CSC316: Cryptography

Unit I – Introduction and Classical Ciphers

Prepared by Er. Arjun Neupane

Contents

1 Overview of Unit I

This unit introduces the basic language of security and cryptography and then studies classical cipher techniques. It follows the BSc. CSIT syllabus and the structure of standard textbooks such as *Cryptography and Network Security* by William Stallings.

The main learning outcomes are:

- understand computer, information and network security and the CIA triad;
- define cryptography, cryptosystem and cryptanalysis;
- explain security threats, types of attacks and basic security services;
- describe classical cryptosystems (Caesar, Hill, Vigenère, Vernam, one-time pad, Playfair, Rail fence);
- differentiate between block vs stream ciphers and symmetric vs asymmetric ciphers.

2 Security: Basic Concepts

2.1 Assets, Vulnerabilities, Threats and Attacks

Asset: Anything of value that must be protected, e.g. computers, networks, data, software, services or even people.

Vulnerability: A weakness in a system that can be exploited. Examples: weak passwords, unpatched software, open ports, careless users.

Threat: A potential cause of an unwanted incident that may harm a system or organisation. Example: a hacker, malware, insider misuse, power failure.

Attack: Any action that attempts to violate security by exploiting a vulnerability. Example: password guessing, SQL injection, DoS flooding.

Security aims to minimise vulnerabilities, understand threats, and design defences so that attacks either fail or are detected and recovered from.

2.2 Computer Security, Information Security, Network Security

2.2.1 Computer Security

Computer security focuses on protecting individual computer systems and their resources.

- Protects hardware, operating system, applications and local data.

- Typical controls: user authentication (passwords, biometrics), local access control, antivirus, host-based firewall, OS patches.
- Example: locking a workstation, enabling full-disk encryption on a laptop so that a thief cannot read the data.

2.2.2 Information Security

Information security (InfoSec) protects *information*, regardless of the format or location.

- Information may be stored on paper, disks, USB drives, databases or in the cloud.
- InfoSec includes technical controls, policies, procedures and legal measures.
- Example: an institute's policy that students' marks and medical information are confidential and may only be accessed by authorised staff.

2.2.3 Network Security

Network security protects data as it travels over communication networks (LANs, WANs, wireless or the Internet).

- Prevents eavesdropping, modification, or injection of packets.
- Uses firewalls, virtual private networks (VPN), secure protocols such as HTTPS, SSH, IPsec, and Wi-Fi security (WPA2/WPA3).
- Example: when a browser connects to a bank via HTTPS, network security ensures confidentiality and integrity of the login data.

These three areas overlap. In practice we simply say *security* and understand that it includes computer, information and network aspects.

2.3 CIA Triad: Confidentiality, Integrity, Availability

Security objectives are usually summarised by the **CIA triad**:

a) **Confidentiality:** Only authorised entities should be able to access information.

b) **Integrity:** Information and systems must not be altered in an unauthorised or undetected manner.

c) **Availability:** Systems and data should be accessible to authorised users whenever required.

2.3.1 Confidentiality

Confidentiality protects against *disclosure* of information.

- Achieved by encryption, access control, classification of documents, secure storage.
- Example: credit-card numbers stored in a database must be encrypted so that a database administrator cannot read them directly.

2.3.2 Integrity

Integrity has two related aspects:

- **Data integrity:** data should be changed only in a specified and authorised way.
- **System integrity:** a system should perform its intended functions, free from unauthorised manipulation (such as rootkits).

Mechanisms: checksums, cryptographic hash functions, message authentication codes (MACs), digital signatures, version control and backups.

2.3.3 Availability

Availability means that authorised users have timely and reliable access to data and services.

- Measured in terms of uptime, response time, and ability to handle load.
- Threatened mainly by hardware failures, natural disasters and deliberate Denial-of-Service (DoS) attacks.

2.3.4 CIA as a Triangle

A good security design balances all three objectives. For example, extremely strict access control may improve confidentiality but reduce availability because legitimate users cannot get their work done.

3 Cryptography, Cryptosystem and Cryptanalysis

3.1 Cryptography

The word *cryptography* comes from Greek "kryptos" (hidden) and "graphien" (writing). Cryptography is the study of mathematical techniques for achieving information security.

