Lecture 4: Hash functions. Public key cryptography. Digital signatures

Course instructors: Alexey Frolov and Yury Yanovich

Teaching Assistant: Stanislav Kruglik

Technical Assistants: Anton Glebov and Evgeny Marshakov

November 8, 2018

Skoltech
Skolkovo Institute of Science and Technology

Outline

Skoltech
Skolkovo Institute of Science and Technology

Hash function

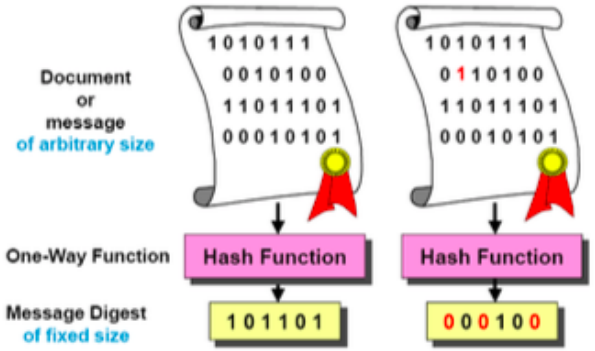
The following mapping $h : \{0,1\}^* \to \{0,1\}^\ell$ is called a hash function.

Skoltech
Skolkovo Institute of Science and Technology

One-way hash function

Let h be a hash function. h is called one-way hash function if the following conditions hold:

- Evaluation of $h(X)$ is a simple operation;
- It is computationally hard task to find $h^{-1}(Y)$.



Skoltech
Skolkovo Institute of Science and Technology

Cryptographic hash functions

- $h : \{0,1\}^* \to \{0,1\}^\ell$
  - Maps arbitrary strings to strings of fixed length
- One-way
- Weak collision resistance
  - For a given X it is difficult to find $Y \neq X$, such that $h(X) = h(Y)$
- Strong collision resistance
  - Hard to find any distinct X and Y, such that $h(X) = h(Y)$
- Security strength of h only depends on ℓ.
- Common examples: SHA-1, MD5

Skoltech
Skolkovo Institute of Science and Technology

Birthday paradox

k-bit hash function, $N = 2^k$. Assume, that the output values have uniform distribution.
The probability, that n values have different hash is as follows:

$$\hat{P}(n) = \prod_{i=0}^{n-1}(1 - i/N) \leq e^{\frac{n(n-1)}{2N}}.$$

Thus, the probability of collision can be calculated as follows

$$P(n) = 1 - \hat{P}(n)$$

$$n_{0.5} \approx \sqrt{2 \log 2} \cdot 2^{k/2}.$$

Skoltech
Skolkovo Institute of Science and Technology

Main principle

Split message into parts: $\{M_i\}_{i=1}^{\ell}$

$$h_i = f(M_i, h_{i-1}), \quad i = 1, \ldots, \ell,$$

where h_0 is some predefined value.

Hash value is a value h_ℓ.

Skoltech
Skolkovo Institute of Science and Technology

Application of cryptographic hash functions

- Password files (one-way)
- Digital signatures –Sign hash of message instead of entire message (collision resistant)
- Data integrity – Compute and store hash of some data & Check later by re-computing hash and comparing (collision resistant)

Skoltech
Skolkovo Institute of Science and Technology

Hash tree

- The concept of hash trees is named after Ralph Merkle who patented it in 1979.
- Hash tree (or Merkle tree) is a tree in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes.
- Hash trees allow efficient and secure verification of the contents of large data structures.

