Discrete Mathematics for Computer Science

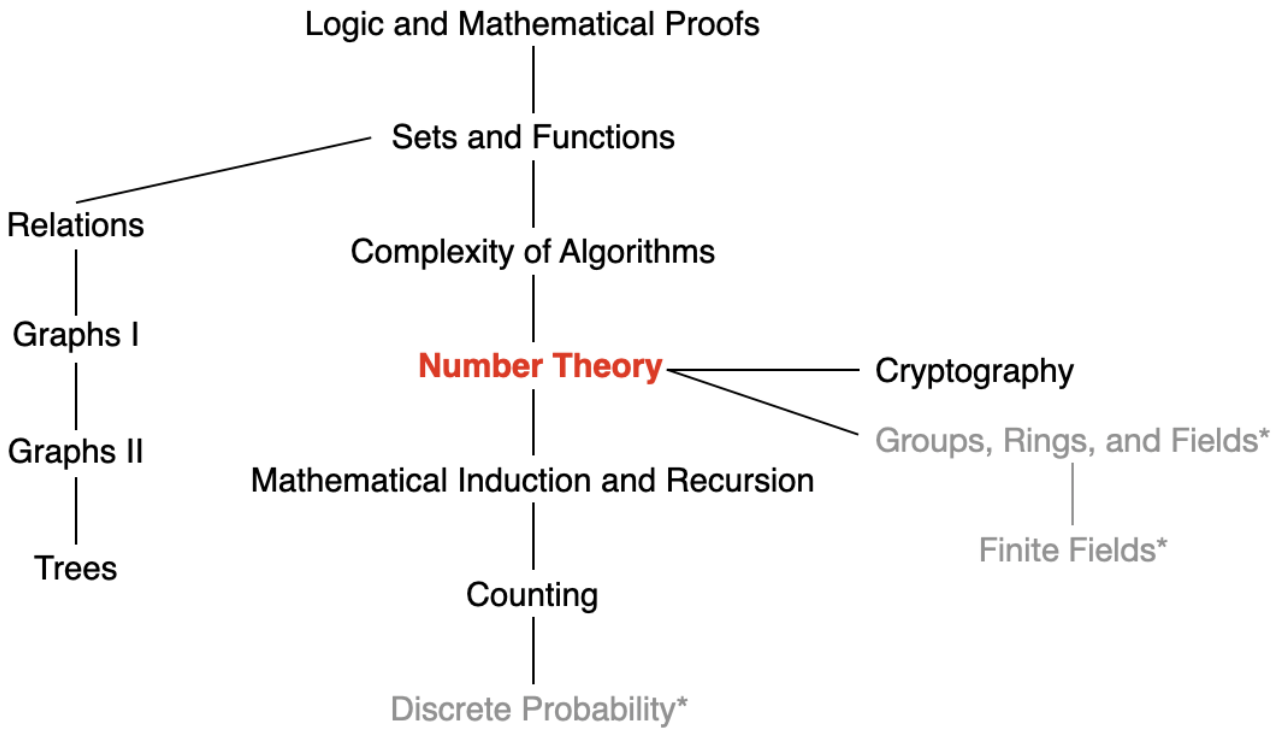
Lecture 9: Cryptography

Dr. Ming Tang

Department of Computer Science and Engineering
Southern University of Science and Technology (SUSTech)
Email: tangm3@sustech.edu.cn

SUSTech Southern University of Science and Technology

This Lecture



Number Theory: divisibility and modular arithmetic, integer representations, primes, greatest common divisors, linear congruences

SUSTech Southern University of Science and Technology

Linear Congruences

A congruence of the form $ax \equiv b \pmod{m}$, where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.

The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.

- An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an inverse of a modulo m.
  - When does an inverse of a modulo m exist? a and m are relatively prime integers and $m > 1$.
    - ★ Existence: $gcd(a, m) = 1 = as + mt$ for some integers s and t; s in an inverse of a;
    - ★ Unique: The inverse is unique modulo m; $\bar{a} \equiv s \pmod{m}$.
  - How to find inverses? Using extended Euclidean algorithm
- $x \equiv \bar{a}b \pmod{m}$

SUSTech Southern University of Science and Technology

Using Inverses to Solve Congruences

Example: What are the solutions of the congruence $3x \equiv 4 \pmod{7}$?

Solution:

- We found that -2 is an inverse of 3 modulo 7.
- $x \equiv -2 \times 4 \pmod{7} \equiv 6 \pmod{7}$

SUSTech Southern University of Science and Technology

Number of Solutions to Congruences

The previous approach (based on the inverse of a modulo m) works for only the scenario with $\gcd(a, m) = 1$.

Theorem*: Let $\gcd(a, m) = d$. Let $m' = m/d$ and $a' = a/d$. The congruence $ax \equiv b$ (**mod** m) has solutions if and only if $d \mid b$.

- If $d \mid b$, then there are exactly d solutions, where by "solution" we mean a congruence class mod m
- If x_0 is a solution, then the other solutions are given by $x_0 + m', x_0 + 2m', ..., x_0 + (d-1)m'$.

Proof:

"only if": Let x_0 be a solution, then $ax_0 - b = km$. Thus, $ax_0 - km = b$. Since $d \mid ax_0 - km$, we must have $d \mid b$.

"if": Suppose that $d \mid b$. Let $b = kd$. Since $\gcd(a, m) = d$, there exist integers s and t such that $d = as + mt$. Multiplying both sides by k. Then, $b = ask + mtk$. Let $x_0 = sk$. Then $ax_0 \equiv b$ (**mod** m).

Number of Solutions to Congruences

Theorem*: Let $\gcd(a, m) = d$. Let $m' = m/d$ and $a' = a/d$. The congruence $ax \equiv b \pmod{m}$ has solutions if and only if $d \mid b$.

- If $d \mid b$, then there are exactly d "solutions", where by "solution" we mean a congruence class mod m.
- If x_0 is a solution, then the other solutions are given by $x_0 + m', x_0 + 2m', ..., x_0 + (d-1)m'$.

Proof:

"The number of solutions is d": Consider two solutions x_0 and x_1. $ax_0 \equiv b \pmod{m}$ and $ax_1 \equiv b \pmod{m}$ imply that $m \mid a(x_1 - x_0)$ and $m' \mid a'(x_1 - x_0)$. This implies further that $x_1 = x_0 + km'$.

To finish the proof, observe that as k runs through the values $0, 1, ..., d-1$ (the residues mod d), the congruence classes $[x_0 + (m/d)k]_m$ run through all the solutions.

SUSTech Southern University of Science and Technology

The Chinese Remainder Theorem

Systems of linear congruences have been studied since ancient times.

今有物不知其数 三三数之剩二 五五数之剩三 七七数之剩二 问物几何

About 1500 years ago, the Chinese mathematician Sun-Tsu asked: "There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?"

- $x \equiv 2 \pmod{3}$
- $x \equiv 3 \pmod{5}$
- $x \equiv 2 \pmod{7}$

SUSTech Southern University of Science and Technology

The Chinese Remainder Theorem

Theorem (The Chinese Remainder Theorem): Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than 1 and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then, the system

$$x \equiv a_1 \ (\mathbf{mod}\ m_1)$$
$$x \equiv a_2 \ (\mathbf{mod}\ m_2)$$
$$\ldots$$
$$x \equiv a_n \ (\mathbf{mod}\ m_n)$$

has a unique solution modulo $m = m_1 m_2 \ldots m_n$.
(That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

SUSTech Southern University of Science and Technology

The Chinese Remainder Theorem

Proof: To show such a solution exists: Let $M_k = m/m_k$ for $k = 1, 2, ..., n$ and $m = m_1 m_2 ... m_n$. Thus, $M_k = m_1 ... m_{k-1} m_{k+1} ... m_n$.

