Co-funded by the Erasmus+ Programme of the European Union

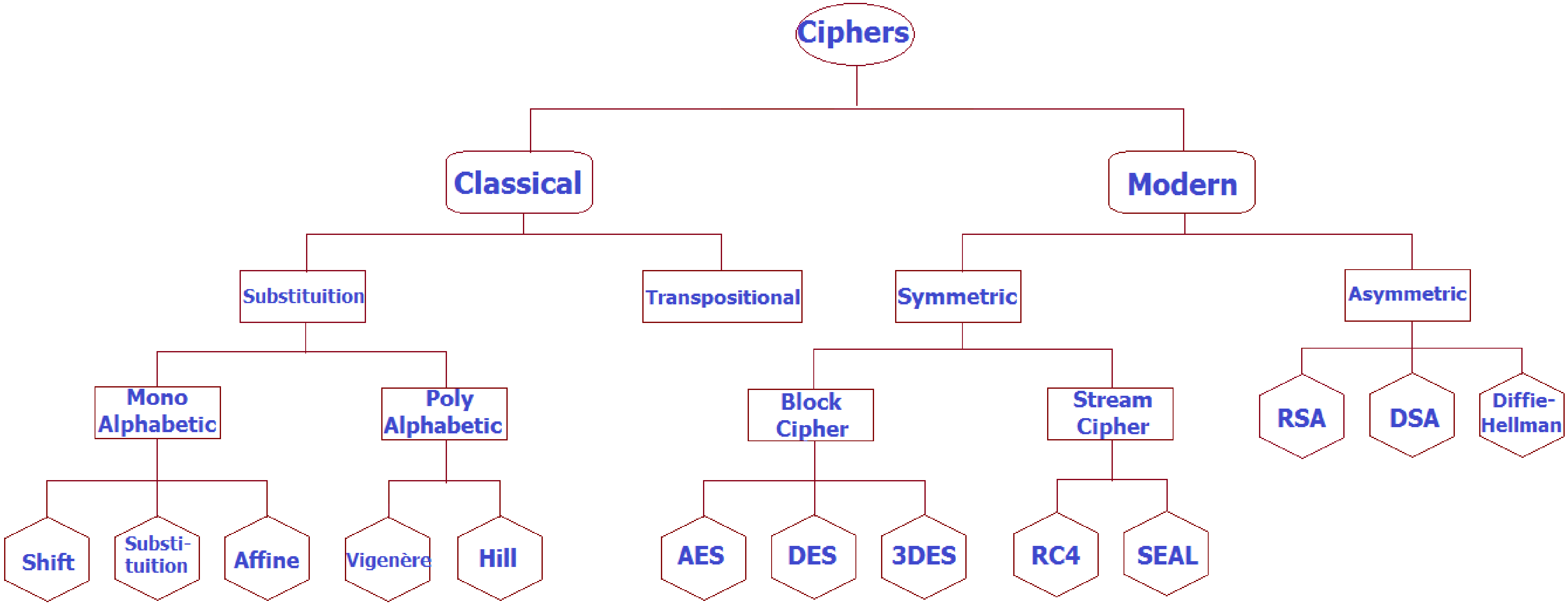
Public-key Cryptography

Truong Tuan Anh
CSE-HCMUT

Outline

- Public-key cryptosystem
- Some fundamental theories
- RSA
- …

Classification



Cryptography: Classical Model

- Secret, common key K
- e_k and d_k for each key K:
  - d_k is either the same as e_k or easily derived from e_k
  - Disclose d_k or e_k will make the system insecure

→ Symmetric-key Cryptosystem

- Require prior communication of the key K (using a secure channel)

→ Difficult to achieve in practice

- Public-key cryptosystem

Public-key Cryptosystem

- Was put forward by Diffie and Hellman in 1976
- The most important cryptosystems: RSA and ElGamal
- Computationally infeasible to determine d_k given e_k
  - e_k is public key
  - Alice sends to Bob an encrypted message using e_k of Bob
  - Bob is the only one who can decrypt the message using his d_k (private key)

→ Never provide unconditional security (why?)

Public-key Cryptosystem (cont.)

- Encryption function is easy to compute
- The inverse function (i.e., the decryption function) should be hard to compute (except for Bob)

→ *one-way function*

- Example: suppose *n* is the product of two large primes *p* and *q*; *b* is a positive integer

$$f : \mathbb{Z}_n \to \mathbb{Z}_n$$

$$\boxed{f(x) = x^b \bmod n.}$$

Trapdoor One-way Functions

- From Bob's view, he does not want e_k to be one-way

→ provide Bob a *trapdoor*: which consists of secret information for the inversion of e_k

- Trapdoor one-way function: a one-way function but it is easy to invert with the knowledge of a certain trapdoor

$$f : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

$$f(x) = x^b \bmod n.$$

$$\boxed{f^{-1} : f(x) = x^a \bmod n}$$

Trapdoor One-way Functions (cont.)

