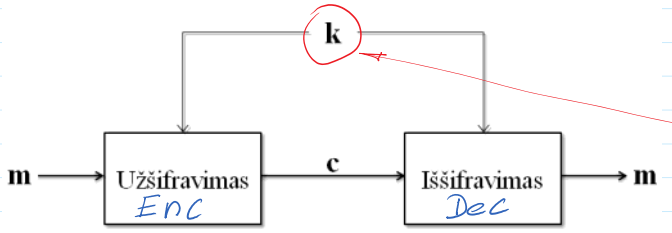
Course work: blockchain, cryptocurrencies
smart contracts, ICO
IoT → 4-th Industrial Revolution

} Oral report
Text ≤ 15 p.
Presentation
~ 12 slides

Midterm exam should be from 8 to 16 week.
It will be arranged during the execises lecture.
https://imimsociety.net/en/14-cryptography
Problems required to solve:
DH-KAP, MiM Attack, ElGamal encryption, ElGamal signature.

Till the 16 week.

Symmetric encryption



Agreed usin Diffie-Hellman Key Agreement Protocol KAP

Vernam cipher ~ 1910

Message m to be encrypted, e.g. $m = 111\,222$

$k = 195\,238\,587$

$A: E(k, m) = c$ — c → — $B: D(k, c) = m$

$m \oplus k = c$ — $c \oplus k = m$

↳ bitwice XOR m with k

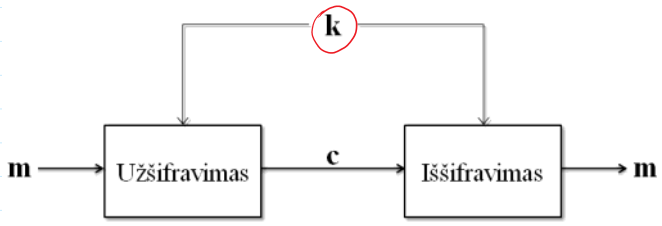
Requirements for Vernam cipher.

1. Key k must be generated random. Cipher security depends on the quality (randomness) of k.
2. Messag m must be at the same length or less than k. $|m| \leq |k|$.
3. Key k must be used one-time for encryption. For every message $m_1, m_2, \ldots$ the ~~different~~ key $k_1, k_2, \ldots$ must be generated.

If these conditions 1, 2, 3 are satisfied ⇒
⇒ Vernam cipher is Perfect Secure.

Other ciphers: Block Ciphers and Stream Ciphers

Other ciphers: Block Ciphers and Stream Ciphers
BC SC
for files encryption data stream encryption



The same secret key k can be used many times for different files encryption and different streams encryption.
For this purpose the psend random number generat. (PRNG) are used:

k → PRNG → S – sequence with a bit length far more than k.

$|k| << |S|$

$AES(k, F) : |k| \in \{128, 192, 256\}$

$|F| = 1\ GB$ $2^{30} = 1073741824$

If we have a set of files $\{F_1, F_2, \ldots, F_N\}$ // $N = 1000\,000$

$AES(k, F_1) = c_1$
$AES(k, F_2) = c_2$
$AES(k, F_N) = c_N$

This encryption is secure.
It has no Perfect Security property.

Asymmetric encryption

ElGamal Cryptosystem

Parameters generation

Strong prime number **p** generation.

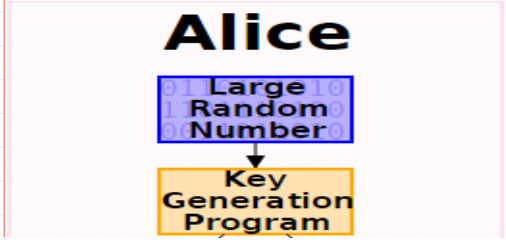
Find a generator **g** in $Z_p^* = \{1, 2, 3, \ldots, p-1\}$ using condition **Fact C.23**.

Strong prime $p=2q+1$, where q is prime, then g is a generator of Z_p^* iff

$g^q \neq 1 \bmod p$ and $g^2 \neq 1 \bmod p$.

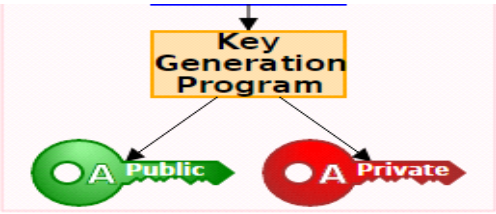
1.Declare **Public Parameters** to the network **PP** = (**p**, **g**); **p=268435019**; **g=2.**

2^28=**268435456**



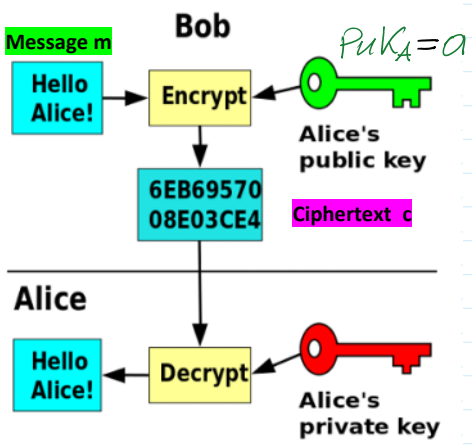
2.***Key generation***

- Randomly choose a private key ***X*** with $1 < x < p - 1$.
- Compute $a = g^x \bmod p$.