Since $\gcd(m_k, M_k) = 1$, there is an integer y_k, an inverse of M_k modulo m_k, such that $M_k y_k \equiv 1 \ (\textbf{mod}\ m_k)$. Let

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_n M_n y_n.$$

It is checked that x is a solution to the n congruences:

$$x \ \textbf{mod}\ m_k = (a_1 M_1 y_1 + a_2 M_2 y_2 + ... + a_n M_n y_n) \ \textbf{mod}\ m_k$$

Since $M_k = m/m_k$, we have $x \ \textbf{mod}\ m_k = a_k M_k y_k \ \textbf{mod}\ m_k$. Since $M_k y_k \equiv 1 \ (\textbf{mod}\ m_k)$, we have $a_k M_k y_k \ \textbf{mod}\ m_k = a_k \ \textbf{mod}\ m_k$. Thus,

$$x \equiv a_k \ (\textbf{mod}\ m_k).$$

SUSTech Southern University of Science and Technology

The Chinese Remainder Theorem

How to prove the uniqueness of the solution modulo m?

Proof: Suppose that x and x' are both solutions to all the congruences. As x and x' give the same remainder, when divided by m_k, their difference $x - x'$ is a multiple of each m_k for all $k = 1, 2, ..., n$.

As m_1, m_2, . . . , m_n be pairwise relatively prime positive integers, their product m divides $x - x'$, and thus x and x' are congruent modulo m, i.e., $x \equiv x' \pmod{m}$.

This implies that given a solution x with $0 \leq x < m$, all other solutions are congruent modulo m to this solution.

SUSTech Southern University of Science and Technology

The Chinese Remainder Theorem: Example

$$x \equiv 2 \ (\textbf{mod}\ 3)$$
$$x \equiv 3 \ (\textbf{mod}\ 5)$$
$$x \equiv 2 \ (\textbf{mod}\ 7)$$

1. Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, and $M_3 = m/7 = 15$.
2. Compute the inverse of M_k modulo m_k:
   - $35 \cdot 2 \equiv 1 \ (\textbf{mod}\ 3)$ $y_1 = 2$
   - $21 \equiv 1 \ (\textbf{mod}\ 5)$ $y_2 = 1$
   - $15 \equiv 1 \ (\textbf{mod}\ 7)$ $y_3 = 1$
3. Compute a solution x:
   $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 233 \equiv 23 \ (\textbf{mod}\ 105)$
4. The solutions are all integers x that satisfy $x \equiv 23 \ (\textbf{mod}\ 105)$.

SUSTech Southern University of Science and Technology

Back Substitution

We may also solve systems of linear congruences with pairwise relatively prime moduli $m_1, m_2, \ldots m_n$ by back substitution.

Example:

(1) $x \equiv 1$ (**mod** 5)
(2) $x \equiv 2$ (**mod** 6)
(3) $x \equiv 3$ (**mod** 7)

According to (1), $x = 5t + 1$, where t is an integer.

Substituting this expression into (2), we have $5t + 1 \equiv 2$ (**mod** 6), which means that $t \equiv 5$ (**mod** 6). Thus, $t = 6u + 5$, where u is an integer.

Substituting $x = 5t + 1$ and $t = 6u + 5$ into (3), we have $30u + 26 \equiv 3$ (**mod** 7), which implies that $u \equiv 6$ (**mod** 7). Thus, $u = 7v + 6$, where v is an integer.

Thus, we must have $x = 210v + 206$. Translating this back into a congruence,

$$x \equiv 206 \text{ (mod } 210).$$

SUSTech Southern University of Science and Technology

The Chinese Remainder Theorem

Find all solutions, if any, to the system of congruences $x \equiv 5$ (**mod** 6), $x \equiv 3$ (**mod** 10), $x \equiv 8$ (**mod** 15).

SUSTech Southern University of Science and Technology

The Chinese Remainder Theorem

What if $m_1, m_2, \ldots, m_n$ are positive integers greater than 1, but they are not pairwise relatively prime?

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\ldots$$
$$x \equiv a_n \pmod{m_n}$$

Translate these congruence into a set of congruence that together are equivalent to the given congruence:

For $x \equiv a_k \pmod{m_k}$, suppose m_k can be written as $m_k = b_k^1 b_k^2 \cdot b_k^r$, where b_k^1, b_k^2, ..., b_k^r are all primes. Then, $x \equiv a_k \pmod{m_k}$ is equivalent to the following set of congruence:

$$x \equiv a_k \pmod{b_k^1}$$
$$x \equiv a_k \pmod{b_k^2}$$
$$\ldots$$
$$x \equiv a_k \pmod{b_k^r}$$

SUSTech Southern University of Science and Technology

The Chinese Remainder Theorem

Find all solutions, if any, to the system of congruences $x \equiv 5$ (**mod** 6), $x \equiv 3$ (**mod** 10), $x \equiv 8$ (**mod** 15).

- $x \equiv 5$ (**mod** 2); i.e., $x \equiv 1$ (**mod** 2)
- $x \equiv 5$ (**mod** 3); i.e., $x \equiv 2$ (**mod** 3)
- $x \equiv 3$ (**mod** 2); i.e., $x \equiv 1$ (**mod** 2)
- $x \equiv 3$ (**mod** 5)
- $x \equiv 8$ (**mod** 3); i.e., $x \equiv 2$ (**mod** 3)
- $x \equiv 8$ (**mod** 5); i.e., $x \equiv 3$ (**mod** 5)

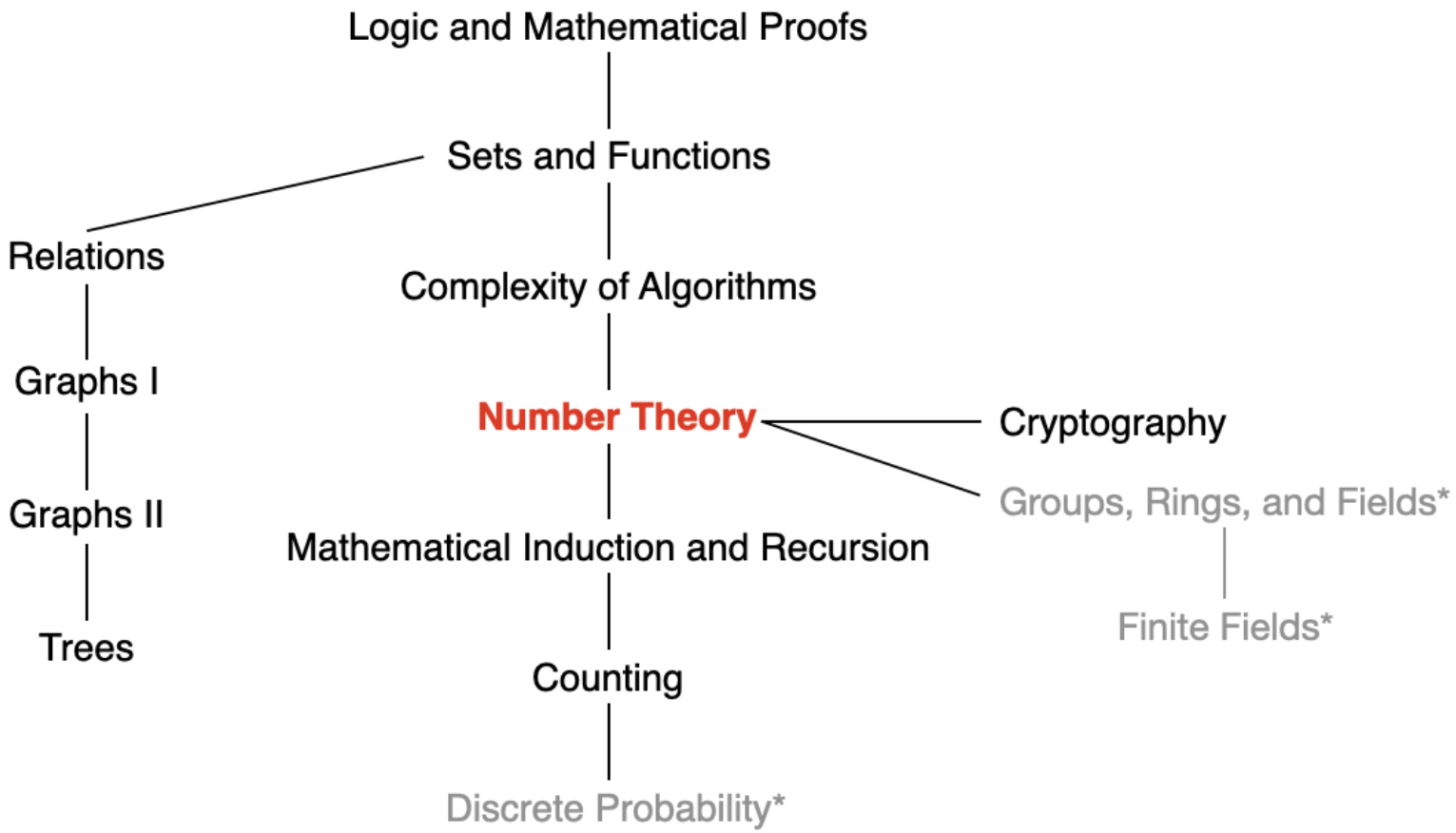
SUSTech Southern University of Science and Technology