Major goals supported by cryptography:

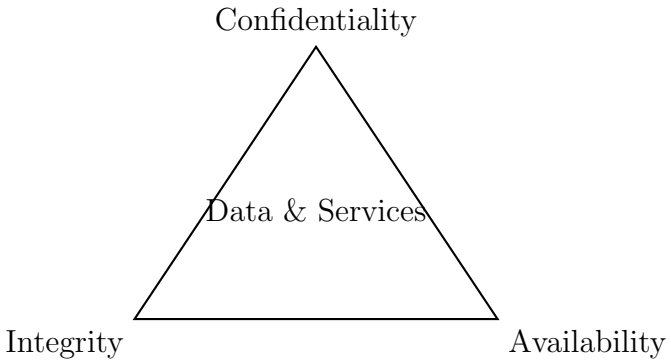

Figure 1: CIA security triad

- confidentiality of data;
- integrity and authentication of messages;
- nonrepudiation (proof that someone performed an action);
- sometimes, anonymity and privacy.

3.2 Encryption and Decryption

Encryption is the process of converting *plaintext* (original readable data) into *ciphertext* (unreadable form) using an algorithm and a secret value called a *key*.

Decryption is the reverse process: converting ciphertext back to plaintext using a key.

Figure 2: Basic encryption–decryption model

Simple illustration (Caesar cipher with shift $k = 3$):

- plaintext: `MEET`;
- ciphertext: `PHHW`.

3.3 Formal Model of a Cryptosystem

A (symmetric) **cryptosystem** can be described mathematically as a 5-tuple

$$(P, C, K, E, D),$$

where

- P is the set of possible plaintexts;
- C is the set of possible ciphertexts;
- K is the key space (set of possible keys);
- for each $k \in K$, $E_k : P \to C$ is the encryption function;
- for each $k \in K$, $D_k : C \to P$ is the decryption function.

For all $p \in P$ and key k,

$$D_k(E_k(p)) = p.$$

3.4 Keys and Key Space

A **key** is a parameter that selects one specific transformation from the many possible encryptions of a cipher.

- In Caesar cipher, the key is the shift value k (0–25).
- In DES, the key is a 56-bit number.
- In modern systems, keys are randomly generated to make brute-force search infeasible.

The security of a cryptosystem should depend on the secrecy of the key, not on the secrecy of the algorithm (Kerckhoffs's principle).

3.5 Cryptanalysis and Cryptanalyst

Cryptanalysis is the science of analysing and breaking ciphers. A **cryptanalyst** studies algorithms, ciphertexts and protocols to find weaknesses and to recover the plaintext or keys without knowing the secret key.

Types of cryptanalytic attacks include:

- **Ciphertext-only attack:** attacker has only ciphertexts.
- **Known-plaintext attack:** attacker knows pairs of plaintext and corresponding ciphertext.
- **Chosen-plaintext / chosen-ciphertext attack:** attacker can obtain ciphertext for chosen plaintexts (or vice versa).
- **Brute-force attack:** try all possible keys until the correct one is found.

The aim of cryptography is to design systems where every practical attack is computationally infeasible.

4 Security Threats, Attacks and Services

4.1 Security Threats

A **security threat** is a potential violation of security that can cause harm such as disclosure of information, loss of integrity or loss of availability.

Threats can be broadly classified into four categories:

i) **Disclosure:** unauthorised access to information (e.g. eavesdropping, reading someone else's e-mail).

ii) **Deception:** acceptance of false data (e.g. spoofed e-mail, fake websites).

iii) **Disruption:** interruption or degradation of correct operation (e.g. deleting files, DoS attacks).

iv) **Usurpation:** unauthorised control of a system (e.g. installing a rootkit, hijacking a session).

4.2 Types of Attacks: Passive vs Active

4.2.1 Passive Attacks

In a **passive attack**, the attacker only observes the data being transmitted or stored, but does not modify it. The goal is to obtain information.

Two important passive attacks in the CSIT syllabus are:

Release of Message Contents

- Attacker simply reads the content of messages.
- Example: an attacker sniffing plaintext passwords sent over an unencrypted HTTP connection or reading unencrypted Wi-Fi traffic.
- Defence: encryption (e.g. HTTPS, VPN), secure protocols.

Traffic Analysis Even if messages are encrypted, the attacker can still analyse the *patterns* of communication:

- who is communicating with whom,
- frequency and timing of messages,

- size of messages.

