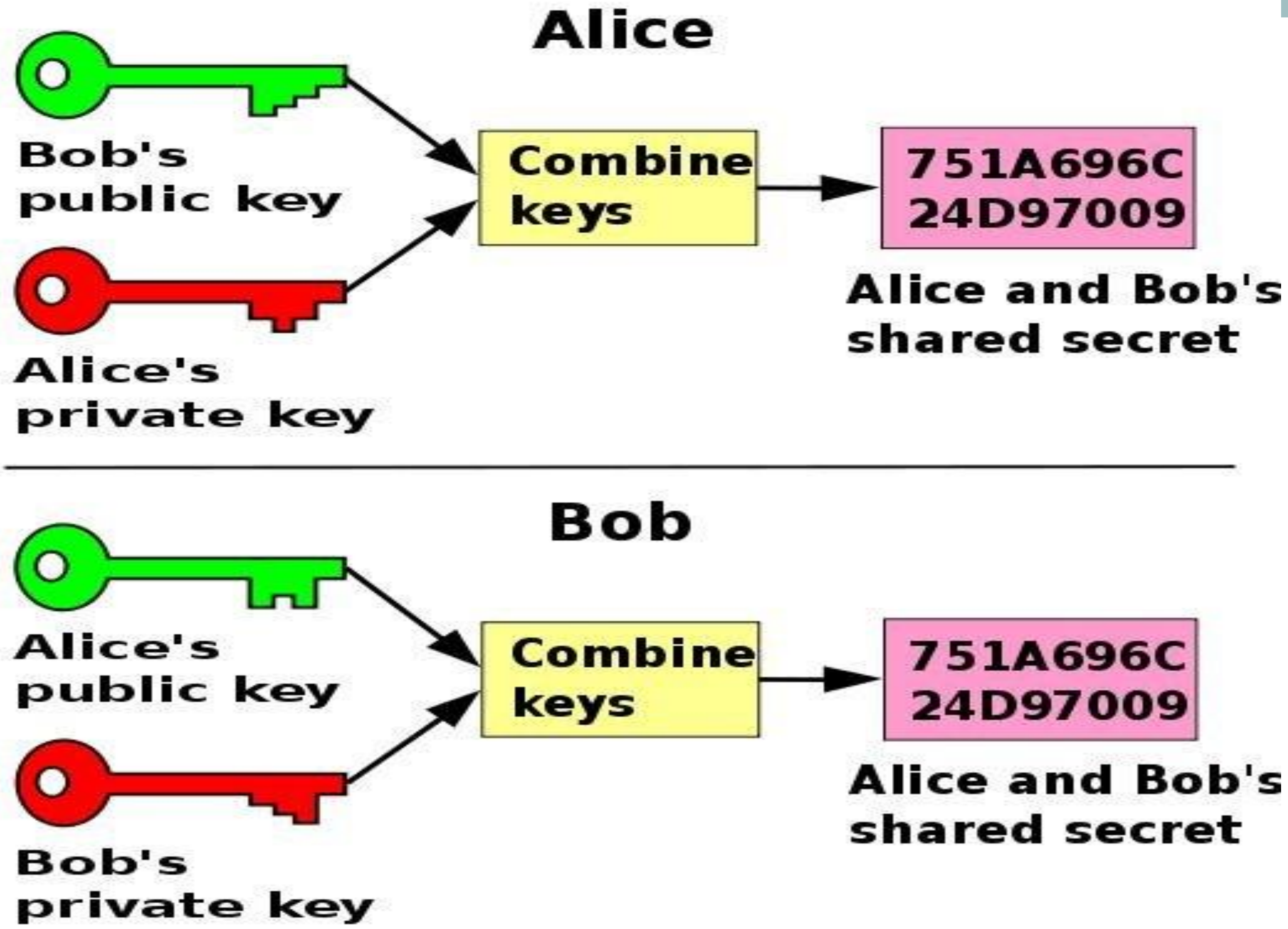
Cipher Text + Digital Envelope + Digital Certificate are send to receiver.