Summary: Linear Congruences

- Compute $ax \equiv b \pmod{m}$, with $\gcd(a, m) = 1$
  - Inverse of a modulo m $a\bar{a} \equiv 1 \pmod{m}$: existence? uniqueness?
  - Extended Euclidean Algorithm
  - $x \equiv \bar{a}b \pmod{m}$
- $ax \equiv b \pmod{m}$, with $\gcd(a, m) = d$
- Chinese Remainder Theorem:
  - $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n$.
  - What if not pairwise relatively prime

SUSTech Southern University of Science and Technology

This Lecture



Number Theory: divisibility and modular arithmetic, integer representations, primes, greatest common divisors, linear congruences, application, ...

SUSTech Southern University of Science and Technology

Modular Arithmetic in CS

Modular arithmetic and congruencies are used in CS:

- Pseudorandom number generators
- Hash functions
- Cryptography

SUSTech Southern University of Science and Technology

Pseudorandom Number Generators

Linear congruential method

We choose four numbers:

- the modulus m
- multiplier a
- increment c
- seed x_0

We generate a sequence of numbers $x_1, x_2, \ldots, x_n, \ldots$ with $0 \leq x_i < m$ by using the congruence

$$x_{n+1} = (ax_n + c) \textbf{ mod } m$$

SUSTech Southern University of Science and Technology

Pseudorandom Number Generators

Linear congruential method

$$x_{n+1} = (ax_n + c) \bmod m$$

$m = 9$, $a = 7$, $c = 4$, and $x_0 = 3$:

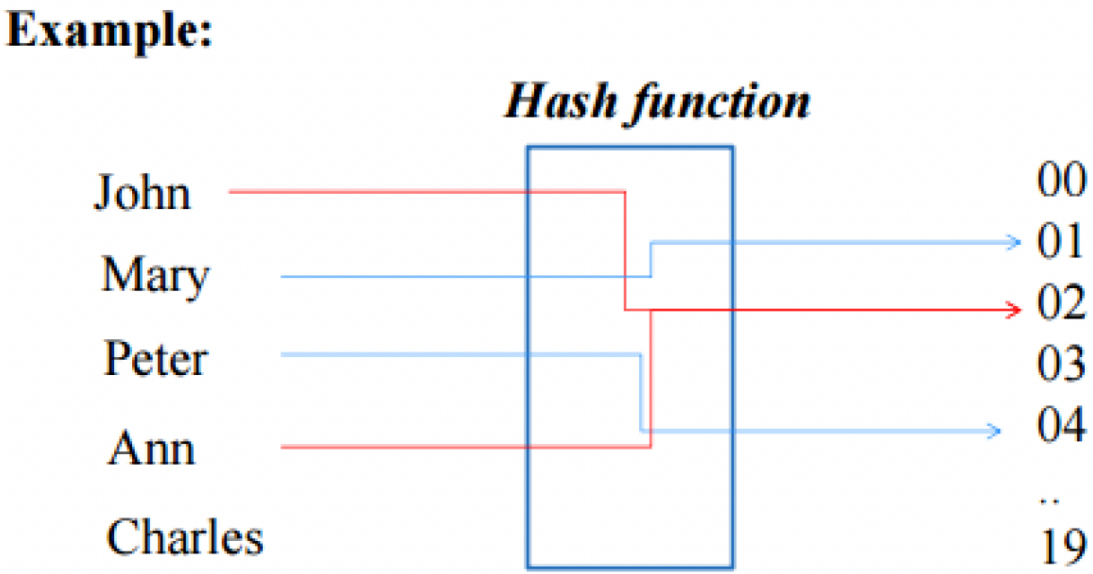
$$\begin{aligned}
x_1 &= 7x_0 + 4 \bmod 9 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 = 7,\\
x_2 &= 7x_1 + 4 \bmod 9 = 7 \cdot 7 + 4 \bmod 9 = 53 \bmod 9 = 8,\\
x_3 &= 7x_2 + 4 \bmod 9 = 7 \cdot 8 + 4 \bmod 9 = 60 \bmod 9 = 6,\\
x_4 &= 7x_3 + 4 \bmod 9 = 7 \cdot 6 + 4 \bmod 9 = 46 \bmod 9 = 1,\\
x_5 &= 7x_4 + 4 \bmod 9 = 7 \cdot 1 + 4 \bmod 9 = 11 \bmod 9 = 2,\\
x_6 &= 7x_5 + 4 \bmod 9 = 7 \cdot 2 + 4 \bmod 9 = 18 \bmod 9 = 0,\\
x_7 &= 7x_6 + 4 \bmod 9 = 7 \cdot 0 + 4 \bmod 9 = \ \ 4 \bmod 9 = 4,\\
x_8 &= 7x_7 + 4 \bmod 9 = 7 \cdot 4 + 4 \bmod 9 = 32 \bmod 9 = 5,\\
x_9 &= 7x_8 + 4 \bmod 9 = 7 \cdot 5 + 4 \bmod 9 = 39 \bmod 9 = 3.
\end{aligned}$$

This sequence contains nine different numbers before repeating.

SUSTech Southern University of Science and Technology

Hash Functions

A hash function is an algorithm that maps data of arbitrary length to data of a fixed length. The values returned by a hash function are called hash values or hash codes.



SUSTech Southern University of Science and Technology

Hash Functions

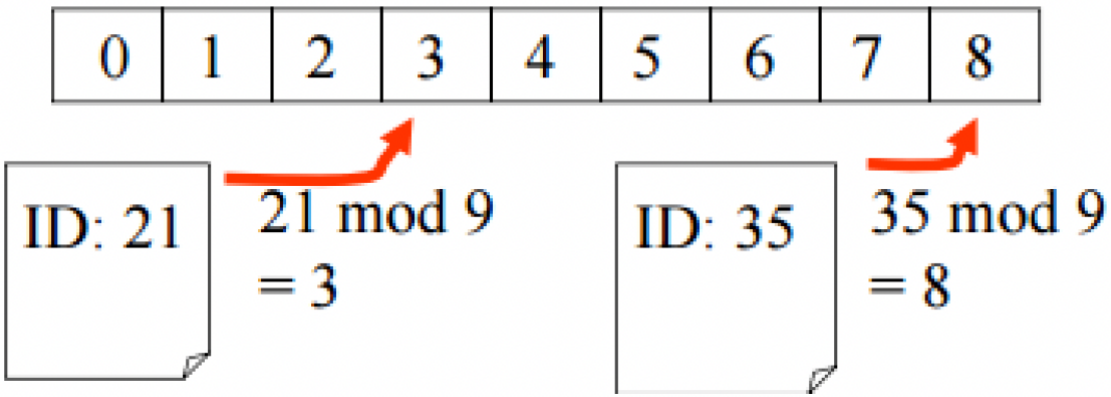
Problem: Given a large collection of records, how can we store and find a record quickly?

