1. Into

Public key cryptography - is a method of encrypting, which allows individuals to securely communicate without sharing the secret key.

2. Rsa

Asymmetric encryption.

Trapdoor one way function - function that can be easily computed in one way, and hard in the inverse without special(secret) information(trapdoor). In this case forward -> encrypt. Inverse -> decrypt.

Private key - is key to decrypt message. Public key - is key to encrypt message.

For signatures private key enables to sign and public to verify this sign validity.

Arithmetic functions, that considered as a one way(not proofed)

1. Multiplication and factorization
2. x^y mod n = z => find y
3. x^y mod n = z => find x
4. x^2 mod n. n - not prime, jacobi(z/n)=1 => find x
5. g^ab mod p => find a

3. Group

Group is set of elements, that are related to each other according to certain well-defined rules.

Z_p^* - is a group with nonzero integers between 1 and p-1 modulo some prime nomber p.

3.1. Axioms

Operation for example is a multiplication.

1. Closure - $a, b \in G, a * b = c \rightarrow c \in G$
2. Associativity $a * (b * c) = (a * b) * c$
3. Identity existence $a * 1 = a$
4. Inverse existence $a * b = 1$

A group is commutative if $a * b = b * a$

A group is cyclic if

$$g \in G, \forall x \in G, \exists n : g^n = x$$

4. Diffie-hellman

4.1. Discrete logarithm problem

Problem - find the y, where g and x are provided, $g^y = x$.

4.2. Core Equation

$$y_1 = (a^{x_1} \bmod p)^{x_2} \bmod p = a^{x_1 x_2} \bmod p$$

Some modular arithmetics to proof:

$$y_1 = (a^{x_1} \bmod p)^{x_2} \bmod p = \left((a \bmod p)^{x_1} \bmod p\right)^{x_2} \bmod p =$$

Reduce extra modulo due to modulo properties:

$$(a \bmod p)^{x_1} \bmod p = a^{x_1} \bmod p$$

Continue:

$$= (a \bmod p)^{x_1 x_2} \bmod p$$

$$= a^{x_1 x_2} \bmod p$$

4.3. Modular arithmetics

$$(ab) \bmod m = [(a \bmod m)(b \bmod m)] \bmod m$$