- Usually, we need to specify a **<u>family of trapdoor one-way functions</u>** F
- A function f is chosen from F randomly and used as the *public encryption function*
- Its inverse function is the *private decryption function*

→ Similar to the random key in the symmetric-key cryptosystems

Some Fundamental Theories

9

Recall: Multiplicative Inverse

Suppose $a \in \mathbb{Z}_m$. The *multiplicative inverse* of a modulo m, denoted $a^{-1} \bmod m$, is an element $a' \in \mathbb{Z}_m$ such that

$$aa' \equiv a'a \equiv 1 \pmod{m}.$$

If m is fixed, we sometimes write a^{-1} for $a^{-1} \bmod m$.

- Examples: in Z_{26}

$$3^{-1} = ?$$

$$17^{-1} = ?$$

Relatively Prime

$b \in \mathbb{Z}_n$ has a multiplicative inverse if and only if $\boxed{\gcd(b, n) = 1}$

the number of positive integers less than n and $\boxed{\text{relatively prime}}$ to n is $\phi(n)$

- *x* and *y* are relatively prime iff *gcd(x,y)* =1

The set of residues modulo n that are relatively prime to n is denoted $\mathbb{Z}_n{}^*$

Any element in $\mathbb{Z}_n{}^*$ have a multiplicative inverse (which is also in $\mathbb{Z}_n{}^*$)

Compute gcd(a,b)

EUCLIDEAN ALGORITHM(a, b)

$r_0 \leftarrow a$
$r_1 \leftarrow b$
$m \leftarrow 1$
while $r_m \neq 0$

$$\textbf{do} \begin{cases} q_m \leftarrow \left\lfloor \frac{r_{m-1}}{r_m} \right\rfloor \\ r_{m+1} \leftarrow r_{m-1} - q_m r_m \\ m \leftarrow m + 1 \end{cases}$$

$m \leftarrow m - 1$
return $(q_1, \ldots, q_m; r_m)$
comment: $r_m = \gcd(a, b)$

Compute b^{-1} modulo a

MULTIPLICATIVE INVERSE(a, b)

$a_0 \leftarrow a$
$b_0 \leftarrow b$
$t_0 \leftarrow 0$
$t \leftarrow 1$
$q \leftarrow \left\lfloor \frac{a_0}{b_0} \right\rfloor$
$r \leftarrow a_0 - qb_0$

while $r > 0$

do $\begin{cases} temp \leftarrow (t_0 - qt) \bmod a \\ t_0 \leftarrow t \\ t \leftarrow temp \\ a_0 \leftarrow b_0 \\ b_0 \leftarrow r \\ q \leftarrow \left\lfloor \frac{a_0}{b_0} \right\rfloor \\ r \leftarrow a_0 - qb_0 \end{cases}$

if $b_0 \neq 1$
  then b has no inverse modulo a
  else return (t)

Chinese Remainder Theorem

Suppose $m_1, \ldots, m_r$ *are pairwise relatively prime positive integers, and suppose* $a_1, \ldots, a_r$ *are integers.*

Then the system of r *congruences* $x \equiv a_i \pmod{m_i}$ $(1 \leq i \leq r)$ *has a* *unique solution modulo* $M = m_1 \times \cdots \times m_r$:

$$\boxed{x = \sum_{i=1}^{r} a_i M_i y_i \bmod M,}$$

where $M_i = M/m_i$ *and* $y_i = M_i^{-1} \bmod m_i$, *for* $1 \leq i \leq r$.

Example

- Suppose $r = 3$, in $m_1 = 7$, $m_2 = 11$, $m_3 = 13$

$\rightarrow M = 1001$ and $M_1 = 143$, $M_2 = 91$, $M_3 = 77$

- $y_1 = ?$, $y_2 = ?$, $y_3 = ?$
- $y_1 = 5$, $y_2 = 4$, $y_3 = 12$

The Function: $\chi^{-1} : \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \mathbb{Z}_{13} \rightarrow \mathbb{Z}_{1001}$

is

$$\boxed{\chi^{-1}(a_1, a_2, a_3) = (715a_1 + 364a_2 + 924a_3) \bmod 1001}$$

Example (cont.)

if $x \equiv 5 \pmod{7}$, $x \equiv 3 \pmod{11}$ and $x \equiv 10 \pmod{13}$

Then we recompute x by:

$$\begin{aligned} x &= (715 \times 5 + 364 \times 3 + 924 \times 10) \bmod 1001 \\ &= 13907 \bmod 1001 \\ &= 894. \end{aligned}$$