Number Theory and Cryptography

CMPS/MATH 2170: Discrete Mathematics

Outline

- Divisibility and Modular Arithmetic (4.1)
- Primes and GCD (4.3)
- Solving Congruences (4.4)
- Cryptography (4.6)

Division

Definition: Let $a, b \in \mathbb{Z}$ with $a \neq 0$. we say a divides b if $b/a \in \mathbb{Z}$

- equivalently, $b = ka$ for some $k \in \mathbb{Z}$
- we use $a \mid b$ to denote a divides b (or b is divisible by a)
- if $a \mid b$, we say that a is a factor or divisor of b

Ex. 1: Determine whether

a. $3 \mid 7$

b. $3 \mid 12$

Ex. 2: How many positive integers not exceeding n are divisible by 3? $\lfloor n/3 \rfloor$

Division (cont.)

Theorem: Let $a, b, c \in \mathbb{Z}$ and $a \neq 0$. Then

(i) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$

(ii) If $a \mid b$, then $a \mid bc$

(iii) If $a \mid b$ and $b \mid c$ $(b \neq 0)$, then $a \mid c$

Prime Numbers

Definition: An integer $p > 1$ is called prime if the only positive factors of p are 1 and p

- p is prime $\Leftrightarrow \forall a \in \mathbb{Z}^+ \colon a \mid p \rightarrow a = 1$ or $a = p$

Definition: An integer > 1 that is not prime is called composite

- 1 is neither prime nor composite

The Fundamental Theorem of Arithmetic

Theorem: Every positive integer > 1 can be written uniquely as a prime or as the product of two or more primes written in a non-decreasing order

- "prime factorization of an integer"

- [ ] prime factorization is hard for large numbers

Ex: $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

$641 = 641$

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$

Proof of the fundamental theorem:

1. existence: strong induction
2. uniqueness: to be proved

Applications of the Fundamental Theorem

Theorem: A composite n has a prime divisor $\leq \sqrt{n}$.

Corollary: An integer $p > 1$ is a prime if it is not divisible by any prime $\leq \sqrt{p}$.

Ex: Show that 101 is prime

Theorem: There are infinitely many primes

- A proof given by Euclid in *The Elements*

Two Great Open Problems on Primes

- Goldbach's conjecture (1742): every even number $n > 2$ is the sum of two primes
  - Every even number $n > 2$ is the sum of at most 6 primes (1995)
  - Every even number $n > 2$ is the sum of a prime and a number that is either prime or the product of two primes (1+2, 1966)
- Twin prime conjecture (before 1849): there are infinitely many twin primes
  - Twin prime pairs: (3, 5), (5,7), (11, 13), (17, 19), (29, 31), …
  - There are infinitely many pairs of prime numbers that differ by 246 or less (2014)

Greatest Common Divisors

Definition: Let $a, b \in \mathbb{Z}$, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b, denoted by $d = \gcd(a, b)$

Ex: $\gcd(24, 36) = 12$

$\gcd(17, 22) = 1$

$\gcd(120, 500) = \gcd(2^3 \cdot 3 \cdot 5,\ 2^2 \cdot 5^3) = 2^2 \cdot 5 = 20$

$$\gcd\left(p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n},\ p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}\right) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

- Is there a more efficient way to find gcd?

Least Common Multiples

Let $a, b \in \mathbb{Z}$, $a, b \neq 0$. The smallest positive integer that is divisible by both a and b is called the least common multiple of a and b, denoted by $\text{lcm}(a, b)$

Ex: $\text{lcm}(24, 36) = \text{lcm}(2^3 \cdot 3, 2^2 \cdot 3^2) = 2^3 \cdot 3^2 = 72$

$$\text{lcm}(p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n},\ p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

Theorem: For any positive integers a and b, $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$

The Division Algorithm

Theorem: Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then there are unique $q, r \in \mathbb{Z}$, with $0 \leq r < d$, such that

$$a = dq + r$$

divisor quotient remainder

Ex: $a = 101, d = 2$

$a = -11, d = 3$

$q = a \text{ div } d = \lfloor a/d \rfloor$

$r = a \text{ mod } d = a - d\lfloor a/d \rfloor$ $\quad d \mid a \Leftrightarrow a \text{ mod } d = 0$

The Division Algorithm

Theorem: Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. Then there are unique $q, r \in \mathbb{Z}$, with $0 \leq r < d$, such that $a = dq + r$

1. Existence (5.2 Example 5): use the well-ordering property: "Every nonempty subset of $\mathbb{N}$ has a least element"

2. Uniqueness (exercise)

The Euclidean Algorithm

- A useful fact about the division algorithm:

Theorem: Let $a = bq + r$, where $a, b, q, r \in \mathbb{Z}$. Then $\gcd(a, b) = \gcd(b, r)$

- A more efficient way to find gcd:

