Lecture 9: Cryptography

Table of contents

Euclidean algorithms

Assume $r_0 = a$ and $r_1 = b$ with $r_0 \geq r_1$.

Euclidean finds $\gcd(a, b)$

- $r_0 = r_1 q_1 + r_2$

  $\vdots$

- $r_{n-2} = r_{n-1} q_{n-1} + r_n$
- $r_{n-1} = r_n q_n + 0$

Conclusion: $\gcd(a, b) = r_n$

Extended Euclidean: $as + bt = \gcd(a, b)$

Notation: * = some number

- $r_n = r_{n-2} + r_{n-1} *$
- Use prev. equation to find r_{n-1}

$$\begin{aligned} r_n &= r_{n-2} + (r_{n-3} * + r_{n-2} *)(-q_{n-1}) \\ r_n &= r_{n-3} * + r_{n-2} * \end{aligned}$$

- Keep doing this till first equation

$$r_n = r_0 s + r_1 t$$

Modular inverses

$a^{-1} \mod m =$ an integer b with $ab \equiv 1 \pmod{m}$. Note that

$$a^{-1} \mod m \text{ exists} \Leftrightarrow \gcd(a, m) = 1$$

To find $a^{-1} \mod m$, we do the following steps

Modular inverses

$a^{-1} \mod m =$ an integer b with $ab \equiv 1 \pmod{m}$. Note that

$$a^{-1} \mod m \text{ exists} \Leftrightarrow \gcd(a, m) = 1$$

To find $a^{-1} \mod m$, we do the following steps

1. Compute $\gcd(a, m)$.
   If $\gcd(a, m) > 1$, $a^{-1} \mod m$ doesn't exist.
   If $\gcd(a, m) = 1$, proceed to the next step.

Modular inverses

$a^{-1} \mod m =$ an integer b with $ab \equiv 1 \pmod m$. Note that

$$a^{-1} \mod m \text{ exists} \Leftrightarrow \gcd(a, m) = 1$$

To find $a^{-1} \mod m$, we do the following steps

1. Compute $\gcd(a, m)$.
   If $\gcd(a, m) > 1$, $a^{-1} \mod m$ doesn't exist.
   If $\gcd(a, m) = 1$, proceed to the next step.
2. Find Bezout coefficients s and t of a and m:

$$as + mt = \gcd(a, m) = 1.$$

Conclusion:

$$a^{-1} \mod m = s.$$

Convert negative to positive in congruence

- In finding $s = a^{-1} \mod m$ by Bezout coefficient, s might be negative. To convert s to positive, we add a suitable multiple of m.
- Examples

Convert negative to positive in congruence

- In finding $s = a^{-1} \mod m$ by Bezout coefficient, s might be negative. To convert s to positive, we add a suitable multiple of m.
- Examples

  Since $3 \cdot (-3) + 2 \cdot 5 = 1$,

$$3^{-1} \mod 5 = (-3) \mod 5 = 2$$

  Since $5 \cdot (-7) + 9 \times 4 = 1$,

$$5^{-1} \mod 9 = (-7) \mod 9 = 2$$

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

1. Find $d = \gcd(a, m)$ (by factorizing a and m)
   - If $d \nmid b$, the equation has no solution.
   - If $d \mid b$, proceed to the next step.
2. Write $a = da_1, b = db_1, m = dm_1$.
   Dividing all terms of $ax \equiv b \pmod{m}$ by d, we obtain

$$a_1 x \equiv b_1 \pmod{m_1} \tag{1}$$

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

1. Find $d = \gcd(a, m)$ (by factorizing a and m)
   - If $d \nmid b$, the equation has no solution.
   - If $d \mid b$, proceed to the next step.
2. Write $a = da_1, b = db_1, m = dm_1$.
   Dividing all terms of $ax \equiv b \pmod{m}$ by d, we obtain
   $$a_1 x \equiv b_1 \pmod{m_1} \tag{1}$$
3. Multiplying both sides of (1) by $a_2 = a_1^{-1} \mod m_1$, we obtain
   $$x \equiv b_1 a_2 \pmod{m_1}.$$

Exercise 1

Let a, b, m be integers with $\gcd(a, m) \nmid b$. Prove that the equation

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

has no solution.

Exercise 2

Consider integers $a = 252$ and $m = 356$.