Solution: Use a hash function, calculate the location of the record based on the record's ID.

A common function is

$$h(k) = k \textbf{ mod } m,$$

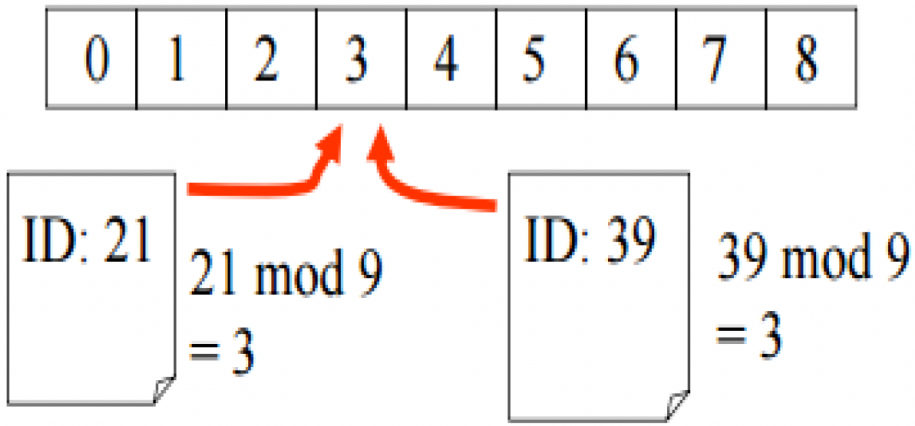
where m is the number of available storage locations.



SUSTech Southern University of Science and Technology

Hash Functions

Two records mapped to the same location



How to address this?

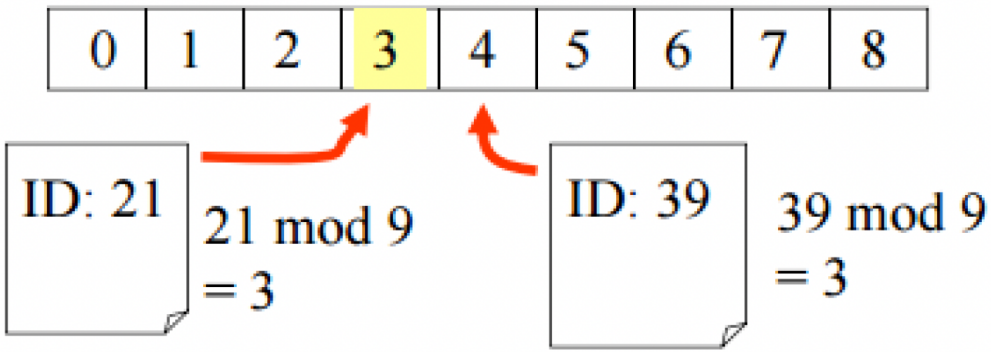
SUSTech Southern University of Science and Technology

Hash Functions

One way is to assign the first free location following the occupied memory location assigned by the hashing function.

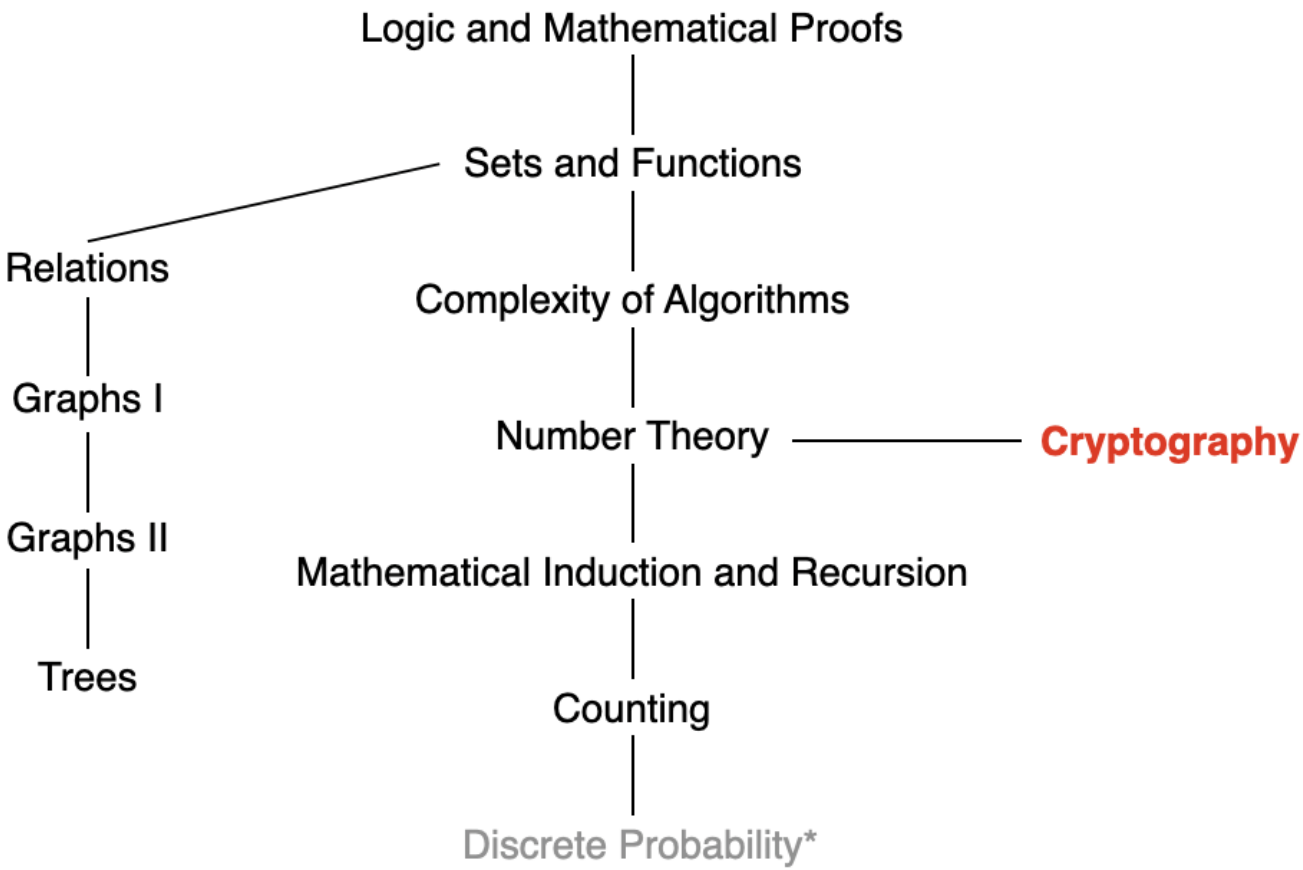
try

$$h_0(k) = k \bmod n$$
$$h_1(k) = (k+1) \bmod n$$
$$\ldots$$
$$h_m(k) = (k+m) \bmod n$$



SUSTech Southern University of Science and Technology

This Lecture



Cryptograhy: classical cryptography, RAS cryptosystem,

SUSTech Southern University of Science and Technology

Cryptography

History of almost 4000 years (from 1900 B.C.)