Skoltech
Skolkovo Institute of Science and Technology

Construction

- calculate a hash of each block

$$Hash_{00} = hash(L_1), \;\; Hash_{01} = hash(L_2), \ldots$$

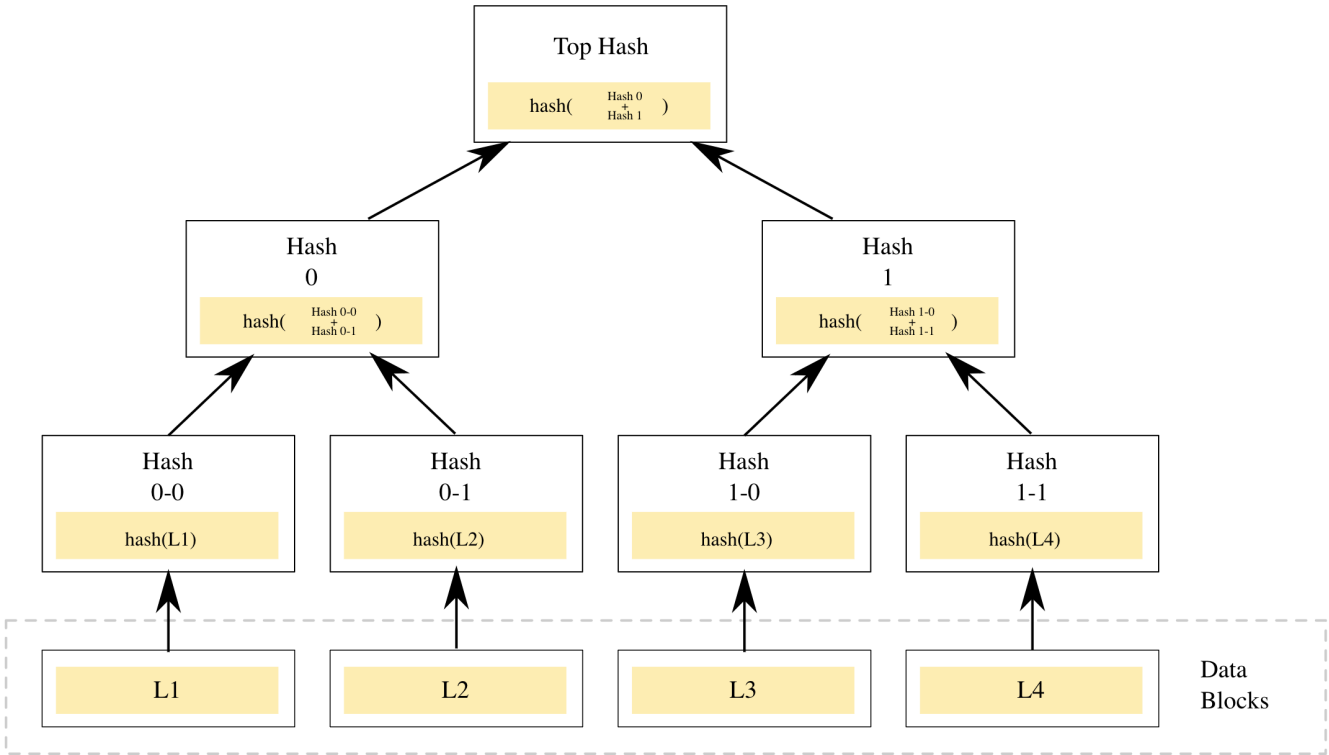
- put these values to the leaves of the tree
- intermediate blocks

$$Hash_0 = hash(Hash_{00} + Hash_{01}),$$

where $+$ means a concatenation.