+

Digital Certificate

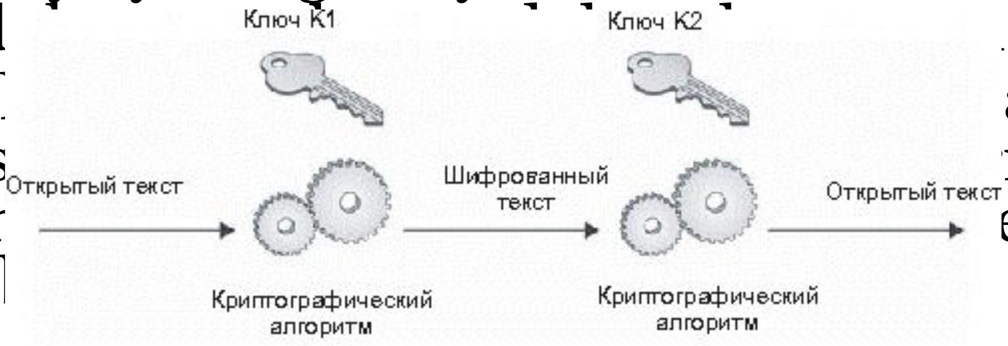
Rijndael Advanced Encryption Standard

- Rijndael Advanced Encryption Standard
- Rijndael algorithm - an algorithm selected in view of its power, applicability to high-speed networks, as well as the possibility of a hardware implementation. It is a block cipher that uses keys, and blocks 128, 192, or 256 bits, which suppresses the attack using brute force. This encryption algorithm consists of 10-14 cycles depending on the size of the key and the plaintext block size. Other encryption algorithms with a secret key
- Different security systems can be distinguished with a secret key encryption algorithms.
- IDEA (International Data Encryption Algorithm. Switzerland). The IDEA uses a 128-bit key; In addition, IDEA is also used in Pretty Good Privacy (PGP).
- RC5. Designed by Ron Rivest at MIT Institute, and allows the use of keys with variable length.
- Skipjack. Developed by the US government for use with the Clipper Chip and uses 80-bit key, which in future will be the unacceptable.
- Blowfish. Allows the use of variable key length to 448 bits; algorithm is optimized to run on 32-bit processors.
- Twofish. It uses 128-bit blocks and keys of 128, 192 or 256 bits.
- CAST-128. It uses a 128-bit key and is used in the new versions of PGP.
- Algorithm Standard (GOST 28147-89). Russian Encryption Standard, developed in response to on DES, the which uses a 256-bit key.
- All these algorithms typically are powerful enough to be used for general purposes.


Alice
Bob's public key
Alice's private key
Combine keys
751A696C 24D97009
Alice and Bob's shared secret
Bob
Alice's public key
Bob's private key
Combine keys
751A696C 24D97009
Alice and Bob's shared secret

Public-key cryptography

- The encryption algorithms used with two key public key. One key - to encrypt the information, the other - at decipherment.
- Public-key cryptography
- Both parties (sender and recipient) must have the key. Keys are associated with each other (so they are called a key pair), but they are different. That is, if the message is encrypted with the key K1, then the message can be decrypted only by using a key K2. And vice versa. Thus one is called .
- The private air. The public key is mation in the clear, si e other key can not



Diffie-Hellman key

- exchange algorithm Diffie-Hellman key
- Whitfield Diffie (Whitfield Diffie) and Martin Hellman (Martin Hellman) developed a public key encryption system in 1976. The system of Diffie-Hellman (Diffie-Hellman) was designed to address key distribution using encryption systems with secret keys. The idea was to use a secure method of matching private key without transmitting the key in any other way. Therefore, it was necessary to find the safest way to get the secret key using the same method of communication for which protection was developed. Diffie-Hellman algorithm can not be used to encrypt or decrypt information.

The algorithm Diffie-Hellman

- Two subscribers (P1 and P2) agree on an encryption key for use between a secure connection.
- P1 and P2 are used two big integers a and b, and 1 <a <b.
- P1 i picks a random number and calculates I = ai mod b, and transmits the subscriber I P2.
- P2 j selects a random number and calculates J = aj mod b, J and transmits subscriber P1.
- P1 calculates k1 = Ji mod b.
- P2 calculates k2 = Ij mod b.
- We have k1 = k2 = ai * j mod b. Hence the conclusion, k1 and k2 are the secret keys, intended for use in the transmission of other data.

Explanation of Diffie-Hellman:

- «Mod» - is the remainder. For example, 12 mod 10 = 2. Two - is the remainder after dividing 12 by 10.
- While listening to an attacker traffic transmitted by cable, it will be known a, b, I and J. However, remain secret i and j. What will be harder to find when i known I = ai mod b, the higher the security level. This problem is called the discrete logarithm problem and is considered to be very difficult (ie. E. With the help of modern computer equipment to solve it practically impossible), if the numbers are very large. Consequently, a and b must be chosen very carefully, both the number and b (b - 1) / 2 must be simple and have a minimum length of 512 bits and 1024 bits is better.