Euclidean Algorithm: find $\gcd(a, b)$ by successively applying the division algorithm

The Euclidean Algorithm

Ex: Find gcd(287,91) using the Euclidean Algorithm

$287 = 91 \cdot 3 + 14 \qquad \gcd(287,91) = \gcd(91,14)$

$91 = 14 \cdot 6 + 7 \qquad \gcd(91,14) = \gcd(14,7)$

$\Rightarrow \gcd(287,91) = \gcd(91,14) = \gcd(14,7) = 7$

GCDs as Linear Combinations

Bezout's Theorem: Let $a, b \in \mathbb{Z}^+$. There exist $s, t \in \mathbb{Z}$ such that

$$\gcd(a, b) = sa + tb$$

Ex: Find $s, t \in \mathbb{Z}$ such that $\gcd(54,15) = s \cdot 54 + t \cdot 15$

$$54 = 3 \cdot 15 + 9$$
$$15 = 1 \cdot 9 + 6$$
$$9 = 1 \cdot 6 + 3$$

$$9 = 54 - 3 \cdot 15$$
$$6 = 15 - 1 \cdot 9$$
$$3 = 9 - 1 \cdot 6$$

$$\begin{aligned} \gcd(54,15) &= \gcd(15,9) \\ &= \gcd(9,6) \\ &= \gcd(6,3) \\ &= 3 \end{aligned}$$

Backward substitution gives

$$\begin{aligned} 3 &= 9 - 1 \cdot 6 \\ &= 9 - 1 \cdot (15 - 1 \cdot 9) \\ &= 2 \cdot 9 - 1 \cdot 15 \\ &= 2 \cdot (54 - 3 \cdot 15) - 1 \cdot 15 \\ &= 2 \cdot 54 - 7 \cdot 15 \end{aligned}$$

$\Rightarrow s = 2,\ t = -7$

Applications of Bezout's Theorem

Lemma: If $a, b, c \in \mathbb{Z}^+$ such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$

- We say that a and b are relatively prime if $\gcd(a, b) = 1$

Corollary: If p is a prime and $p \mid a_1 a_2 \dots a_n$ where each a_i is an integer, then $p \mid a_i$ for some i.

The Fundamental Theorem of Arithmetic: Every positive integer > 1 can be written uniquely as a prime or as the product of two or more primes where the primer factors are written in non-decreasing order

Proof: 1. existence: strong induction

2. uniqueness: using the above corollary

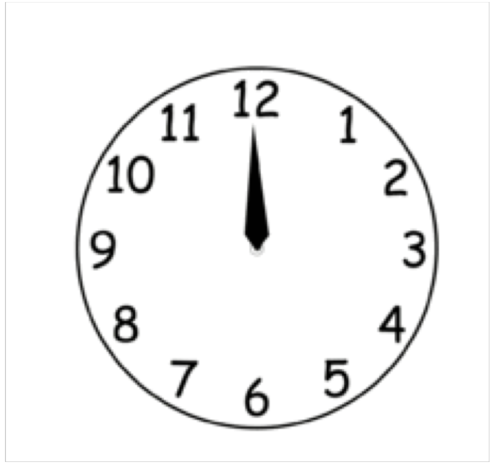
Wrap Up

1. Divisibility: $a \mid b \Leftrightarrow b = ka$ for some integer k
2. Primes
   - the Fundamental theorem of Arithmetic
   - A composite n has a prime divisor $\leq \sqrt{n}$
   - there are infinite many primes
3. Greatest common divisor and least common multiple
4. Division algorithm: $a = dq + r,\ 0 \leq r < d$
   - $\gcd(a, d) = \gcd(d, r)$
5. Euclidean algorithm: find gcd by successively applying the division algorithm
6. Bezout's Theorem: $\gcd(a, b) = sa + tb$
   - If $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$

Congruences

Definition: Let $a, b \in \mathbb{Z}, m \in \mathbb{Z}^+$, we say a is congruent to b modulo m if $m \mid (a-b)$

- If a is congruent to b modulo m, we write $a \equiv b \pmod{m}$



- Examples
  - $17 \equiv 5 \pmod{6}$? $14 \equiv 2 \pmod{12}$
  - $11 \equiv 8 \pmod{2}$? $23 \equiv 11 \pmod{12}$

- $a \equiv b \pmod{m} \Leftrightarrow m \mid (a-b)$

$$\Leftrightarrow a - b = km \text{ for some } k \in \mathbb{Z}$$

$$\Leftrightarrow a = km + b \text{ for some } k \in \mathbb{Z}$$

Congruences (cont.)

Theorem: Let $a, b, c, d \in \mathbb{Z}, m \in \mathbb{Z}^+$

- $a \equiv b \pmod{m} \Leftrightarrow (a \bmod m) = (b \bmod m)$
- If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Theorem: Let $a \in \mathbb{Z}, m \in \mathbb{Z}^+$. There is a unique $a_0 \in \{0,1, \ldots, m-1\}$ such that $a \equiv a_0 \pmod{m}$.