(a) Let s, t be Bezout coefficients of a, m. What is s?

(A) -24 (B) 332 (C) -380 (D) Any A,B,C (E) None of A,B,C

(b) For what $b \in \mathbb{Z}$ does equation $252x \equiv b \pmod{356}$ have solution?

(c) Solve $252x \equiv 12 \pmod{356}$?

(d) How many $x \in \{0, 1, \ldots, 355\}$ satisfies $252x \equiv 12 \pmod{356}$?

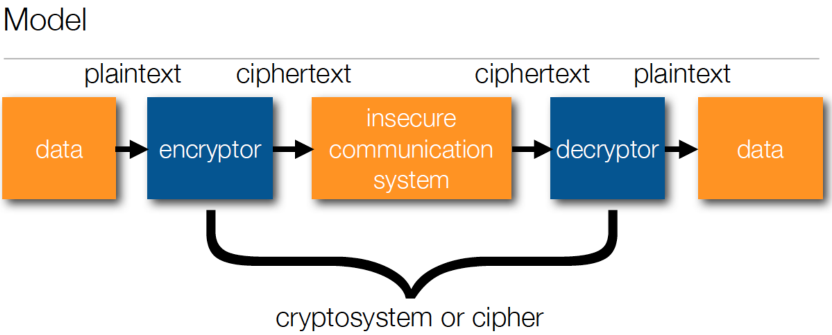
What is cryptography?

- The subject of transforming information so that it cannot be easily recovered without special knowledge
- Cryptography is a branch in **cryptology** which comprises of
  1. **Cryptography** - How to design methods to hide information.
  2. **Cryptanalysis** - How to break methods that hide information.

Applications of cryptography

- Secrecy in communications: Military, spies, diplomats, banking (ATM cards, credit cards, PayPal)
- Integrity protection (ability to detect change in messages): Electronic form submission.

Cryptography model



Conventional notations

- The plaintext is denoted by P
- The ciphertext is denoted by C
- **Encryption**

  The sender encrypts $P \to C$ and send C over the insecure channel.

Conventional notations

- The plaintext is denoted by P
- The ciphertext is denoted by C
- **Encryption**

  The sender encrypts $P \to C$ and send C over the insecure channel.
- **Decryption**

  Upon receiving C, the receiver decrypts $C \to P$ to retrieve the information.

Caesar cipher: Encryption

1. Identify each letter with an integer between 0 and 25. Write out the plaintext P after this identification.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Caesar cipher: Encryption

1. Identify each letter with an integer between 0 and 25.
   Write out the plaintext P after this identification.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2. Fix a key $k \in \mathbb{Z}_{26} = \{0, 1, \dots, 25\}$ (**kept secret**)

Caesar cipher: Encryption

1. Identify each letter with an integer between 0 and 25.
   Write out the plaintext P after this identification.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2. Fix a key $k \in \mathbb{Z}_{26} = \{0, 1, \ldots, 25\}$ (**kept secret**)
3. The plaintext P is encrypted to a cipher text C by

$$C = P + k \mod 26.$$

Convert C back to a string of letters.

Caesar cipher: Decryption

- Since $C = P + k \mod 26$, we have

$$P = C - k \mod 26.$$

Example 1

Encrypt the following text using Caesar cipher with the key $k = 11$.

WEWILLMEETATMIDNIGHT.

Example 1 solution

- Convert the plaintext into integers between 0 and 25.

W	E	W	I	L	L	M	E	E	T	A	T	M	I	D	N	I	G	H	T
22	4	22	8	11	11	12	4	4	19	0	19	12	8	3	13	8	6	7	19

$P = (22, 4, 22, 8, 11, 11, 12, 4, 4, 19, 0, 19, 12, 8, 3, 13, 8, 6, 7, 19)$

Example 1 solution

- Add each integer by 11 and compute the result modulo 26.

