Fubswrjudskb

Frxuvh qxpehu: 4003-482
Lqvwuxfwr: Lyrqd Ehcdnryd

Wrgdb’v Wrslfv:

1. Orjlvwlfv:
   - Fodvv olvw
   - Vboodexv

2. Wkh Pdwk

3. Zkdw lv Fubswrjudskb

4. Vrph Fodvvlfdo Fubswrvbvwhpv
Today's topics:

1. Logistics:
   - Class list
   - Syllabus

2. The Math

3. What is Cryptography

4. Some Classical Cryptosystems
We will go beyond descriptions of cryptographic algorithms and ways how to break them.

We will use a lot of math and CS theory in this course, including:

- some abstract algebra (number theory, groups, rings, fields)
- some linear algebra
- some probability and information theory
- some complexity theory

It is important to be comfortable with math!
What is Cryptography

- the study of secure communication over insecure channels.

Typical scenario:
What is Cryptography

Private-key cryptosystems: Chapter 2 (& 4)
- Alice and Bob agree on a key beforehand

Alice: plaintext -> encryption (via the key) -> ciphertext -> send to Bob
Bob: decrypt the ciphertext (using the key) to reconstruct the plaintext
What is Cryptography

Eve:
- she does not know the key, she cannot decrypt... ???
- she tries to read the current message, she can also try to figure out the key
- in our book she sometimes acts as a malicious active attacker (usually called Mallory): corrupting Alice’s message, or masquerading as Alice

Symmetric-key cryptosystems:
- private-key cryptosystems use (essentially) the same key for encryption and decryption
Some Cryptanalysis Terminology

Cryptanalysis
- the process of attempting to compute the key
- the most common attack models:
  - ciphertext only attack
  - known plaintext attack: both plaintext and ciphertext
  - chosen plaintext attack: you choose a plaintext and get it encrypted
  - chosen ciphertext attack: you choose a ciphertext and get it decrypted

What’s the weakest type of attack? ciphertext only
Cryptographic Applications

1. Confidentiality
2. Data integrity
3. Authentication
4. Non-repudiation
Conventions:
- plaintext: lowercase
- CIPHERTEXT: uppercase
- Spaces and punctuations will be usually omitted.
- Letters of the alphabet will be often identified with numbers $0, 1, \ldots, 25$. 
Monoalphabetic Ciphers

- Each letter is mapped to a unique letter.
- Examples: shift cipher, substitution cipher, affine cipher

- We will need modular arithmetic (and we’ll introduce more than we need in this chapter - it will all be useful later).
Modular Arithmetic

Let $a, b$ be integers, $m$ be a positive integer.

We write:

$$a \equiv b \pmod{m} \text{ if } m \text{ divides } (a-b)$$

(Read it as: “$a$ is congruent to $b$ mod $m$”.)

Examples: (true/false)

- $7 \equiv 5 \pmod{3}$ \(\checkmark\)
- $7 \equiv 1 \pmod{3}$ \(\checkmark\)
- $66 \equiv 0 \pmod{3}$ \(\checkmark\)
- $4 \equiv 1 \pmod{3}$ \(\checkmark\)
- $-4 \equiv -1 \pmod{3}$ \(\checkmark\)
- $-8 \equiv 7 \pmod{3}$ \(\checkmark\)
Modular Arithmetic

Let $a$ be an integer, $m$ be a positive integer. We use:

$$a \mod m$$

to denote the remainder when $a$ is divided by $m$. The remainder is always a number from $\{0,1,2,\ldots,m-1\}$.

Examples:

- $8 \mod 3 = 2$
- $1 \mod 1 = 0$
- $0 \mod 2 = 0$
- $63 \mod 7 = 0$
- $-8 \mod 3 = 1$
- $3 \mod 6 = 3$
- $-63 \mod 7 = 0$

Is $\%$ in Java/C/C++ the same as $\mod$? almost except negatives
Modular Arithmetic

$\mathbb{Z}_m$ denotes the set \{0, 1, 2, ..., m-1\}, with two operations:

- **addition** (modulo m)
- **multiplication** (modulo m)

$\mathbb{Z}_m$ is a **commutative ring**, i.e.:

- addition and multiplication (mod m) are closed, commutative, associative, and multiplication is distributive over addition

\[(a+b)+c = a+(b+c)\]
\[(ab)c = a(bc)\]
\[a \times (b+c) = a \times b + a \times c\]

- 0 is the additive identity
  \[a+0 = a\]

- each element has an additive inverse
  \[\text{For every } a, \exists b : a+b = 0\]

**Note:** For $m>1$, $\mathbb{Z}_m$ is a commutative ring with identity.
Shift Cipher

The key $k$ is an element of $\mathbb{Z}_{26}$.

