ĐẠI HỌC
BÁCH KHOA HÀ NỘI
HANOI UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Digital signature algorithm

Group 18:
- Nguyễn Trung Hiếu - 20204877
- Nguyễn Lân Cường - 20204872
- Nguyễn Văn Thanh Tùng - 20190090

Hanoi, February 2023

ONE LOVE. ONE FUTURE.

HUST

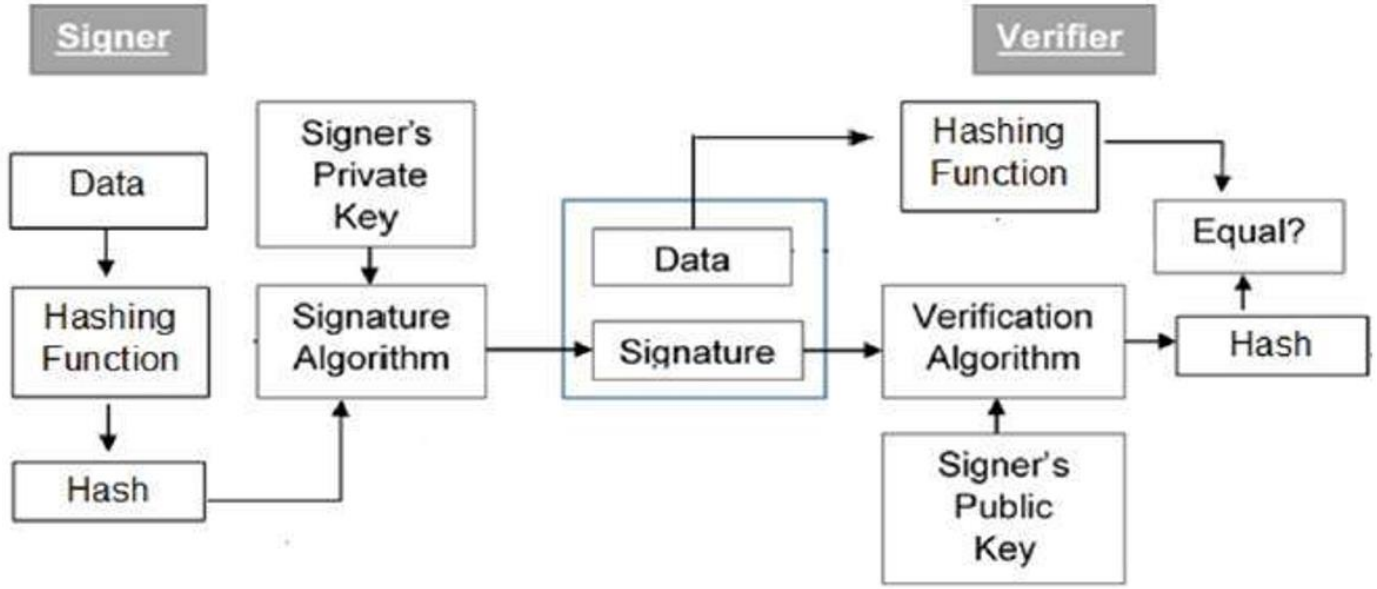
hust.edu.vn fb.com/dhbkhn

Content

1. Introduction
2. Background
3. Algorithm
4. Conclusion
5. References

1. Introduction

- In 1991, The National Institute of Standards and Technology (NIST) has published Federal Information Processing Standard FIPS 186, known as the **Digital Signature Algorithm (DSA)**
- The latest versions of it incorporate RSA and elliptic-curve cryptography.
- It has become standard for digital signature by FED.