Arithmetic Modulo m

$\mathbb{Z}_m = \{0,1, \dots, m-1\}$

Addition modulo m: $a +_m b = (a + b) \bmod m$

Multiplication modulo m: $a \cdot_m b = (a \cdot b) \bmod m$

Ex: $6 +_{12} 9$, $7 \cdot_{11} 8$

- $a +_m b = c \Rightarrow a + b \equiv c \pmod{m}$
- $a \cdot_m b = c \Rightarrow a \cdot b \equiv c \pmod{m}$

Properties of $\mathbb{Z}_m$

For any $a, b, c \in \mathbb{Z}_m$

- Closure: $a +_m b \in \mathbb{Z}_m$

  $a \cdot_m b \in \mathbb{Z}_m$

- Associativity: $(a +_m b) +_m \ c = a +_m (b +_m c)$

  $(a \cdot_m b) \cdot_m \ c = a \cdot_m (b \cdot_m c)$

- Commutativity: $a +_m b = b +_m a$

  $a \cdot_m b = b \cdot_m a$

Properties of $\mathbb{Z}_m$

For any $a, b, c \in \mathbb{Z}_m$

- Distributivity: $a \cdot_m (b +_m c) = a \cdot_m b +_m a \cdot_m c$

  $(a +_m b) \cdot_m c = a \cdot_m c +_m b \cdot_m c$

- Identity elements: $a +_m 0 = 0 +_m a = a$

  $a \cdot_m 1 = 1 \cdot_m a = a$

- Additive inverse: For every $a \in \mathbb{Z}_m$, there is $b \in \mathbb{Z}_m$, such that $a +_m b = 0$

  $0 +_m 0 = 0$

  $a +_m (m - a) = 0$ for $a \neq 0$

Properties of $\mathbb{Z}_m$

- For $a \in \mathbb{Z}_m$, $b \in \mathbb{Z}_m$ is a multiplicative inverse of a if $a \cdot_m b = 1$,
  - does 2 have a multiplicative inverse in $\mathbb{Z}_4$? No
  - does 2 have a multiplicative inverse modulo $\mathbb{Z}_5$? Yes $2 \cdot 3 \equiv 1 \pmod 5$
- Theorem: a has a multiplicative inverse in $\mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$.
- Corollary: Every non-zero element has a multiplicative inverse in $\mathbb{Z}_p$ when p is prime

Additive Inverse and Multiplicative Inverse

- For $a, b \in \mathbb{Z}$,
  - b is an additive inverse of a modulo $m \in \mathbb{Z}^+$ if $a + b \equiv 0 \pmod{m}$
  - b is an multiplicative inverse of a modulo $m \in \mathbb{Z}^+$ if $a \cdot b \equiv 1 \pmod{m}$

- Theorem: $a \in \mathbb{Z}$ and $a \neq 0$ has a multiplicative inverse modulo $m \in \mathbb{Z}^+$ if and only if $\gcd(a, m) = 1$. Furthermore, an inverse, when it exists, is unique modulo m.

Find Multiplicative Inverses

Ex 1: Find a multiplicative inverse of 3 modulo 7

$$3x \equiv 1 \equiv 8 \equiv 15 \pmod{7} \Rightarrow x \equiv 5 \pmod{7}$$

Ex 2: Find a multiplicative inverse of 5 modulo 3

$$5x \equiv 1 \equiv 4 \equiv 7 \equiv 10 \pmod{3} \Rightarrow x \equiv 2 \pmod{3}$$

Use Bezout's Theorem to find an inverse of a modulo m, where $\gcd(a, m) = 1$

- find $s, t \in \mathbb{Z}$ such that $sa + tm = 1$
- s is a multiplicative inverse of a modulo m

Ex 3: Find an inverse of 101 modulo 4620 (4.4 Example 2)

Solving Linear Congruences

Problem: Given $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, find $x \in \mathbb{Z}$ such that

$$ax \equiv b \pmod{m}$$

Let us first assume $\gcd(a, m) = 1$.

Ex: Find the solution of $3x \equiv 4 \pmod{7}$

$$3x \equiv 4 \equiv 11 \equiv 18 \pmod{7}$$

$$\Rightarrow x \equiv 6 \pmod{7}$$

We know $3 \cdot 5 \equiv 1 \pmod{7}$

Then $3x \equiv 4 \pmod{7}$

$$\Rightarrow 5 \cdot 3x \equiv 5 \cdot 4 \pmod{7}$$

$$\Rightarrow x \equiv 20 \equiv 6 \pmod{7}$$

Solving Linear Congruences

Problem: Given $a, b \in \mathbb{Z},\ m \in \mathbb{Z}^+$, find all $x \in \mathbb{Z}$ such that

$$ax \equiv b \pmod{m}$$

Q: What if $\gcd(a, m) = d > 1$?