- Disadvantage: it can be vulnerable to attacks by the intermediary. In other words, when you place your computer by an attacker between the subscribers P1 and the P2, connect it to the communication channel and to intercept all information transmitted, he will be able to exchange data with the P2, posing as P1, and P1 in the guise P2. Implementation of such an attack requires a large amount of resources, and in the real world such attacks are rare.

The RSA algorithm

- The RSA algorithm
- Rivest-Shamir-Adleman (RSA) public key is used for encryption and decryption.
- The basic algorithm to provide data confidentiality:

- = Cipher text (plain text) e mod n
- Plaintext = (ciphertext) d mod n
- Secret key = {d, n}
- Public key = {e, n}

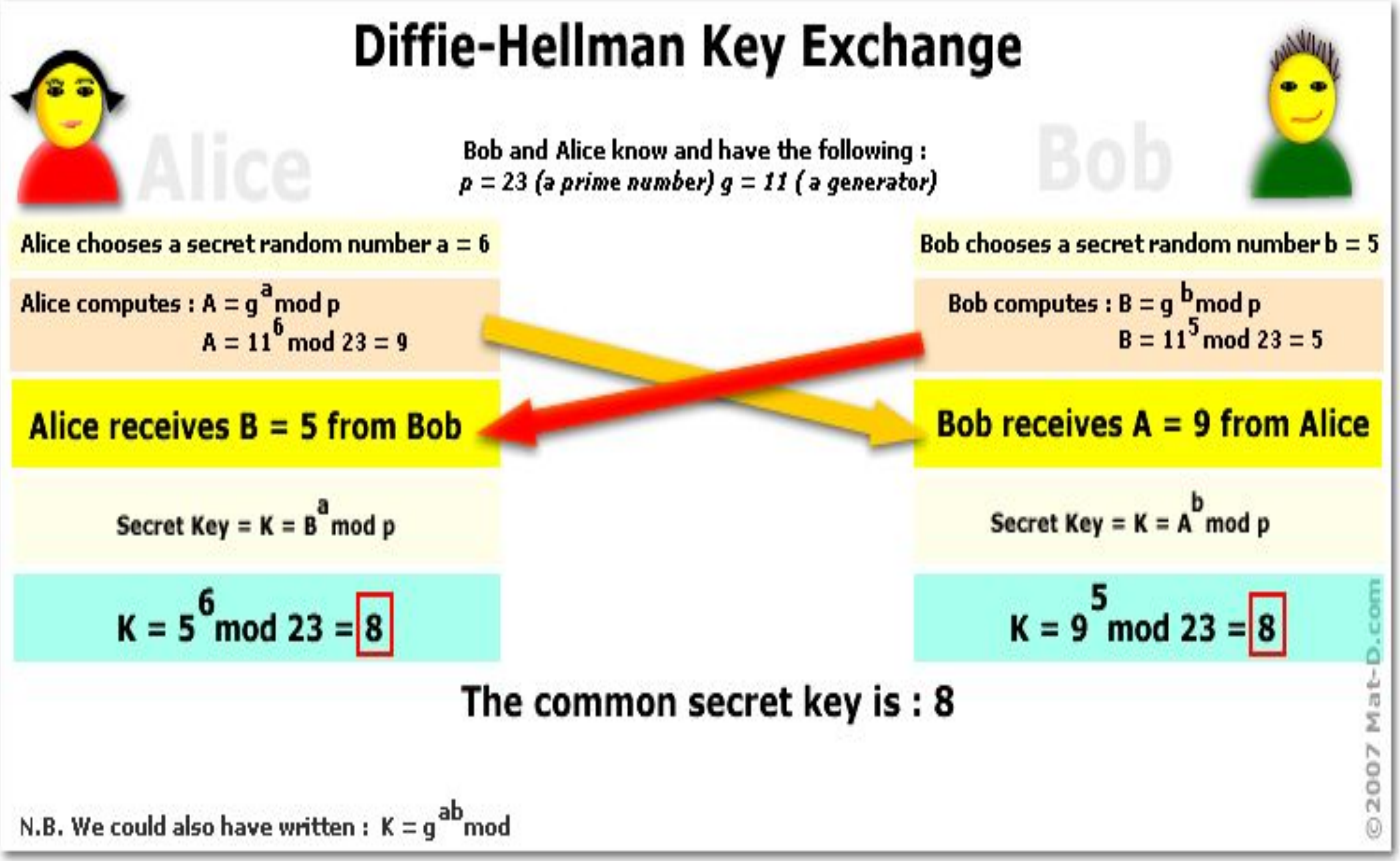
- Security is provided by the complexity of calculating the d in the presence of known e and n, that the owner of the key pair keeps the private key secret, and that the public key is transmitted in clear text. Consequently, when encrypting with the public key, it can decrypt only the owner of the key pair.
- To ensure the authentication of the sender algorithm acquires the following form.