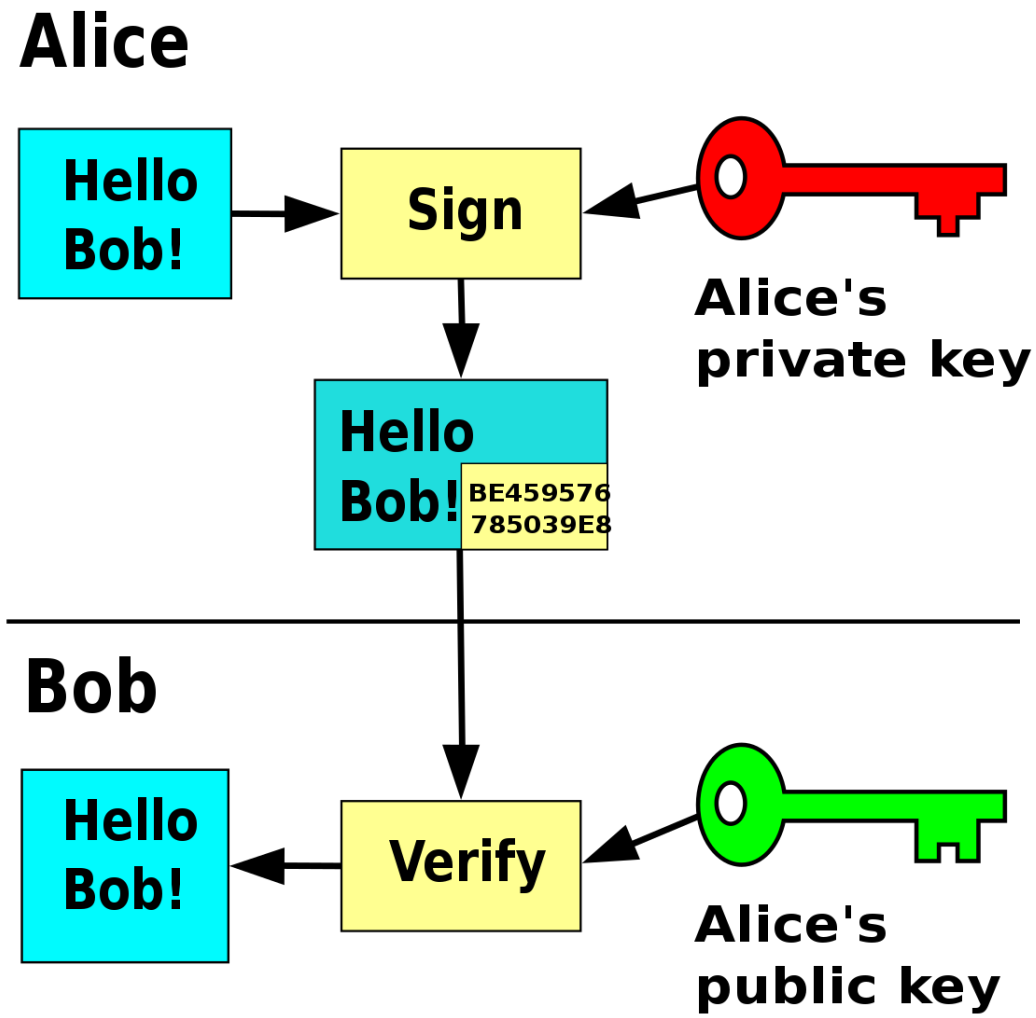
2. Background

Digital signature scheme

- Main idea:
  - A signer S creates a public key p_k and private key s_k.
  - The signer use s_k to sign a message.
  - Anyone knows p_k can verify that the message comes from S and not modified.
- A digital signature scheme consists of 3 probabilistic polynomial-time algorithms:
  - A key-generation algorithm: takes input 1^n where n is a security parameters, output a public key p_k and a private key s_k.
  - A signing algorithm: takes the private key s_k and the message m, output a signature σ.
  - A deterministic verification algorithm: takes the public key p_k, the message m and the signature σ as the inputs. The algorithm will determine if the signature is valid or not.

2. Background

Digital signature scheme



Discrete Logarithm problem

Problem: Given a finite cyclic group Z_p^* of order $p - 1$ and a primitive element $g \in Z_p^*$ and another element $y \in Z_p^*$. The Discrete Logarithm problem of determining integer $1 \leq x \leq p - 1$ such that

$$g^x = y \bmod p$$

- With g, x, p known, it's straightforward to compute y.
- With g, y, p known, it's difficult to compute x, provides that $p - 1$ is not multiply of small prime numbers.

→ This forms a one-way function.

2. Background

Miller – Rabin test:

Miller- Rabin algorithm to check primality:

Property 1: If p is a prime number then $a^2 = 1\ mod\ p$ if and only if $a = 1\ mod\ p$ or $a = -1\ mod\ p$

Property 2:

Let p be a prime number greater than 2. We can then write $p - 1 = 2^k q$ with $k > 0$, q odd. Let a be any integer in the range $1 < a < p - 1$. Then one of the two following conditions is true:

1. a^q is congruent to 1 modulo p. That is, a^q mod p = 1, or equivalently, $a^q \equiv 1 (\text{mod } p)$.
2. One of the numbers $a^q, a^{2q}, a^{4q}, ..., a^{2^{k-1}q}$ is congruent to -1 modulo p. That is, there is some number j in the range $(1 \leq j \leq k)$ such that $a^{2^{j-1}q}$ mod p = -1 mod p = p - 1 or equivalently, $a^{2^{j-1}q} \equiv -1 (\text{mod } p)$.