Cryptography = kryptos + graphos

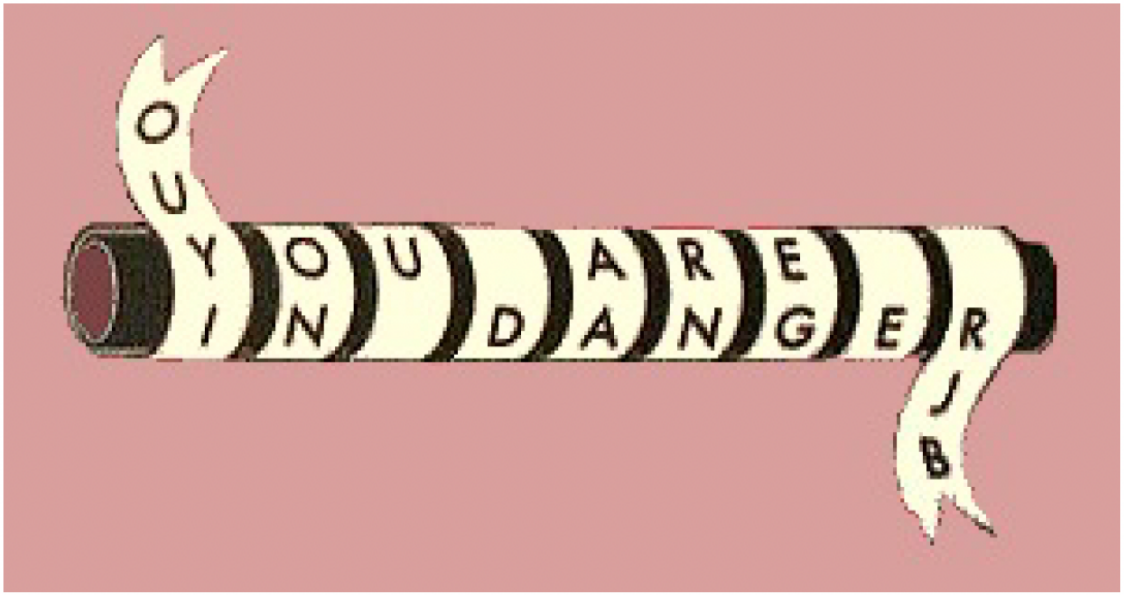
- kryptos: secret
- graphos: writing

One-sentence definition: "Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries." – Ronald L. Rivest

SUSTech Southern University of Science and Technology

Some Examples

In 405 B.C., the Greek general LYSANDER OF SPARTA was sent a coded message written on the inside of a servant's belt.



SUSTech Southern University of Science and Technology

Some Examples

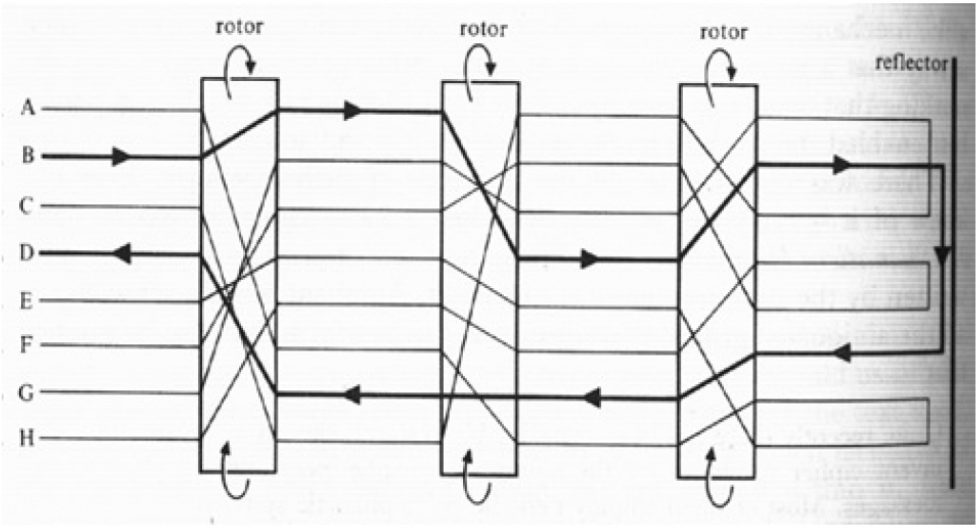
The Greeks also invented a cipher which changed letters to numbers. A form of this code was still being used during World War I.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

SUSTech Southern University of Science and Technology

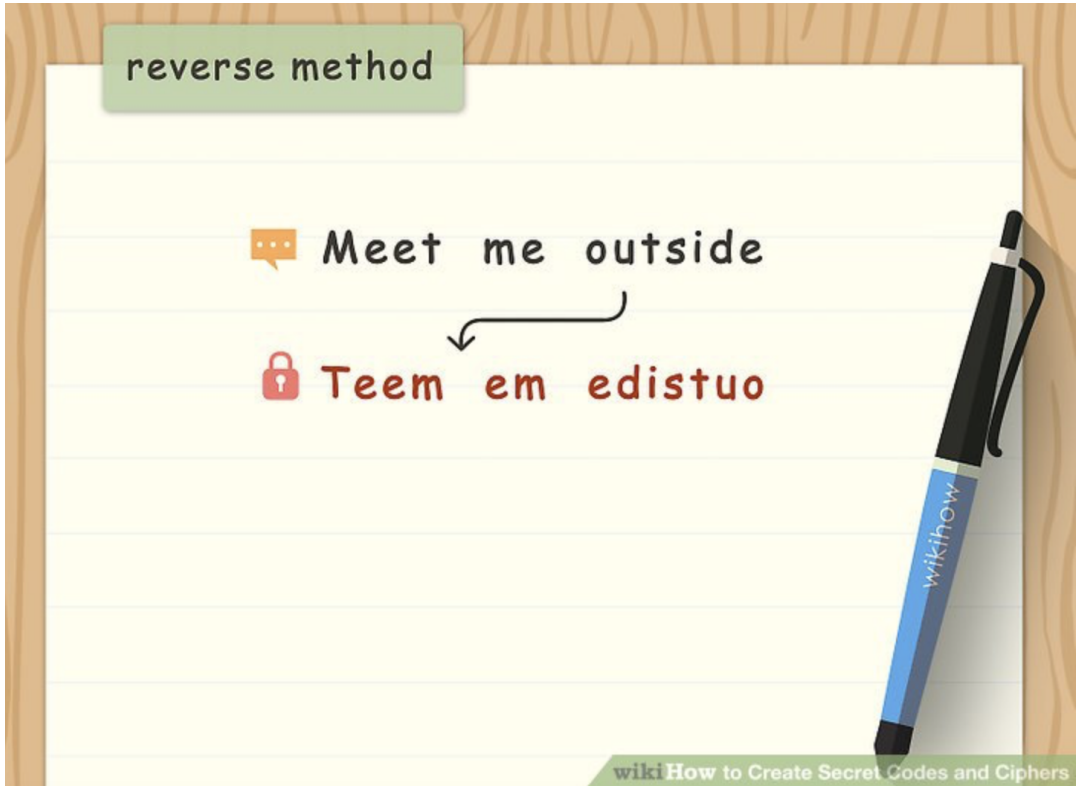
Some Examples

Enigma, Germany coding machine in World War II.



SUSTech Southern University of Science and Technology

Some Examples



SUSTech Southern University of Science and Technology

Shift Ciphers

Shift Ciphers: Make messages secret by shifting each letter several letters forward in the alphabet.

Encryption:

- Assign each letter an integer $p \in \mathbf{Z}_{26} = \{0, 1, ..., 25\}$ based on the location of the letter in the alphabet.
- Replace p with $f(p)$:

$$f(p) = (p + k) \bmod 26.$$

- Maps $f(p)$ back to the alphabet.

SUSTech Southern University of Science and Technology

Shift Ciphers

Example: What is the secret message produced from the message "MEET YOU IN THE PARK" using the Shift cipher with $k = 3$?

Solution: First replace the letters in the message with numbers. This produces

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10.

Now replace each of these numbers p by $f(p) = (p + 3)$ **mod** 26. This gives

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13.

Translating this back to letters produces the encrypted message "PHHW BRX LQ WKH SDUN."