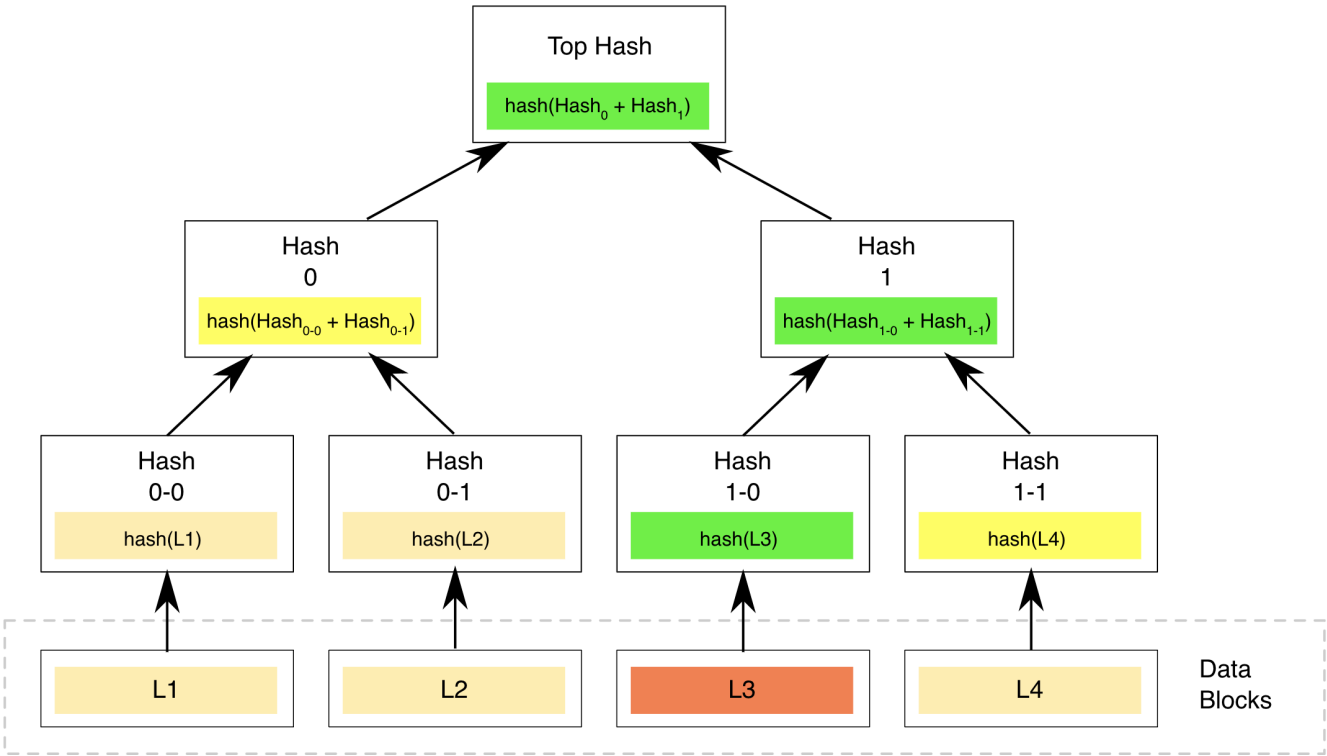
Skoltech
Skolkovo Institute of Science and Technology

Merkle tree



Skoltech
Skolkovo Institute of Science and Technology

Merkle tree



Skoltech
Skolkovo Institute of Science and Technology

Content verification

$$TopHash \neq hash(Hash_0 + hash(hash(L_3) + Hash_{11}))$$

Verification complexity: the depth of the tree – $\mathcal{O}(\log N)$.

Skoltech
Skolkovo Institute of Science and Technology

Outline

Skoltech
Skolkovo Institute of Science and Technology

Euler's phi function $\varphi(n)$

Definition

$\varphi(n)$ is a number of integers k in the range $1 \leq k \leq n$ co-prime with n, i.e. $(n, k) = 1$.

Skoltech
Skolkovo Institute of Science and Technology

Euler's phi function $\varphi(n)$

- $\varphi(p) = p - 1$

Skoltech
Skolkovo Institute of Science and Technology

Euler's phi function $\varphi(n)$

- $\varphi(p) = p - 1$
- $\varphi(p^k) = p^k - p^{k-1}$

Skoltech
Skolkovo Institute of Science and Technology

Euler's phi function $\varphi(n)$

- $\varphi(p) = p - 1$
- $\varphi(p^k) = p^k - p^{k-1}$
- $n = \prod_i p^{k_i}$, $\varphi(n) = \prod_i \varphi p^{k_i}$

Skoltech
Skolkovo Institute of Science and Technology

Euler's theorem

Theorem

Let $(a, n) = 1$, *then*

$$a^{\varphi(n)} = 1 \ \ mod \ \ n$$

Skoltech
Skolkovo Institute of Science and Technology

Euclidean algorithm

How to calculate (a, b)?