Example: From a hospital's encrypted traffic, an attacker might observe that a particular doctor suddenly communicates frequently with an oncology specialist, revealing something about a patient's condition.

Defence: traffic padding, mixing, tunnelling, hiding metadata.

Passive attacks are difficult to detect because they do not involve changes to the data; prevention is therefore more important than detection.

4.2.2 Active Attacks

In an **active attack**, the attacker changes data, injects messages or disrupts the service. These attacks threaten integrity and availability.

Important types:

Replay Attack

- The attacker records a valid message and later replays it.
- Example: recording an authenticated bank transfer request and sending it again to perform an unauthorised second transfer.
- Defence: use of nonces, timestamps, sequence numbers and strong authentication.

Denial-of-Service (DoS) Attack

- The attacker makes a resource (server, network, application) unavailable to legitimate users.
- Methods: flooding with huge number of requests, exploiting protocol weaknesses (SYN flood), or crashing the server with malformed input.
- Distributed DoS (DDoS) uses many compromised machines (botnet).

Other typical active attacks (useful to mention in class):

- **Masquerade:** one entity pretends to be another (identity theft).
- **Modification of messages:** changing fields in a message (e.g. altering the amount in a transaction).

4.3 Security Services

4.3.1 Authentication

Authentication verifies the identity of an entity or the origin of data.

- **Peer-entity authentication:** ensures that the communicating entity (user, computer, process) is the one claimed.
- **Data-origin authentication:** ensures that a received message was actually sent by the claimed sender and not modified.

Methods: passwords, biometrics, challenge–response protocols, MACs and digital signatures.

4.3.2 Access Control

Access control determines who is allowed to access which resources and in which way (read, write, execute, delete).

- Based on authentication and authorisation rules.
- Implemented using access control lists (ACLs), role-based access control (RBAC), firewalls, and application-level checks.

4.3.3 Nonrepudiation

Nonrepudiation prevents a sender or receiver from denying a previously performed action.

- A sender should not be able to deny having sent a message.
- A receiver should not be able to deny having received it.
- Digital signatures and secure logging provide nonrepudiation.

4.3.4 Other Common Services (for completeness)

- **Data confidentiality:** protection from unauthorised disclosure (encryption).
- **Data integrity:** protection from unauthorised modification (hash functions, MAC).
- **Availability:** ensuring services remain accessible.

4.4 Security Mechanisms, Policy and Mechanism

4.4.1 Security Mechanisms

A **security mechanism** is a specific method, tool or procedure used to achieve a security service. Examples:

- encryption algorithms (AES, DES, RSA);
- hash functions and MACs;
- digital signatures;
- authentication protocols;
- firewalls, intrusion detection systems, antivirus.

4.4.2 Security Policy

A **security policy** is a high-level statement of what is allowed and what is prohibited in an organisation.

- Example: "Only system administrators may access the server room."
- Example: "Students may read their own grade reports but cannot modify them."

4.4.3 Relationship Between Policy and Mechanism

- Policy answers *what* must be protected and *which* actions are allowed.
- Mechanism answers *how* to enforce that policy technically.

For example, if policy says that exam files are confidential, encryption, access control on the file server and logging are the mechanisms that enforce this policy.

5 Classical Cryptosystems

Classical cryptosystems were used before the development of modern computers. They operate mostly on letters rather than bits. They are not secure today but are excellent for teaching the principles of cryptography and cryptanalysis.

5.1 Hierarchy of Ciphers

The CSIT syllabus classifies ciphers as follows:

1. **By operation:**
   - **Substitution ciphers:** characters (or groups of characters) are replaced by other characters;
   - **Transposition ciphers:** character positions are permuted.
2. **By number of alphabets used (for substitution):**
   - **Monoalphabetic:** one fixed substitution alphabet (Caesar, general substitution, Hill);
   - **Polyalphabetic:** multiple alphabets (Vigenère, Vernam, one-time pad, Playfair).

   We study substitution techniques first and then transposition.

5.2 Substitution Techniques

5.2.1 Monoalphabetic Substitution Ciphers

In a monoalphabetic substitution cipher each plaintext letter maps to exactly one ciphertext letter, and this mapping is fixed throughout the message.