SUSTech Southern University of Science and Technology

Shift Ciphers

Shift Ciphers: Make messages secret by shifting each letter several letters forward in the alphabet.

Decryption:

- Assign each letter an integer $p \in \mathbf{Z}_{26} = \{0, 1, ..., 25\}$ based on the location of the letter in the alphabet.
- Replace p with $f^{-1}(p)$:

$$f^{-1}(p) = (p-k) \bmod 26.$$

- Maps $f^{-1}(p)$ back to the alphabet.

SUSTech Southern University of Science and Technology

Shift Ciphers

We can generalize shift ciphers further to slightly enhance security by using a function of the form

$$f(p) = (ap + b) \textbf{ mod } 26.$$

How about the decryption? Suppose $\gcd(a, 26) = 1$.

Suppose that $c = (ap + b)$ **mod** 26 with $\gcd(a, 26) = 1$. To decrypt, we need to show how to express p in terms of c. That is, we solve the congruence for p:

$$c \equiv ap + b \ (\textbf{mod } 26).$$

Subtract b from both sides, we have $ap \equiv c - b$ (**mod** 26). Since $\gcd(a, 26) = 1$, we know that there is an inverse $\bar{a}$ of a modulo 26:

$$p \equiv \bar{a}(c - b) \ (\textbf{mod } 26).$$

SUSTech Southern University of Science and Technology

Cryptanalysis

The process of recovering plaintext from ciphertext without knowledge of both the encryption method and the key is known as cryptanalysis or breaking codes.

How to break messages that were encrypted using a shift cipher?

Solution 1: Try each 26 possible shifts.

Solution 2: Try different values of k based on the frequency of letters in the ciphertext. The nine most common letters in English text: E: 13%, T: 9%, A: 8%, O: 8%, I: 7%, N: 7%, S: 7%, H: 6%, and R: 6%.

SUSTech Southern University of Science and Technology

Private Key Cryptosystem

In a **private key cryptosystem**, once you know an encryption key, you can quickly find the decryption key.

When a private key cryptosystem is used, two parties who wish to communicate in secret must share a secret key.

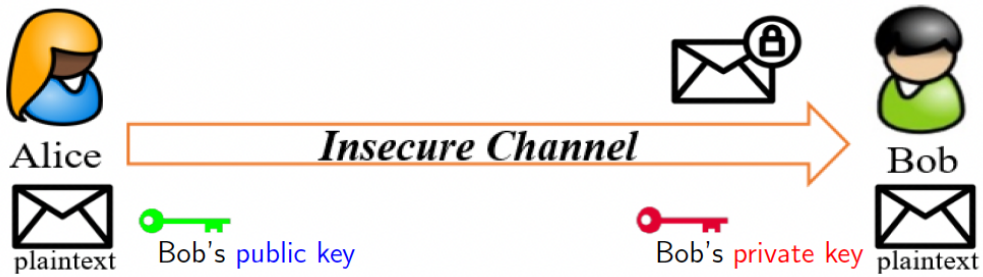
Any problems?

- Two people who want to communicate securely need to securely exchange this key.
- New key is used for each communication session between two parties.

SUSTech Southern University of Science and Technology

Public Key Cryptosystem

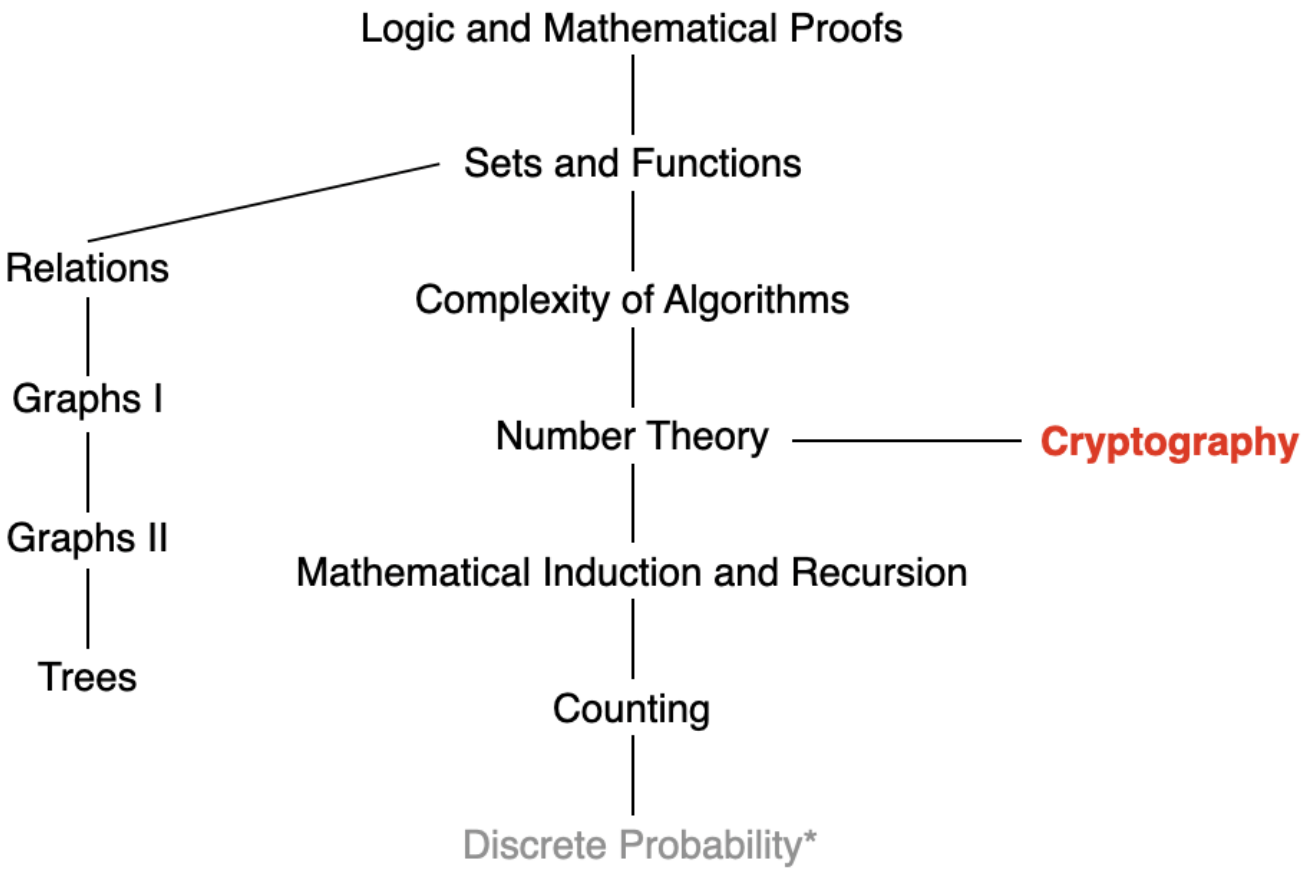
In **public key cryptosystems**, knowing how to send an encrypted message does not help decrypt messages.



- Public key is known to the public.
- Private key is kept secret: only the intended recipient of a message can decrypt it.

SUSTech Southern University of Science and Technology

This Lecture

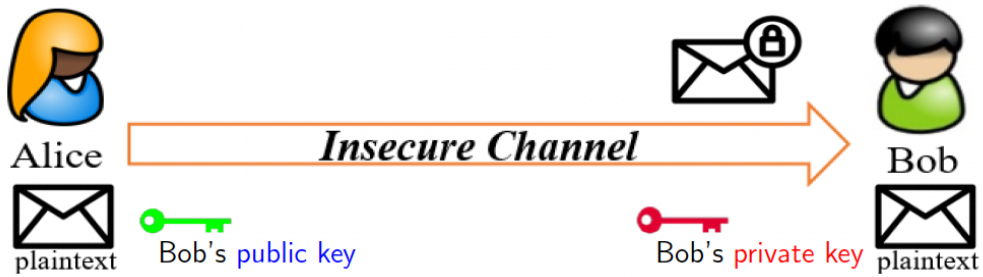


Cryptograhy: classical cryptography, RSA cryptosystem, ...