A: For the linear congruence to have a solution, we must have $d \mid b$

$\Rightarrow$ We only need to solve $a'x \equiv b' \pmod{m'}$ where $a' = \frac{a}{d},\ b' = \frac{b}{d}$, and $m' = \frac{m}{d}$

Ex: Find the solution of $15x \equiv 6 \pmod{9}$

Modular Exponentiation and Fermat's Little Theorem

Pierre de Fermat

Ex: Find 2^7 mod 7

Fermat's Little Theorem: If p is prime, then for every integer a we have

$$a^p \equiv a \pmod{p}$$

Further, if a is not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

➢ See 4.4 Exercise 19 for a proof sketch

Ex: Find 7^{222} mod 11

To compute a^n mod p where p is prime and $p \nmid a$

- First write $n = q(p-1) + r$ where $0 \leq r < p - 1$
- Then $a^n = a^{q(p-1)+r}$

$$= (a^{p-1})^q a^r$$

$$\equiv 1^q a^r \pmod{p}$$

$$\equiv a^r \pmod{p}$$

Fast Modular Exponentiation

Ex: Find 3^{36} mod 645

$36 = 2^5 + 2^2$

3^{2^1} mod 645 = 9

3^{2^2} mod 645 = 9^2 mod $645 = 81$

3^{2^3} mod 645 = 81^2 mod $645 = 6561$ mod $645 = 111$

3^{2^4} mod 645 = 111^2 mod $645 = 12{,}321$ mod $645 = 66$

3^{2^5} mod 645 = 66^2 mod $645 = 4356$ mod $645 = 486$

3^{36} mod $645 = 3^{2^5} \cdot 3^{2^2}$ mod $645 = 486 \cdot 81$ mod $645 = 21$

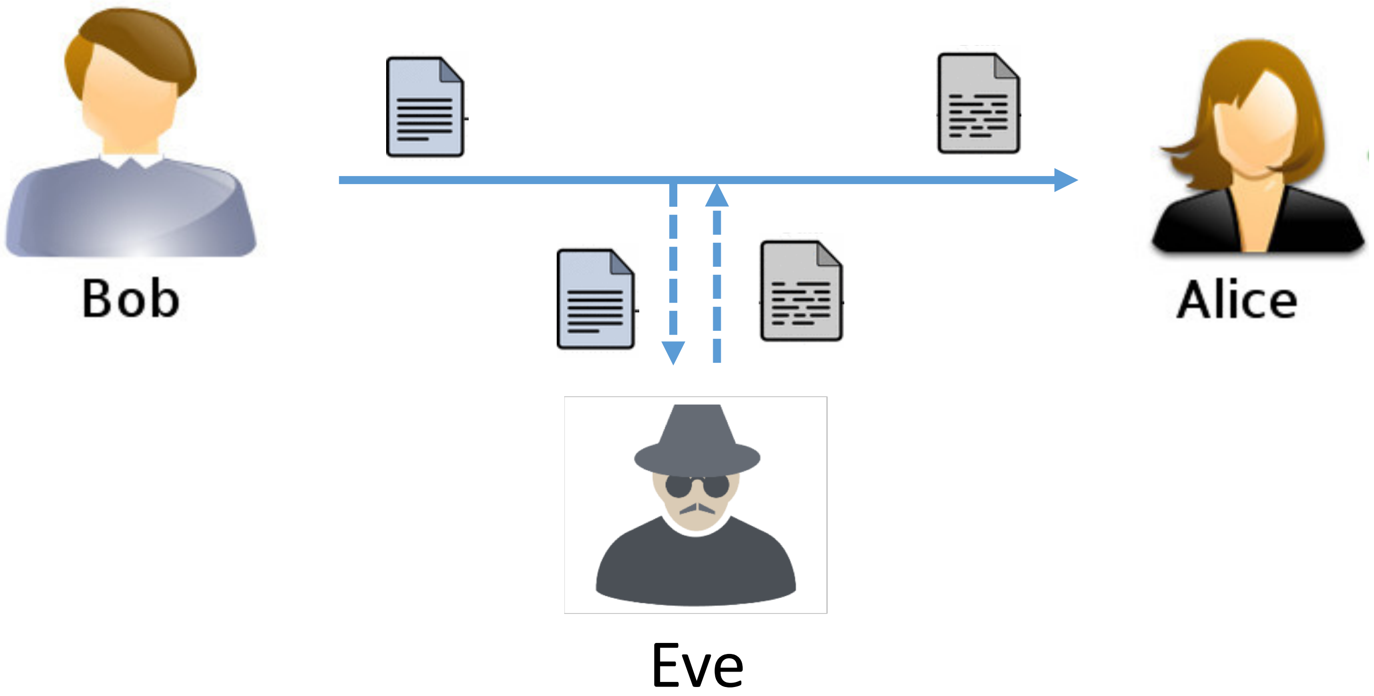
Outline

- Divisibility and Modular Arithmetic (4.1)
- Primes and GCD (4.3)
- Solving Congruences (4.4)
- Cryptography (4.6)