Skoltech
Skolkovo Institute of Science and Technology

Euclidean algorithm

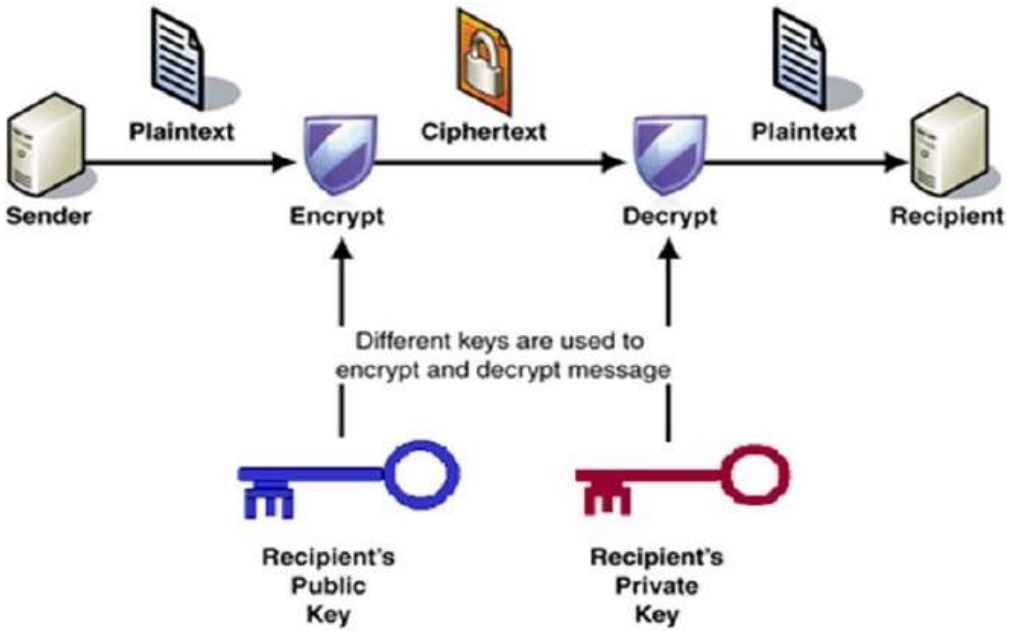
Let $a \geq b$. Note, that $(a, b) = (a \mod b, b)$

$$
\begin{aligned}
a &= bq_0 + r_1, \\
b &= r_1 q_1 + r_2, \\
r_1 &= r_2 q_2 + r_3, \\
&\dots \\
r_{k-2} &= r_{k-1} q_{k-1} + r_k, \\
&\dots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, \\
r_{n-1} &= r_n q_n
\end{aligned}
$$

Skoltech
Skolkovo Institute of Science and Technology

$$(a, b) = d = as + bt.$$

Public key cryptosystem



Skoltech
Skolkovo Institute of Science and Technology

Public key cryptosystem

Brief history

- concept conceived by Diffe and Hellman in 1976
- Rivest, Shamir and Adleman (RSA) were first to describe a public key system in 1978
- Merkle and Hellman published a different solution, later in 1978
- many proposals have been broken (including the 1978 Merkle-Hellman proposal broken by Shamir)

Current systems

- RSA
- Diffie-Hellman
- El Gamal

Skoltech
Skolkovo Institute of Science and Technology

Diffie–Hellman key exchange

- Alice and Bob choose prime number p and base g (primitive modulo p)
- Alice chooses a number a and send the following integer to Bob

$$A = g^a mod \ \ p$$

- Bob chooses b and sends

$$B = g^b mod \ \ p$$

- Secret key:

$$K = B^a mod \ \ p = A^b mod \ \ p = g^{ab} mod \ \ p.$$

Skoltech
Skolkovo Institute of Science and Technology

Inventers: Rivest–Shamir–Adleman

Martin Gardner. Mathematical Games: A new kind of cipher that would take millions of years to break // Scientific American. – 1977.

Key generation

- Choose prime numbers p and q
- Calculate

$$n = pq$$

- Calculate Euler's function

$$\varphi(n) = (p-1)(q-1)$$

- Public exponent

$$1 < e < \varphi(n); \;\; (e, \varphi(n)) = 1$$

- Private exponent

$$d = e^{-1} \;\; mod \;\; \varphi(n)$$

Skoltech
Skolkovo Institute of Science and Technology

Key generation

- Public key: (n, e)
- Private key: (n, d)