SUSTech Southern University of Science and Technology

Overview

- RSA as Public Key System
  - Only target recipient can decrypt the message:



- RSA as Digital Signature
- Diffie-Hellman Key Exchange Protocol

SUSTech Southern University of Science and Technology

RSA Cryptosystem

Rivest-Shamir-Adleman **2002 Turing Award**

2002	Ronald L. Rivest, Adi Shamir and Leonard M. Adleman	For their ingenious contribution for making **public-key cryptography** useful in practice.

Pick two large primes p and q. Let $n = pq$. **Encryption key** (n, e) and **decryption key** (n, d) are selected such that

- $\gcd(e, (p-1)(q-1)) = 1$
- $ed \equiv 1$ (**mod** $(p-1)(q-1)$)

RSA encryption: $C = M^e$ **mod** n

RSA decryption: $M = C^d$ **mod** n

SUSTech Southern University of Science and Technology

RSA Encryption

1. Translate a plaintext message into integers, each with two digits, e.g, A is translated into 00, B into 01, . . . , and Z into 25.
2. Divide this string into equally sized blocks of $2N$ digits
   - $2N$ is the largest even number such that the number 2525...25 with $2N$ digits does not exceed n.
3. For each block, transform it into a ciphertext block:

$$C = M^e \ \textbf{mod} \ n$$

SUSTech Southern University of Science and Technology

RSA Encryption: Example

Encrypt the message "STOP" with key $(n = 2537, e = 13)$. Note that $2537 = 43 \cdot 59$, where $p = 43$ and $q = 59$ are primes, and $\gcd(e, (p-1)(q-1)) = 1$.

Solution:

1. Translate into integers: 18191415
2. Divide this into blocks of 4 digits (because $2525 < 2537 < 252525$): 1819 1415
3. Encrypt each block using the mapping

$$C = M^{13} \textbf{ mod } 2537.$$

We have 1819^{13} **mod** $2537 = 2081$ and 1415^{13} **mod** $2537 = 2182$. The encrypted message is 2081 2182.

SUSTech Southern University of Science and Technology

RSA Decryption

For each block, transform the ciphertext into plaintext message:

$$M = C^d \ \textbf{mod}\ n$$

Example: What is the decrypted message of 0981 0461 with $e = 13$, $p = 43$, $q = 59$?

Solution: Recall that $ed \equiv 1\ (\textbf{mod}\ (p-1)(q-1))$. Thus, $d = 937$ is an inverse of 13 modulo $42 \cdot 58 = 2436$.

For each block, transform it into plaintext message:

$$M = C^{937} \ \textbf{mod}\ 2537.$$

Since $0981^{937}\ \textbf{mod}\ 2537 = 0704$ and $0461^{937}\ \textbf{mod}\ 2537 = 1115$, the plaintext message is 0704 1115, which is "HELP".

SUSTech Southern University of Science and Technology

RAS Cryptosystem

Pick two large primes p and q. Let $n = pq$. **Encryption key** (n, e) and **decryption key** (n, d) are selected such that

(1) $\gcd(e, (p-1)(q-1)) = 1$

(2) $ed \equiv 1$ (**mod** $(p-1)(q-1)$)

RSA encryption: $C = M^e$ **mod** n;
RSA decryption: $M = C^d$ **mod** n. Why?

According to (1), the inverse d exists. According to (2), there exists an integer k such that

$$de = 1 + k(p-1)(q-1).$$

It follows that $C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)}$(**mod** n).

Assuming that $\gcd(M, p) = \gcd(M, q) = 1$, we have $M^{p-1} \equiv 1$ (**mod** p) and $M^{q-1} \equiv 1$(**mod** q). (see Theorem 3 in Section 4.4)

RAS Cryptosystem

According to (1), the inverse d exists. According to (2), there exists an integer k such that

$$de = 1 + k(p-1)(q-1).$$

It follows that $C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} (\textbf{mod } n)$.

Assuming that $\gcd(M, p) = \gcd(M, q) = 1$, we have $M^{p-1} \equiv 1 \ (\textbf{mod } p)$ and $M^{q-1} \equiv 1 (\textbf{mod } q)$.

$$C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 = M \ (\textbf{mod } p)$$
$$C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 = M \ (\textbf{mod } q).$$

Because $\gcd(p, q) = 1$, we have

$$C^d \equiv M \ (\textbf{mod } pq).$$

This basically implies that

$$M = C^d \textbf{ mod } n$$

SUSTech Southern University of Science and Technology

RSA as Public Key System

Pick two large primes p and q. Let $n = pq$. **Encryption key** (n, e) and **decryption key** (n, d) are selected such that

(1) $\gcd(e, (p-1)(q-1)) = 1$

(2) $ed \equiv 1$ (**mod** $(p-1)(q-1)$)

RSA encryption: $C = M^e$ **mod** n;
RSA decryption: $M = C^d$ **mod** n.

RSA as a Public Key System

- Public key: (n, e)
- Private key: d
- p, q must be kept secret!

Why is the RSA cryptosystem suitable for public key cryptography?

SUSTech Southern University of Science and Technology

RSA as Public Key System

RSA as a Public Key System

- Public key: (n, e); Private key: (n, d)
- p, q must be kept secret!

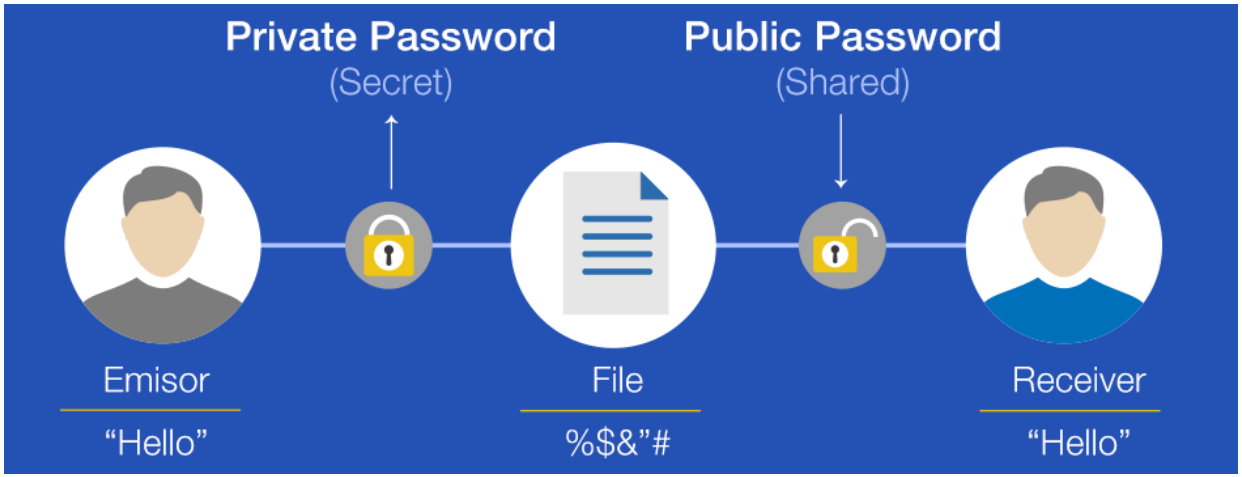
Why is the RSA cryptosystem suitable for public key cryptography?

- It is possible to rapidly construct a public key by finding two large primes p and q, each with more than 200 digits.
- When we know p and q, we can quickly find an inverse d.
- However, no method is known to decrypt messages that is not based on finding a factorization of n.
  - Factorization is believed to be a difficult problem.
  - The most efficient factorization methods known (as of 2010) require billions of years to factor 400-digit integers.