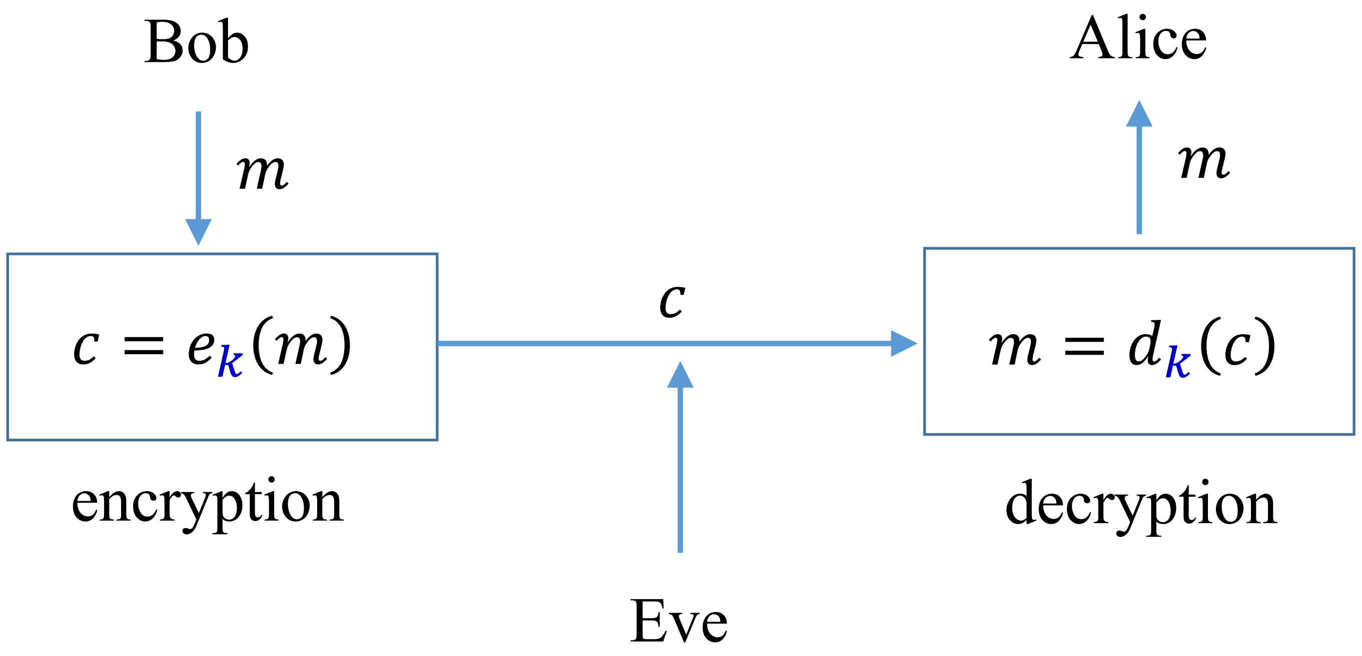
Introduction to Cryptography

- Classical Cryptography
  - Shift Cipher
  - Affine Cipher
- Public Key Cryptography
  - RSA

Symmetric Key Cryptography



Symmetric Key Cryptography



- Bob and Alice need to share the secret key k
- Need to make sure $m = d_k(e_k(m))$

Shift Cipher

- Caesar Cipher: shift each letter three letters forward in the alphabet
  - Plain: $A\ B\ C\ D\ E\ F\ \ldots T\ U\ V\ W\ X\ Y\ Z$
  - Cipher: $d\ e\ f\ g\ h\ i\ \ldots w\ x\ y\ z\ a\ b\ c$
  - Ex: TULANE $\rightarrow$ $wxodqh$

- Mathematically, encode letters as numbers in $\mathbb{Z}_{26} = \{0,1,\ldots,25\}$
  - $A\ B\ C\ D\ E\ F\ \ldots\ U\ V\ W\ X\ Y\ Z$
  - $0\ 1\ 2\ 3\ 4\ 5\ \ldots\ 20\ 21\ 22\ 23\ 24\ 25$

- Encryption: $c = e_k(m) = (m + k) \bmod 26$
- Decryption: $m = d_k(c) = (c - k) \bmod 26$
- Do we have $m = d_k(e_k(m))$?

m: plaintext, c: ciphertext, k: key

$m, c, k \in \mathbb{Z}_{26}$

Affine Cipher

- Encryption: $c = (a \cdot m + b) \bmod 26$
  - (a, b) is the key where $a, b \in \mathbb{Z}_{26}$ and $\gcd(a, 26) = 1$
  - Ex: $a = 7, b = 3,\ m = 10$ (‘K’), what is c? $c = 21$ (‘v’)
- Decryption: $m = \bar{a}(c - b) \bmod 26$
  - $\bar{a} \in \mathbb{Z}_{26},\ a\bar{a} \equiv 1 \pmod{26}$
- Do we have $m = d_k(e_k(m))$?