Skoltech
Skolkovo Institute of Science and Technology

Encryption-Decryption

Message m, $0 \leq m \leq n-1$

Encryption

$$c = E_{(n,e)}(m) = m^e \mod n$$

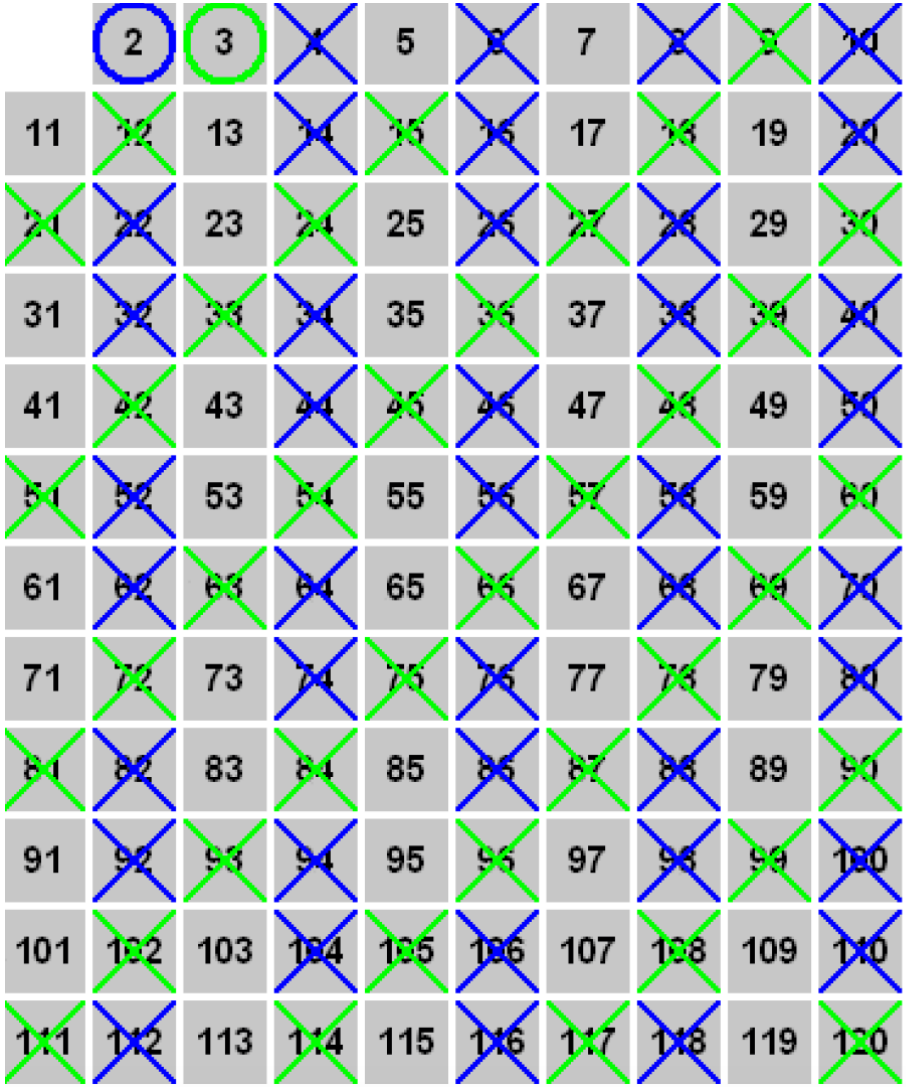
Decryption

$$m' = D_{(n,d)}(c) = c^d \mod n$$

Skoltech
Skolkovo Institute of Science and Technology

How to check if the number is prime?

Sieve of Eratosthenes



Prime numbers

2 3

Skoltech
Skolkovo Institute of Science and Technology

Outline

Skoltech
Skolkovo Institute of Science and Technology

El-Gamal cryptosystem

- Based on the Diffie–Hellman key exchange
- The system provides an additional layer of security by asymmetrically encrypting keys previously used for symmetric message encryption
- It was described by Taher Elgamal in 1985
- It is based on difficulty of computing discrete logarithm in finite field
- It is used in the free GNU Privacy Guard software
- In comparison with RSA was not patented so become more popular

Skoltech
Skolkovo Institute of Science and Technology

Key generation mechanism

1. Choose big prime number p
2. Choose two random numbers g and x
3. Compute $y = g^x \mod p$

Public key (y, g, p)

Secret key (x, g, p)

Skoltech
Skolkovo Institute of Science and Technology

Encryption mechanism

1. Let message $M < p$
2. Choose random number k s.t. $1 < k < p - 1$
3. Compute $a = g^k \mod p$ and $b = y^k M \mod p$

Ciphertext (a, b)

Skoltech
Skolkovo Institute of Science and Technology

Decryption mechanism

$$M = \frac{b}{a^x} \mod p$$

Skoltech
Skolkovo Institute of Science and Technology

Proof of correctness

$$a^x = g^{kx} \mod p$$

$$\frac{b}{a^x} = \frac{y^k M}{a^x} = \frac{g^{kx} M}{g^{kx}} = M \mod p = M$$

Skoltech
Skolkovo Institute of Science and Technology

Decryption without knowledge of private key

- We know g, p, y, $a = g^k \mod p$, $b = y^k M \mod p$
- We want to find $M = by^{-k} \mod p$ where $k = \log_g a \mod p$
- Only sub-exponential algorithms of finding k
- We need $2.7 * 10^{28}$ MIPS to decrypt El-Gamal cipher text with key length 1300 bit