SUSTech Southern University of Science and Technology

Overview

- RSA as Public Key System
- RSA as Digital Signature
  - The recipient of the message knows that it came from the person they think it came from.



- Diffie-Hellman Key Exchange Protocol

SUSTech Southern University of Science and Technology

RSA as Digital Signature

Alice's RSA public key is (n, e) and her private key is d.

Alice splits the plaintext message into blocks and applies her decryption function:

$$S = M^d \textbf{ mod } n \quad \textbf{(RSA signature)}$$

When a recipient receives her message, they apply Alice's encryption function:

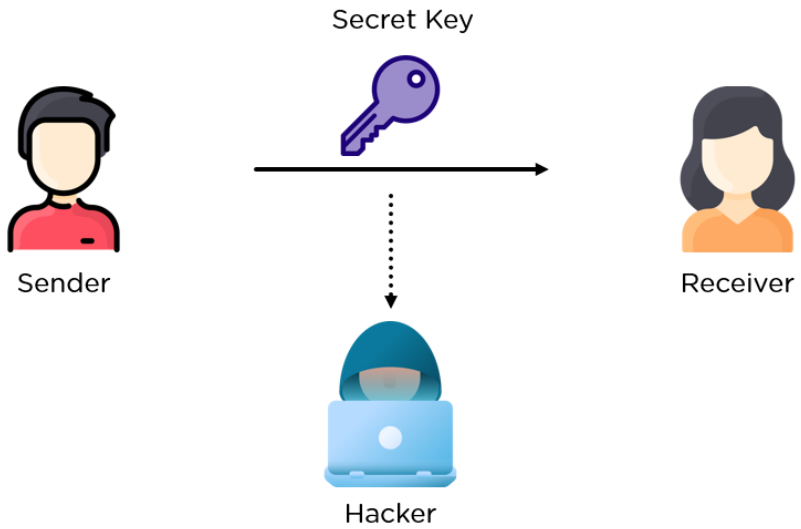
$$M = S^e \textbf{ mod } n \quad \textbf{(RSA verification)}$$

Alice can send her message to as many people as she wants and by signing it in this way, every recipient can be sure it came from Alice.

SUSTech Southern University of Science and Technology

Overview

- RSA as a Public Key System
- RSA as Digital Signature
- Diffie-Hellman Key Exchange Protocol
  - Exchange a secret key over an insecure communications channel



SUSTech Southern University of Science and Technology

Diffie-Hellman Key Exchange Protocol

Two parties exchange a secret key over an insecure communications channel without having shared any information in the past.

Diffie-Hellman Key Exchange Protocol

Before introducing the protocol:

Definition: A primitive root modulo a prime p is an integer r in $\mathbf{Z}_p$ such that every nonzero element of $\mathbf{Z}_p$ is a power of r.

Example: Whether 2 is a primitive root modulo 11?

When we compute the powers of 2 in $\mathbf{Z}_{11}$, we obtain $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^9 = 6$, $2^{10} = 1$.
Because every element of $\mathbf{Z}_{11}$ is a power of 2, 2 is a primitive root of 11.

SUSTech Southern University of Science and Technology

Diffie-Hellman Key Exchange Protocol

Suppose that Alice and Bob want to share a common key. Consider $\mathbf{Z}_p$.

(1) Alice and Bob agree to use a prime p and a primitive root a of p.

(2) Alice chooses a secret integer k_1 and sends a^{k_1} **mod** p to Bob.

(3) Bob chooses a secret integer k_2 and sends a^{k_2} **mod** p to Alice.

(4) Alice computes $(a^{k_2})^{k_1}$ **mod** p.

(5) Bob computes $(a^{k_1})^{k_2}$ **mod** p.

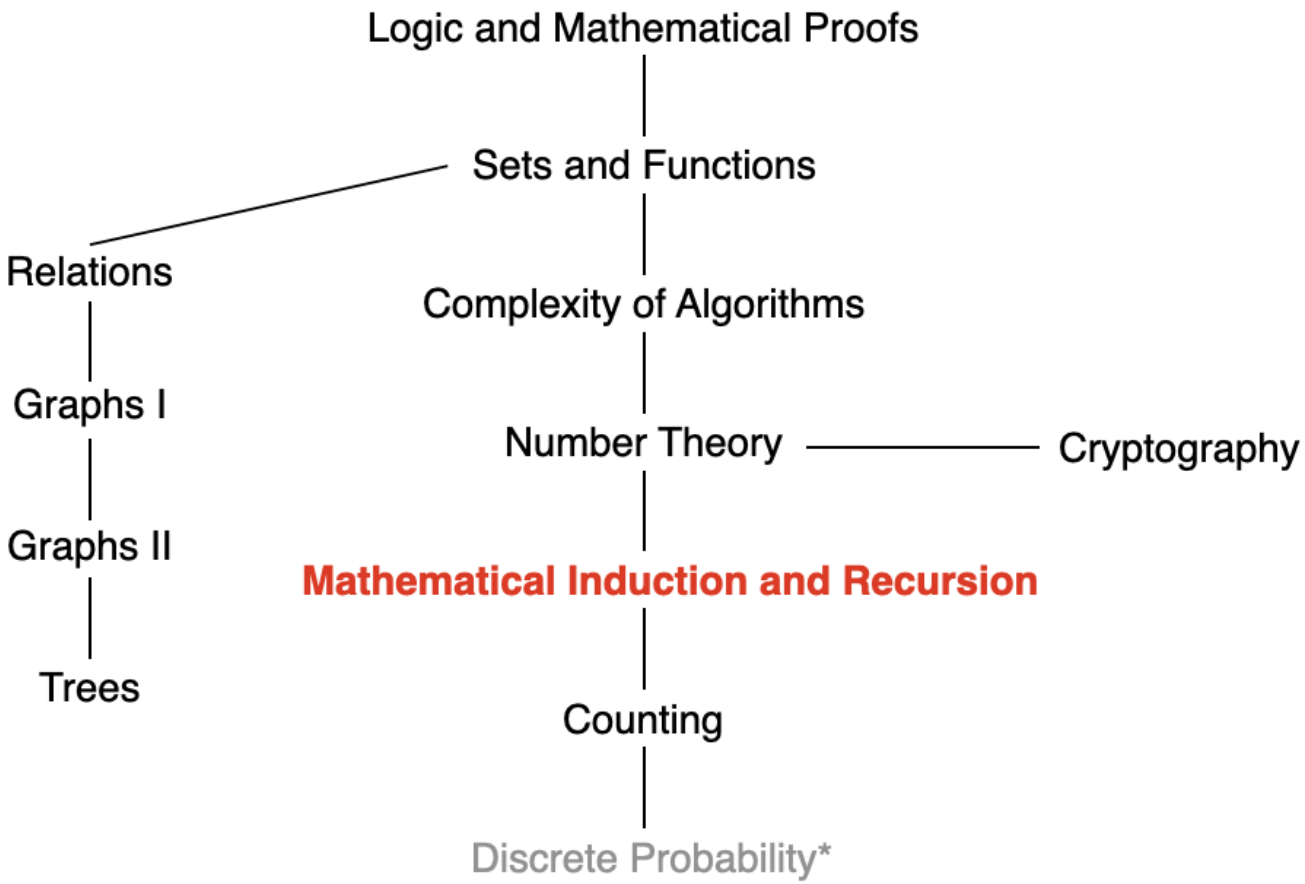
Alice and Bob have computed their shared key:

$$(a^{k_2})^{k_1} \textbf{ mod } p = (a^{k_1})^{k_2} \textbf{ mod } p.$$

- Public information: p, a, a^{k_1} **mod** p, and a^{k_2} **mod** p
- Secret: k_1, k_2, $(a^{k_2})^{k_1}$ **mod** $p = (a^{k_1})^{k_2}$ **mod** p

Note that it is very hard to determine k_1 with a, p, and a^{k_1} **mod** p.

Next Lecture



SUSTech Southern University of Science and Technology