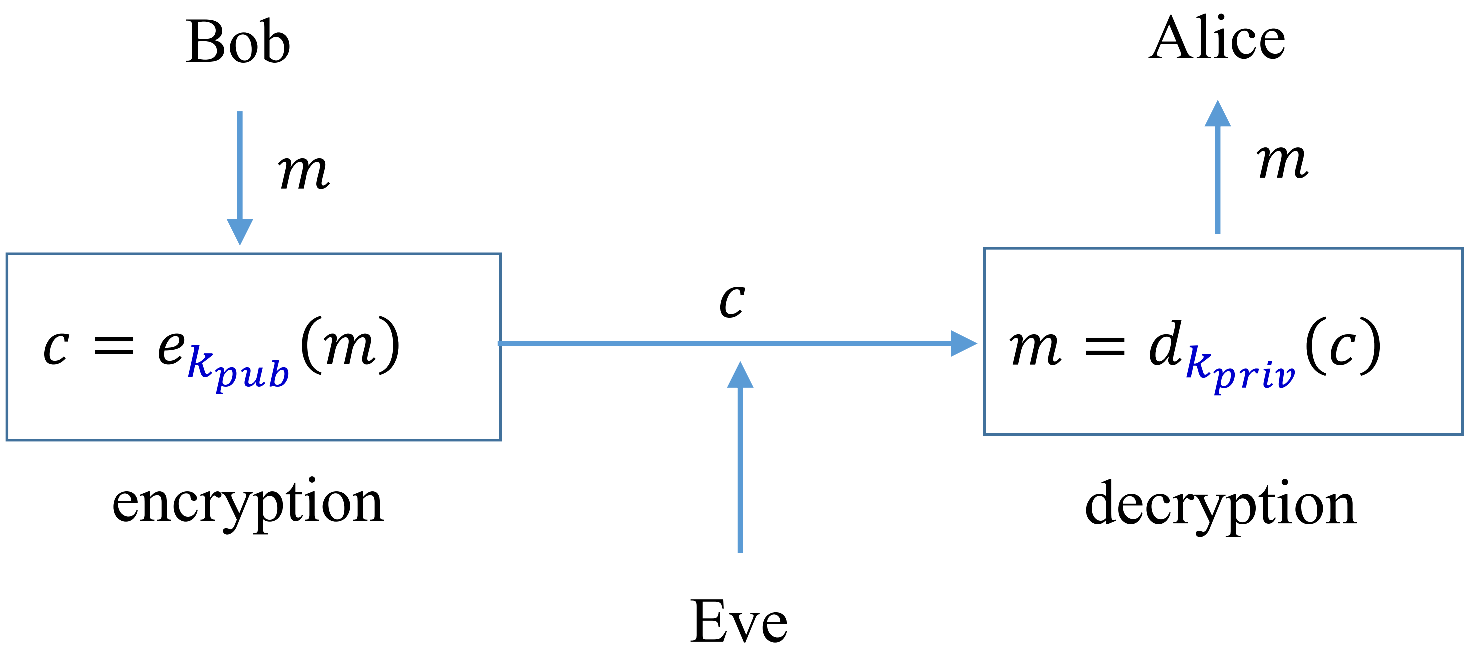
Public Key Cryptography

Anyone can send a secret (encrypted) message to the receiver, without any prior contact, using publicly available info.

Public Key Cryptography

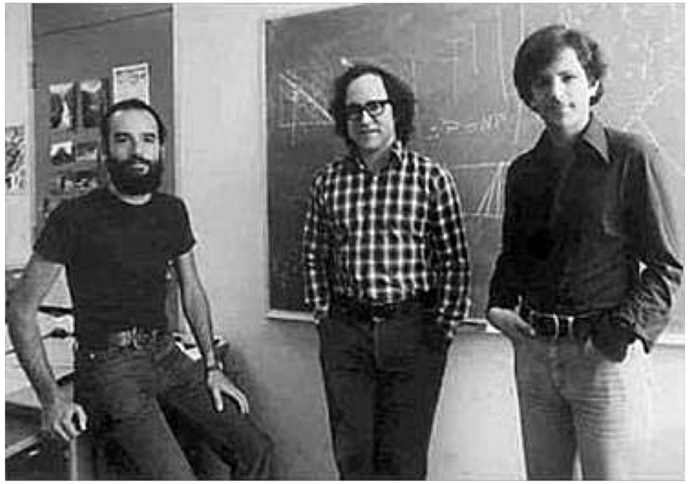
- Invented by Diffie & Hellman in 1976
  - They shared the 2015 Turing Award
- Why Public Key Cryptography?
  - Key distribution
  - Digital signature