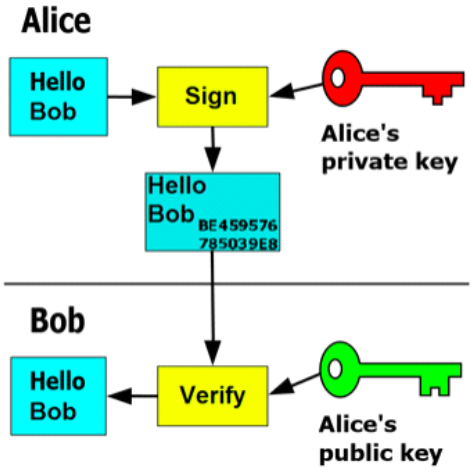


- Compute $a = g^x \bmod p$.
- The public key is PuK = a.
- The private key is PrK = x.

Asymmetric Encryption - Decryption
c=Enc(PuK$_A$, m)
m=Dec(PrK$_A$, c)



Asymmetric Signing - Verification
S=Sig(PrK$_A$, m)
V=Ver(PuK$_A$, S, m), V∈{True, False}≡{1, 0}



El-Gamal Encryption

Let message ***m*** needs to be encrypted, e.g. ***m*** = 111222.

p=268435019 $\Rightarrow m < p \Rightarrow m \bmod p = m.$

A: $PuK_A = a$ → B: is able to encrypt m to A.

B: $r \leftarrow randi(\mathbb{Z}_p^*)$

$E = m \cdot a^r \bmod p$
$D = g^r \bmod p$
$\} c = (E, D)$ → A: is able to decrypt $c = (E, D)$ using her $PrK_A = x$.

1. $D^{-x} \bmod p$
2. $E \cdot D^{-x} \bmod p = m$

$$D^{-x} \bmod p = D^{p-1-x} \bmod p$$

Correctness

$$Enc_{PuK_A}(m, r) = C = (E, D) = (E = m \cdot a^r \bmod p, D = g^r \bmod p)$$

$$Dec_{PrK_A}(C) = E \cdot D^{-x} \bmod p = m a^r \cdot (g^r)^{-x} \bmod p =$$
$$= m \underbrace{(g^x)^r}_{a} \cdot g^{-rx} = m \cdot g^{xr} \cdot g^{-rx} = m \cdot g^{xr-rx} \bmod p = m \cdot g^0 \bmod p =$$
$$= m \cdot 1 \bmod p = m \bmod p = m$$

$= m \underbrace{(g^x)}_{a}{}^{r} \cdot g^{-r} = m \cdot g^{xr} \cdot g^{-rx} \bmod p = m \cdot g^0 \bmod p =$

$= m \cdot 1 \bmod p = m \bmod p = m$

since $m < p$

If $m > p \rightarrow m \bmod p \neq m$; $27 \bmod 5 = 2 \neq 27$.

If $m < p \rightarrow m \bmod p = m$; $19 \bmod 31 = 19$.

Decryption is correct if $m < p$.

ElGamal encryption is probabilistic: encryption of the same message m two times yields the different cyphertexts c_1 and c_2.

1-st encryption:

$r_1 \leftarrow randi(\mathbb{Z}_p^*)$

$E_1 = m \cdot a^{r_1} \bmod p$

$D_1 = g^{r_1} \bmod p$

$\Big\} C_1 = (E_1, D_1)$

$r_1 \neq r_2$

2-nd encryption

$r_2 \leftarrow randi(\mathbb{Z}_p^*)$

$E_2 = m \cdot a^{r_2} \bmod p$

$D_2 = g^{r_2} \bmod p$

$\Big\} C_2 = (E_2, D_2)$

$c_1 \neq c_2$

Security considerations. Total break of cryptosystem (CS) is to find a $PrK = x$.

The data available to compromise CS are the following

$PP = (p, g)$; $PuK = a$; $\{(m_1, c_1), (m_2, c_2), \ldots (m_n, c_1)$

$a = g^x \bmod p$; $\Rightarrow$ to find x it is required to find a discrete logarithm of a:

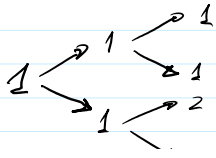
$\log_g(a) = \log_g(g^x \bmod p) \Rightarrow \log_g(a) = x$.

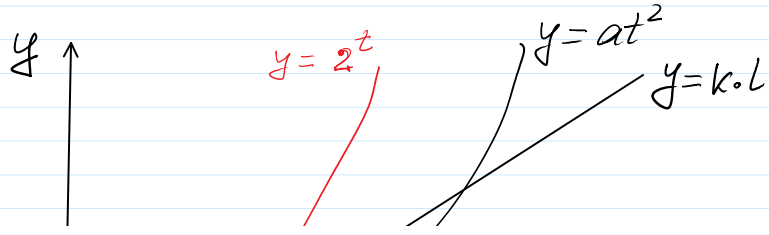
For sufficiently large p to find x is infeasible.

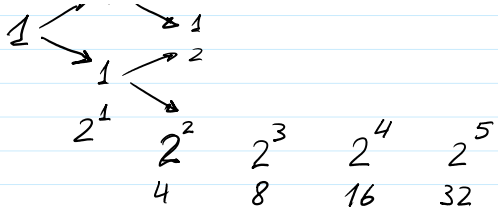
$p \sim 2^{2048} \rightarrow |p| = 2048$ bit length.

Security of ElGamal CS relies on the Discrete Logarithm Assumption – DLA: finding x is infeasible when $PP = (p, g)$ and $PuK = a$ are given.

Function of grows






1
1
1
2
2^1
2^2
2^3
2^4
2^5
4
8
16
32


y = log2 t
t