22	4	22	8	11	11	12	4	4	19	0	19	12	8	3	13	8	6	7	19
7	15	7	19	22	22	23	15	15	4	11	4	23	19	14	24	19	17	18	4

$$C = P + 11 \mod 26 = (7, 15, 7, 19, 22, 22, 23, 5, 15, 4, 11, \ldots)$$

Example 1 solution

Convert the integers back to letters

7	15	7	19	22	22	23	15	15	4	11	4	23	19	14	24	19	17	18	4
H	P	H	T	W	W	X	P	P	E	L	E	X	T	O	Y	T	R	S	E

HPHTWWXPPELEXTOYTRSE

Summary on Caesar cipher

Encryption: $\mathbf{P} \to \mathbf{C}$

1. Identify each letter with an integer between 0 and 25.
   Write out the plaintext P after this identification.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2. Fix a key $k \in \mathbb{Z}_{26} = \{0, 1, \ldots, 25\}$.
3. The plaintext P is encrypted to a cipher text C by

$$C = P + k \mod 26.$$

Decryption: $\mathbf{C} \to \mathbf{P}$

$$P = C - k \mod 26.$$

Exercise 3

Using the Caesar cipher with the key $k = 6$, **encrypt** the plaintext

SITISGREAT

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Exercise 4

Decrypt the ciphertext ZNK KGXRE HOXJ MKZY ZNK CUXS using Caesar cipher with the key $k = 6$.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

How to break Caesar cipher?

The Caesar cipher is easy to break, as the key space is small.

1. There are 26 possible values $0, 1, \ldots, 25$ for the key k.
2. Try all possible values.

Affine cipher: Encryption

1. Identify each letter with an integer between 0 and 25. Write out the plaintext P after this identification.

Affine cipher: Encryption

1. Identify each letter with an integer between 0 and 25. Write out the plaintext P after this identification.
2. Choose $a, b \in \mathbb{Z}_{26}$ such that $\gcd(a, 26) = 1$.

$$a \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

Affine cipher: Encryption

1. Identify each letter with an integer between 0 and 25. Write out the plaintext P after this identification.
2. Choose $a, b \in \mathbb{Z}_{26}$ such that $\gcd(a, 26) = 1$.

$$a \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

3. The plaintext P is encrypted to a ciphertext C by

$$C = aP + b \mod 26.$$

Affine cipher: Decryption

- Decryption: Since $C = aP + b \mod 26$, we have
$$P = a^{-1}(C - b) \mod 26.$$
- **Remark.** $a^{-1} \mod 26$ exists because $\gcd(a, 26) = 1$.

Remarks on affine cipher

- When $a = 1$, the affine cipher becomes Caesar cipher.

Remarks on affine cipher

- When $a = 1$, the affine cipher becomes Caesar cipher.
- The key space for affine cipher is

$$K = \{(a, b) : a, b \in \mathbb{Z}_{26}, \gcd(a, 26) = 1\}.$$

Key space of affine cipher

$$K = \{(a, b) : a, b \in \mathbb{Z}_{26}, \gcd(a, 26) = 1\}.$$

Key space of affine cipher

$$K = \{(a, b) : a, b \in \mathbb{Z}_{26}, \gcd(a, 26) = 1\}.$$

- There are 12 choices for a

$$a \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

- There are 26 choices for b

$$b \in \{0, 1, \ldots, 25\}$$

Key space of affine cipher

$$K = \{(a, b) : a, b \in \mathbb{Z}_{26}, \gcd(a, 26) = 1\}.$$

- There are 12 choices for a

$$a \in \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

- There are 26 choices for b

$$b \in \{0, 1, \ldots, 25\}$$

- The key space is $|K| = 12 \cdot 26 = 312$.

Example 2

Encrypt the plaintext SITISTHEBEST using affine cipher with the key $(a, b) = (3, 13)$.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Summary on affine cipher

Encryption: $\mathbf{P} \to \mathbf{C}$

1. Identify each letter with an integer between 0 and 25. Write out the plaintext P after this identification.
2. Choose a key $k = (a, b)$ with $a \in \mathbb{Z}_{26}^{*}, b \in \mathbb{Z}_{26}$.
3. The plaintext P is encrypted to a cipher text C by

$$C = aP + b \mod 26.$$

Decryption: $\mathbf{C} \to \mathbf{P}$

$$P = a^{-1}(C - b) \mod 26.$$

Exercise 5

In this exercise, we decrypt the ciphertext AXG using affine cipher with key $(a, b) = (7, 3)$

(a) Write out the formula which gives **decryption rule** for affine cipher with the key $(a, b) = (7, 3)$.

Exercise 5

(b) Find $7^{-1} \mod 26$ and decrypt AXG using affine cipher with key $(a, b) = (7, 3)$.