General Properties

- There are 26! possible substitution alphabets for English letters.
- However, letter frequency is preserved; e.g. "E" is still the most common letter. This allows frequency-analysis attacks.

  Below we detail two monoalphabetic ciphers required by the syllabus.

5.2.2 Caesar Cipher

The Caesar cipher shifts each letter by a fixed number k positions in the alphabet.

Mathematical Description Map letters to numbers: A=0, B=1, ..., Z=25.

$$\text{Encryption:} \quad C = (P + k) \bmod 26$$

$$\text{Decryption:} \quad P = (C - k) \bmod 26$$

where P and C are numerical equivalents of plaintext and ciphertext.

Example Let key $k = 3$.

- Plaintext: `HELLO`.
- H(7)→10(J), E(4)→7(H), L(11)→14(O), O(14)→17(R).
- Ciphertext: `KHOOR`.

Algorithm (Student-friendly Steps)

1. Write alphabet with indexes 0–25.
2. Convert each plaintext letter into its index.
3. Add k to each index and take modulo 26.
4. Convert resulting indexes back to letters.

Security Key space is only 26; a brute-force attacker can try all shifts easily. Therefore Caesar cipher is used only for demonstrations and puzzles.

5.2.3 Hill Cipher

The Hill cipher is a polygraphic substitution cipher using linear algebra. Instead of encrypting one letter at a time, it encrypts blocks of n letters using matrix multiplication modulo 26.

Here we consider the 2–letter (2×2) case.

Key

- Choose a 2×2 invertible matrix

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

  such that $\det(K) = ad - bc$ is relatively prime to 26 (i.e. $\gcd(\det(K), 26) = 1$).

- This ensures that K has an inverse modulo 26.

Encryption

1. Map letters to numbers 0–25.
2. Group plaintext into pairs of letters to form column vectors $P = \begin{bmatrix} p_1 \ p_2 \end{bmatrix}^T$.
3. Compute
$$C = KP \bmod 26.$$
4. Convert numbers in C back to letters to get ciphertext.

Decryption

1. Compute the inverse matrix K^{-1} mod 26.
2. For each ciphertext vector C, compute
$$P = K^{-1}C \bmod 26.$$

Example Let key matrix
$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$
and plaintext "HI".

- H=7, I=8, so $P = \begin{bmatrix} 7 \ 8 \end{bmatrix}^T$.
- Compute $C = KP$ mod 26:
$$C = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 45 \\ 54 \end{bmatrix} \equiv \begin{bmatrix} 19 \\ 2 \end{bmatrix} \pmod{26}.$$
- $19 \to$ T, $2 \to$ C, so ciphertext is "TC".

The Hill cipher hides single-letter frequency but is still breakable using linear algebra and known-plaintext attacks.

5.2.4 Polyalphabetic Substitution: Vigenère Cipher

The Vigenère cipher uses a keyword to select different Caesar shifts at different positions in the message.

Key and Keystream

- Choose a keyword, e.g. `LEMON`.
- Repeat keyword to match plaintext length.
- Map letters A–Z to numbers 0–25.

  If plaintext letters are p_i and key letters k_i,

$$c_i = (p_i + k_i) \bmod 26, \qquad p_i = (c_i - k_i) \bmod 26.$$

Example Plaintext: `ATTACKATDAWN`
Key: `LEMONLEMONLE`
Ciphertext: `LXFO PVEZ RNHR`.

Security Vigenère resists simple frequency analysis because the same plaintext letter may encrypt to different ciphertext letters. However, with tools like the Kasiski test and index of coincidence, an attacker can estimate the keyword length and break the cipher.

5.2.5 Vernam Cipher and One-Time Pad

Vernam Cipher Gilbert Vernam proposed a cipher working on binary data where the key is a random binary sequence. Encryption is bitwise XOR:

$$C_i = P_i \oplus K_i,$$

and decryption uses the same operation:

$$P_i = C_i \oplus K_i.$$

One-Time Pad When the key sequence

- is truly random,
- is at least as long as the message,
- is never reused and kept completely secret,

the scheme is called a **one-time pad**. It provides *perfect secrecy*: ciphertext gives no information about plaintext. In practice it is hard to manage such keys, so one-time pads are rarely used except in very high-security applications.

5.2.6 Playfair Cipher

Playfair is a digraph (pair-of-letters) substitution cipher using a 5×5 key matrix.