- = Cipher text (plain text) d mod n
- Plaintext = (ciphertext) e mod n
- Secret key = {d, n}
- Public key = {e, n}

- For authentication information is encrypted using a private key. Any person can decrypt the data and verify that the data was received from the owner of the key pair.

Generation of RSA keys

- Generation of RSA keys
- Are selected and kept in secret two prime numbers p and q.
- We compute n = pq.
- Compute f (n) = (p - 1) (q - 1).
- Vyberaem is e, that it is mutually prime with respect to f (n).
- Such designation d, to (d) (e) = 1 mod f (n) and d <f (n).



Diffie-Hellman Key Exchange

Alice

Bob

Bob and Alice know and have the following :
$p = 23$ (a prime number) $g = 11$ (a generator)

Alice chooses a secret random number $a = 6$

Alice computes : $A = g^{a} \bmod p$
$A = 11^{6} \bmod 23 = 9$

Alice receives B = 5 from Bob

Secret Key = $K = B^{a} \bmod p$

$K = 5^{6} \bmod 23 = \boxed{8}$

Bob chooses a secret random number $b = 5$

Bob computes : $B = g^{b} \bmod p$
$B = 11^{5} \bmod 23 = 5$

Bob receives A = 9 from Alice

Secret Key = $K = A^{b} \bmod p$

$K = 9^{5} \bmod 23 = \boxed{8}$

The common secret key is : 8

N.B. We could also have written : $K = g^{ab} \bmod$

©2007 Mat-D.com

Example with easily verifiable numbers.

- Choose the number p = 11 and q = 13.
- We calculate n = pq. We have n = 11 x 13 = 143.
- We compute f (n) = (p - 1) (q - 1) = (11 - 1) (13 - 1) x 12 = 10 = 120.
- Select the number of e so that it is relatively simple f (n). Here, the value e = 7 was chosen.
- It is necessary to determine a d, to (d) (e) = 1 mod f (n). Therefore, (d) (7) = 1 mod 120; d should be less than 120. We find that d = 103. (103 multiplied by 7 and get 721. 721 divided by 120 and get 6 with the remainder of 1.)
- The secret key is {103, 143}.
- The public key: {7} 143.

To run directly encrypt and decrypt using the original formula.

- = Cipher text (plain text) e mod n
- Plaintext = (ciphertext) d mod n

- Suppose you want to send a "9" message.

- The cipher text = (9) 7 143 = 48 mod.

- When a decrypted Info:

- Plaintext = (48) 103 mod 143 = 9.

Algorithm El Gamal
Digital signature algorithm

- Algorithm El Gamal
- El-Gamal (Taher Elgamal) advanced algorithm Diffie-Hellman algorithm, which was used for both encryption and authentication to ensure. Since this algorithm is based on the Diffie-Hellman system, the security of information provided when you use the complexity of solving the discrete logarithm problem.

- Digital signature algorithm
- Digital Signature Algorithm Algorithm (DSA) - the standard algorithm for digital signatures, which is based on ElGamal system, but only allows you to authenticate. Privacy is provided by this algorithm does not.

- Encryption using elliptic curves
- encryption using elliptic curves (ECC) is as follows: given two points A and B on an elliptic curve such that A = kB, very difficult to determine an integer k. The biggest advantage is that the keys have a smaller length (because of the complexity of the problem), causing faster calculations are performed while maintaining security.
- Disadvantage: in this area is still necessary to carry out a number of studies on the existing ECC several patents registered.

The development of encryption systems

- This design is intended to demonstrate the use of encryption in the information system for providing authentication, confidentiality and integrity, it is understood how the use of an encryption system with a private key (AES), and the public key (RSA or Diffie-Hellman).