Skoltech
Skolkovo Institute of Science and Technology

Problem

There are sub-exponential algorithm to decrypt El-Gamal and RSA

Skoltech
Skolkovo Institute of Science and Technology

Solution

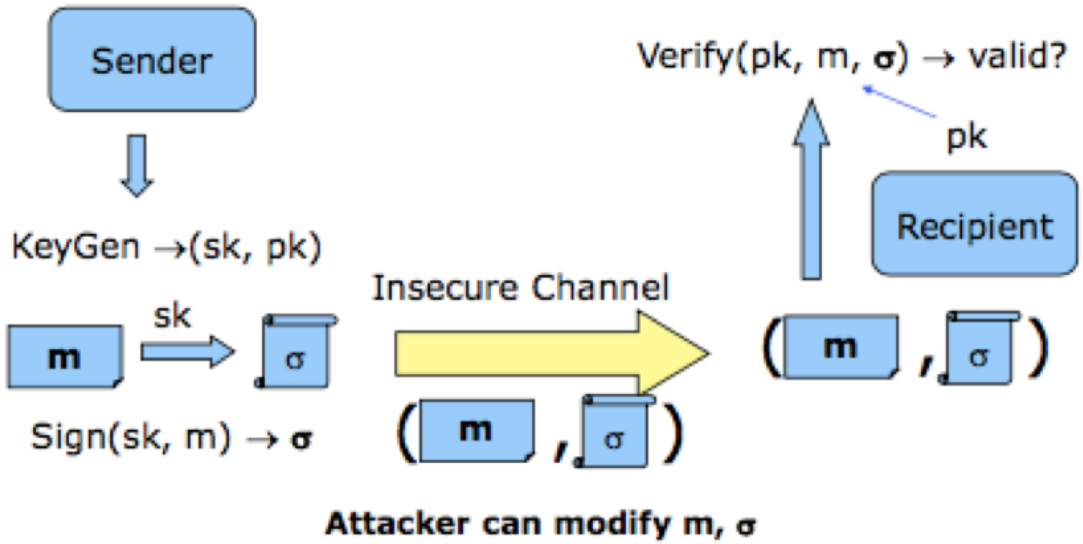
Cryptography on elliptic curves over finite fields.

Skoltech
Skolkovo Institute of Science and Technology

Outline

Skoltech
Skolkovo Institute of Science and Technology

Digital signatures



Skoltech
Skolkovo Institute of Science and Technology

Pubic key digital signature

- Alice's keys are d_{alice} and e_{alice}
- Alice sends to Bob $m||\{m\}d_{alice}$
- In case of dispute, judge computes $\{\{m\}d_{alice}\}e_{alice}$ and if it's m then it means that Alice signed this message

Alice is the only one who knows d_{alice}

Skoltech
Skolkovo Institute of Science and Technology

RSA digital signature

1. $n = pq$, where p and q are prime numbers
2. $\phi(n) = (p-1)(q-1)$
3. Choose $1 < e < \phi(n)$ s.t. $(e, \phi(n)) = 1$
4. $d = e^{-1} \mod \phi(n)$

Open key (n, e)

Secret key (n, d)

Skoltech
Skolkovo Institute of Science and Technology

$Sign(privatekey, m)$: $\sigma = m^d \mod n$

$Verify(publickey, m, \sigma)$: $\sigma^e \mod n == m$

Skoltech
Skolkovo Institute of Science and Technology

El-Gamal digital signature

$y = g^x \mod p$

Open key: y, g, p

Private key: x, g, p

Skoltech
Skolkovo Institute of Science and Technology

$Sign(privatekey, m)$

- Choose arbitrary k s.t. $(k, p-1) = 1$
- $a = g^k \mod p$
- $b = (m - xa)k^{-1} \mod (p-1)$
- $\sigma = (a, b)$

$Verify(publickey, m, \sigma)$: $y^a a^b \mod p = g^m \mod p$

Skoltech
Skolkovo Institute of Science and Technology

Thank you for your attention!

Skoltech
Skolkovo Institute of Science and Technology