Public Key Cryptography



- Alice has a key pair $k = (k_{pub}, k_{priv})$, Bob only knows k_{pub}
- Need to make sure $m = d_{k_{priv}}(e_{k_{pub}}(m))$

The RSA Cryptosystem



- One of the first practical public key cryptosystems
- Invented by Ronald Rivest, Adi Shamir, and Lenoard Adleman in 1976
  - They shared the 2002 Turing Award
- Based on the difficulty of factoring large numbers into primes

The RSA Cryptosystem

Message Encoding:

1. Each letter is encoded into a two-digit number

A	B	C	… I	J	K	L …	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	… 08	09	10	11 …	14	15	16	17	18	19	20	21	22	23	24	25

2. A message is divided into N letter blocks such that the maximum $2N$ digits does not exceed n

Ex: $n = 2537$, a message is divided into 2 letter blocks (2525 < 2537<252525)

- Message STOP is translated into two blocks 1819 1415

Plain and cipher texts are numbers in $\mathbb{Z}_n = \{0,1, \dots, n-1\}$.

The RSA Cryptosystem

Key generation (by Alice):

1. Select two large primes $p, q,\ p \neq q$
2. $n = p \cdot q$
3. Select a small odd integer e that is relatively prime to $(p-1)(q-1)$
4. Compute d such that $de \equiv 1 \pmod{(p-1)(q-1)}$
5. $k_{pub} = (n, e)$ is the public key
6. $k_{priv} = (n, d)$ is the private key

Ex: $p = 43\ \ q = 59\quad n = p \cdot q = 2537\quad e = 13\quad d = 361$

$k_{pub} = (2537, 13),\ k_{priv} = (2537, 361)$

RSA Encryption and Decryption

To encrypt a plaintext m use the public key (n, e)

$$c = m^e \bmod n$$

To decrypt a ciphertext c use the private key (n, d)

$$m = c^d \bmod n$$

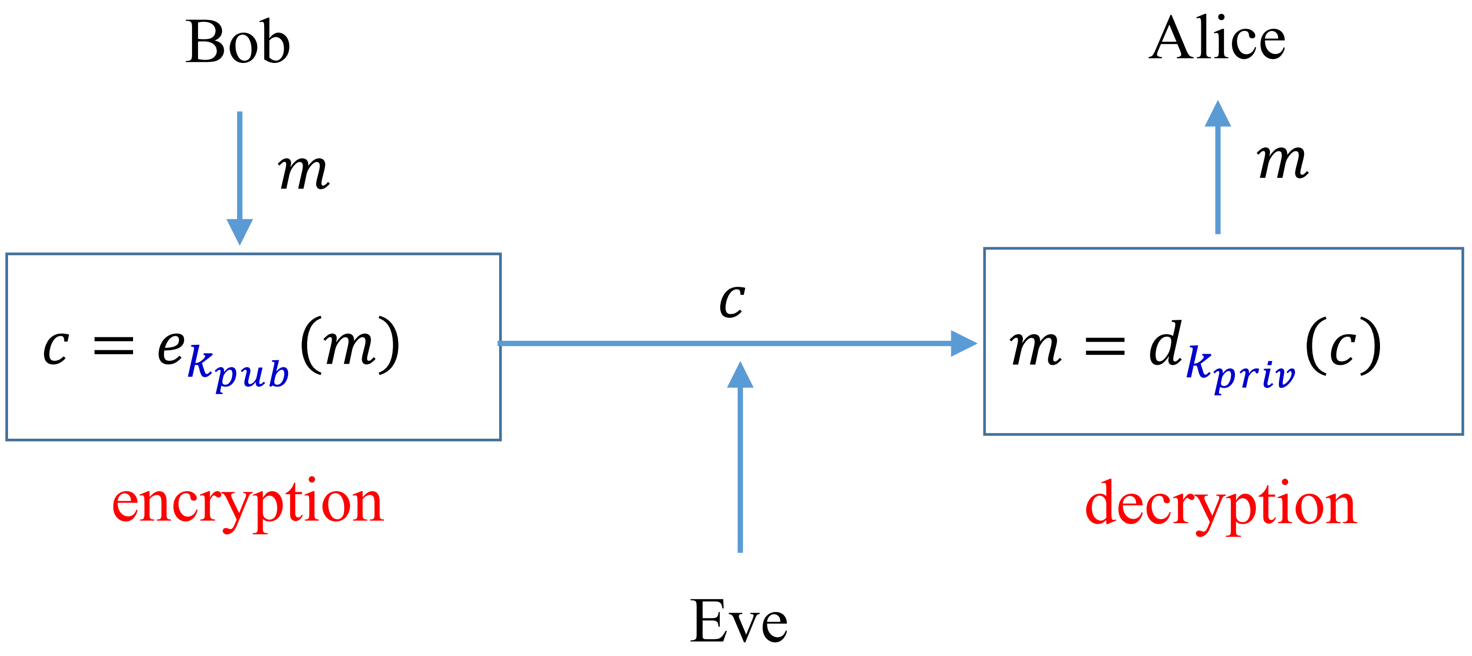
Ex: Encrypt the message STOP with the public key $(2537, 13)$

