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 - $a, b \in G, a * b = c \to c \in G$
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 there is generator g

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

3.2. How to choose or check that a is a generator?

Theorem $g \in Z_p^*$ is a generator of Z_p^* if and only if $g^{\frac{p-1}{q}} \neg \equiv 1 \bmod p$ for all primes q such that $q|(p-1)$

4. Diffie-hellman

Protocol:
1. Choose large prime p and large generator a in Z_p^*, choose x_1, where $0 < x_1 < p - 1$

4.1. Discrete logarithm problem

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

G is generator in group. g^x is uniformly distributed in group.

The problem is that y's can have many values, and we need to try each value.

4.2. Factorization problem

For example RSA relies on difficulty of factoring the product of two large prime numbers.

But for this need to determine or find large prime number.

Determine if number is prime:
1. Simple methods(advanced brute force, without 2,3 and maybe some memoization,etc)
2. Probabilistic tests(all primes + some non primes - never FN, but sometimes FP)