We encrypt a letter $x \in \mathbb{Z}_{26}$ as follows:

$$x \rightarrow (x+k) \mod 26$$

How to decrypt?

$$x \rightarrow (x-k) \mod 26$$

Remarks:

- For $k=3$ this is known as the Caesar cipher, attributed to Julius Caesar.

- Shift cipher works over any $\mathbb{Z}_m$. 
Shift Cipher

How good is it?
- the good: efficient encryption/decryption computation
- the bad: easy to attack (not very secure)
- how?
  - brute force if ciphertext only (26 possibilities)
  - if known plaintext: need a single symbol, then do the math

Kerckhoff’s Principle:
- Eve knows the cipher but does not know the key.
- Always assumed in cryptanalysis.
Substitution Cipher

- Monoalphabetic cipher defined by a permutation of the alphabet.

- Example:

abcdefgijklmnopqrstuvwxyz
ONETWHRFUISINGABCJKLMQPQYZ

What is the key in this example?

- Exercise:

decrypt: EDYBKARDOBFY
crypto...y
Substitution Cipher

How good is it?
- the good: efficient encryption/decryption
- the bad(?): is it secure?
  - approach 1: try all possible keys
    - is this feasible?
      NO, too many possibilities

26! keys
Substitution Cipher

How good is it?
- the good: efficient encryption/decryption
- the bad(?): is it secure?
  - approach 1: try all possible keys
    - is this feasible?

  approach 2: frequency analysis (possibly incl. digrams, trigrams)

Hint: frequency tables, e.g., for English see Table 2.1, page 17
Affine Ciphers

The key is a pair \((\alpha, \beta) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}\) such that \(\gcd(\alpha, 26) = 1\).

Then, encryption is done via an affine function:

\[ x \rightarrow (\alpha x + \beta) \mod 26 \]

How to decrypt?

\[ x \rightarrow (x - \beta) \cdot \alpha^{-1} \]

Subtraction is OK because we have additive inverses.

Example:

\[ \begin{align*}
\alpha &= 5 \\
\beta &= 2
\end{align*} \]

\[ \begin{align*}
\alpha &\rightarrow C \\
\beta &\rightarrow H
\end{align*} \]

(0\rightarrow z) (1\rightarrow ?)

Remark: The affine cipher can be defined over any \(\mathbb{Z}_m\).
Affine Ciphers

Questions:
- How does it relate to the shift and the substitution ciphers?
  - shift is a special case, take $\alpha = 1$
  - affine cipher is a special case of substitution cipher
- How many possible keys are there?
  - $\alpha$: 12 possibilities
  - $\beta$: 26 possibilities
  - together: #keys: 12 * 26
- Why do we have the condition $\gcd(\alpha, 26) = 1$?
  - to have $\alpha^{-1}$
- What is $\alpha^{-1}$?
Affine Ciphers

Questions:
- Efficiently computable encryption and decryption?
  - Yes, multiplication takes $O(n \log n)$ for two numbers of $n$ digits.
  - Addition: $O(n)$.
  - Computing $a^{-1}$: fast, we'll see.
- Is it secure? How to cryptanalyze?
  - All substitution cipher attacks apply.
  - Example:
    - $0 \rightarrow 2, 0 \cdot a + \beta = 2$
    - $1 \rightarrow 7, 1 \cdot a + \beta = 7$
    - $\Rightarrow \beta = 2, a = 5$
  - Encryption:
    - $X_i \rightarrow y_i, X_i \cdot a + \beta = y_i$
    - $X_2 \rightarrow y_2, X_2 \cdot a + \beta = y_2$
    - $(X_i - X_2) \cdot a = y_i - y_2$
    - $a = (y_i - y_2) \cdot (X_i - X_2)^{-1}$
    - Then $\beta = y_i - X_i \cdot a$.