- Message STOP is translated into two blocks $1819 \;\; 1415$
- Compute $1819^{13} \bmod 2537$, $1415^{13} \bmod 2537$ using fast modular exponentiation

Do we have $m = d_k(e_k(m))$? Need to show $(m^e)^d \equiv m \pmod{pq}$ (Section 4.6)

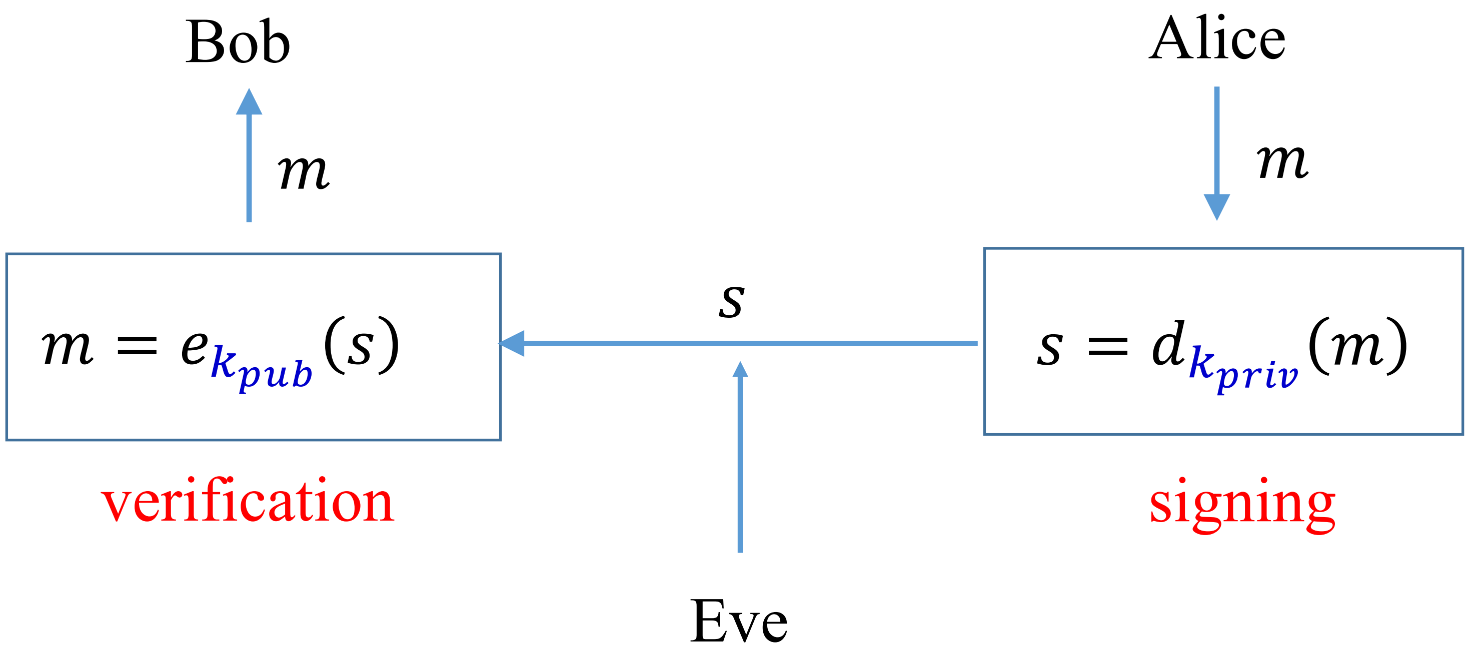
Security of RSA: It is hard to guess d given (n, e) (hard to factor $n = pq$ for large p and q)

Public Key Cryptography



- Alice has a key pair $k = (k_{pub}, k_{priv})$, Bob only knows k_{pub}
- Need to make sure $m = d_{k_{priv}}(e_{k_{pub}}(m))$

Digital Signature



- Alice has a key pair $k = (k_{pub}, k_{priv})$
- Need to make sure $m = e_{k_{pub}}(d_{k_{priv}}(m))$