2. Background

Miller – Rabin test:

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n - 1 = 2^k q);
2. Select a random integer a, 1 < a < n - 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k - 1 do
5. if a^(2^j q) mod n = n - 1 then return("inconclusive");
6. return("composite");
```

3. Algorithm

Key generation algorithm:

Global parameters generation:

- p: a L bits prime numbers. $L = 1024$ in this project .
- q: a N bits prime divisor of $p - 1$. $N = 160$ in this project.
- $g = h^{\frac{p-1}{q}} \bmod p$, where h is selected randomly from $\{2, 3, \dots, p-2\}$

➢ The global parameters are (p, q, g)

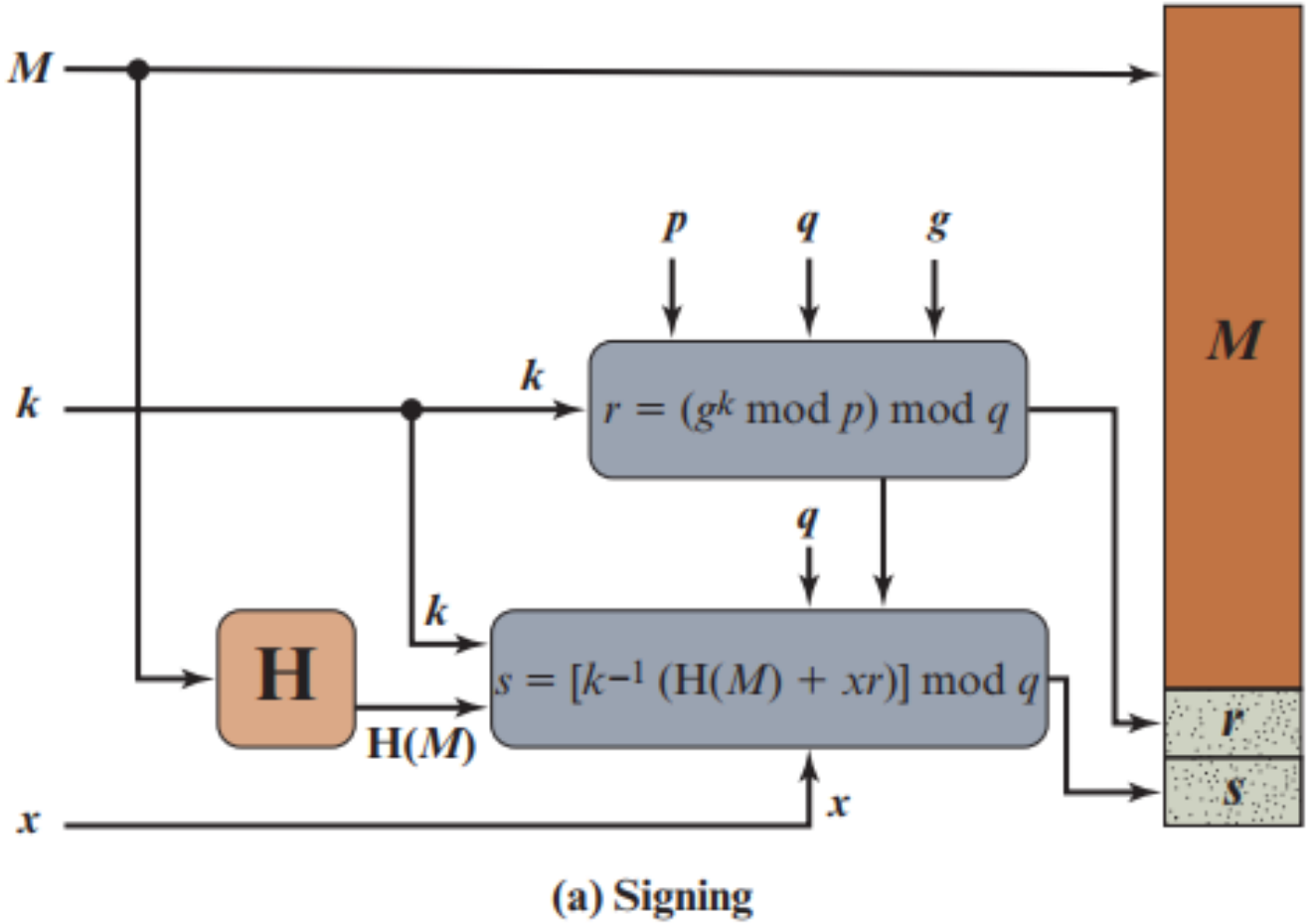
Key generation algorithm:

- Private key x: select randomly from $\{1, 2, \dots, q-1\}$
- Public key $y = g^x \bmod p$

Note: $g = h^{\frac{p-1}{q}} \bmod p \Rightarrow g^q \equiv h^{p-1} \equiv 1 \bmod p$ by Fermat's little theorem → g has order q.

3. Algorithm

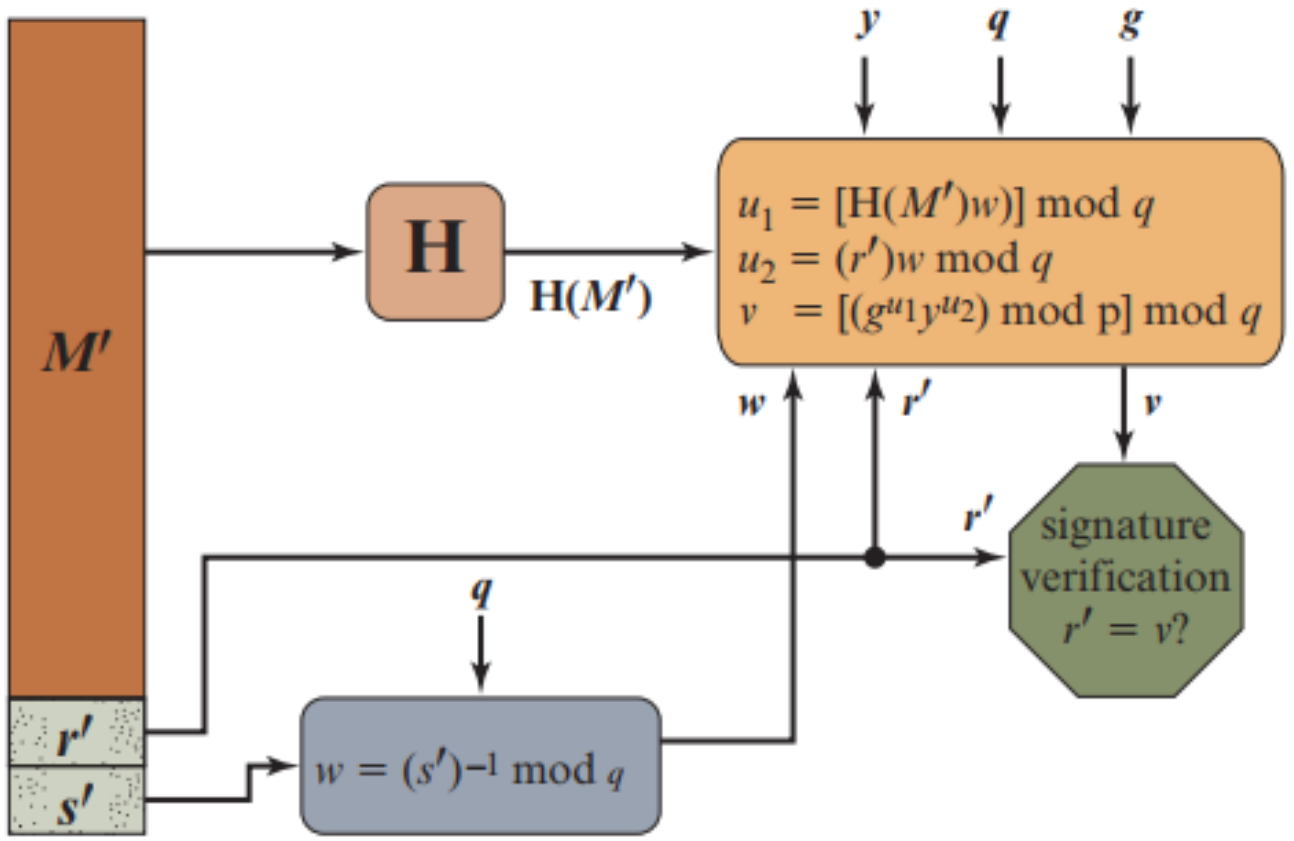
Signing algorithm



(a) Signing

3. Algorithm

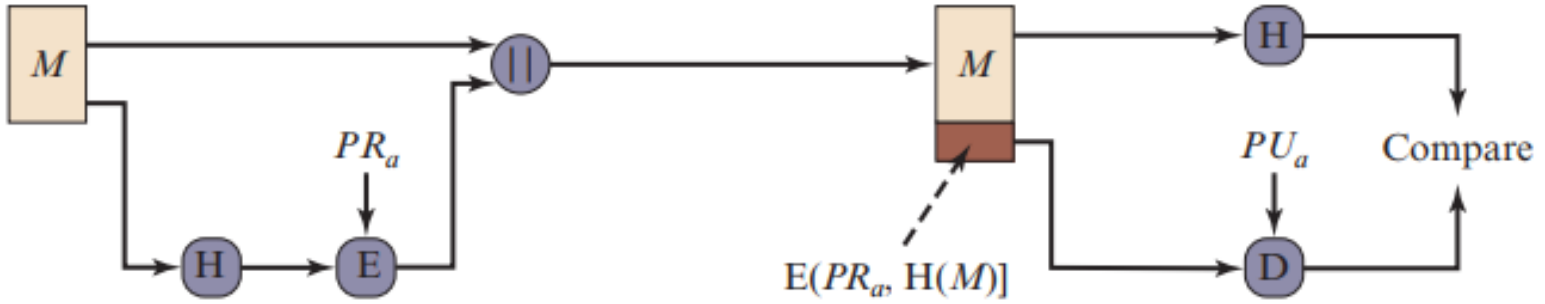
Verification algorithm



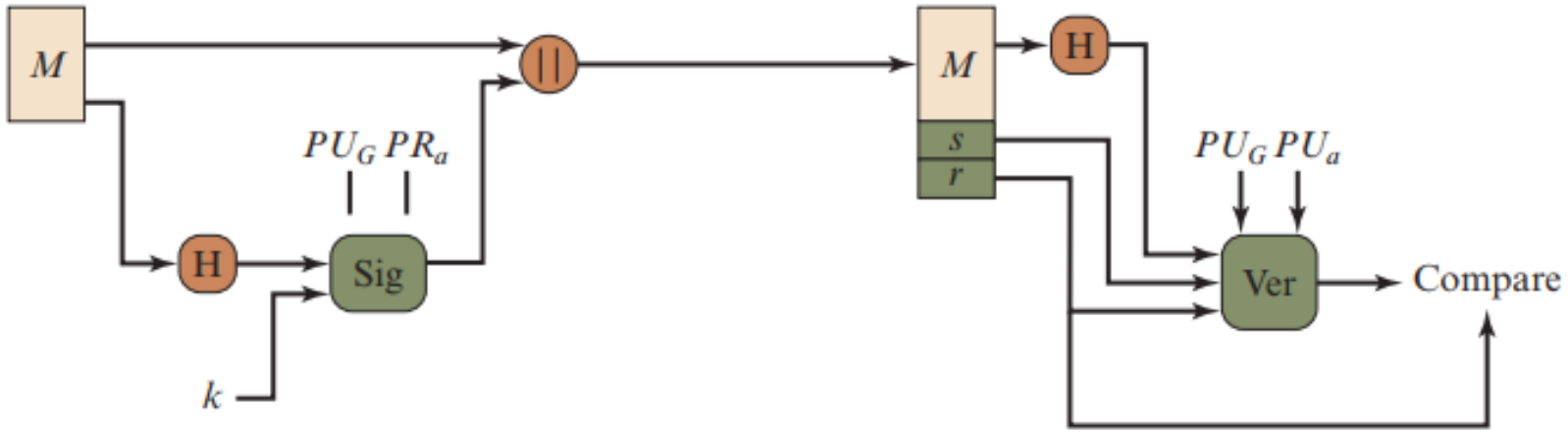
(b) Verifying

3. Algorithm

Comparison with RSA



(a) RSA approach



(b) DSA approach

4. Conclusion

- Extended from ElGamal and Schnorr signature schemes, The (NIST) Digital Signature Algorithm has become standardized method used in digital signature.
- We can attack it by solving the discrete logarithm problem.
- This framework can be easily extended by replacing the private prime numbers by points in elliptic curve to obtain ECDSA, another powerful method to ensure digital signature schemes.

5. References

1. William Stallings - Cryptography and Network Security_ Principles and Practice, Global Edition-Pearson (2022)

2. Digital Signature Standard – NIST 186-4 (2015)

HUST

hust.edu.vn fb.com/dhbkhn

THANK YOU !