Constructing the Key Matrix

1. Choose a keyword, e.g. `MONARCHY`.
2. Remove duplicate letters and write the keyword row-wise.
3. Fill remaining cells with the unused letters of the alphabet in order. I and J are usually merged.

   Example matrix:

$$\begin{array}{ccccc} M & O & N & A & R \\ C & H & Y & B & D \\ E & F & G & I/J & K \\ L & P & Q & S & T \\ U & V & W & X & Z \end{array}$$

Preparing Plaintext

1. Remove spaces and punctuation.
2. Split into digraphs.
3. If a pair has the same letter (e.g. `EE`), insert a filler (usually X) between them.
4. If a single letter remains at the end, append X.

Encryption Rules For each pair of letters:

1. If both letters are in the same row, replace each with the letter to its right (wrapping around).
2. If both are in the same column, replace each with the letter below (wrapping around).
3. Otherwise, they form the corners of a rectangle: each letter is replaced by the letter in the same row but in the column of the other letter.

Small Example Using keyword `NESOAPP` (similar to your handwritten notes), build the matrix and encrypt the plaintext "YOUAREAWESOME". Students should practise the steps of matrix construction, digraph formation and application of the three Playfair rules.

Playfair obscures single-letter frequency but can be attacked using digraph frequency analysis and known-plaintext attacks.

5.3 Transposition Techniques

5.3.1 Substitution vs Transposition

- **Substitution:** identity of symbols changes but their positions remain.
- **Transposition:** symbols stay the same but positions are permuted.

Often, practical ciphers combine both operations.

5.3.2 Rail Fence Cipher

The Rail Fence cipher is a simple transposition technique where plaintext is written in a zigzag pattern on multiple "rails" and then read off row by row.

Encryption Procedure (2 Rails)

1. Write the message without spaces: e.g. `MEETMEAFTERNOON`.
2. Write characters diagonally down and up on 2 rails:

Rail 1:	M		E		T		A		T		R		N
Rail 2:		E		T		E		F		E		O		O

3. Read row 1 then row 2: ciphertext = `MEMATRNEEFEOO`.

Decryption Idea

1. Know the number of rails and ciphertext length.
2. Mark the zigzag positions, then fill row by row with ciphertext characters.
3. Read off in zigzag to recover plaintext.

Rail Fence alone is very weak; an attacker can try small numbers of rails and use language patterns to reconstruct the message.

6 Modern Ciphers: Brief Overview

Although Unit I focuses on classical ciphers, the syllabus also asks for a brief idea of modern ciphers.

6.1 Block vs Stream Ciphers

6.1.1 Block Ciphers

- Encrypt fixed-size blocks (e.g. 64 or 128 bits).
- For each key, encryption is a reversible permutation on the block space.
- Examples: DES (64-bit block, 56-bit key), AES (128-bit block, 128/192/256-bit keys).

Long messages are encrypted by splitting into blocks and using a *mode of operation* (ECB, CBC, CFB, OFB, CTR).

6.1.2 Stream Ciphers

- Encrypt data as a continuous stream of bits or bytes.
- A keystream generator produces a pseudorandom sequence of bits derived from a short secret key.
- Each plaintext bit is XORed with the corresponding keystream bit.
- Examples: RC4 (historical), modern ciphers like ChaCha20.

Stream ciphers are suitable for real-time voice/video and constrained devices.

6.2 Symmetric vs Asymmetric Ciphers

6.2.1 Symmetric-Key (Private-Key) Cryptography

- Same secret key is used for encryption and decryption.
- Requires secure key distribution between communicating parties.
- Very fast; used for bulk data encryption.
- Examples: all block and stream ciphers (DES, 3DES, AES).

6.2.2 Asymmetric-Key (Public-Key) Cryptography

- Each user has a public key and a private key.
- Public key is widely distributed; private key is kept secret.
- Data encrypted with the public key can only be decrypted with the corresponding private key, and vice versa.
- Enables digital signatures and easier key distribution.
- Examples: RSA, Diffie–Hellman, elliptic-curve cryptography (ECC).

6.2.3 Combined Use

In real systems, both types are combined:

- Public-key algorithms are used to securely exchange a short *session key*.
- Symmetric algorithms then encrypt the actual data using that session key.

Example: in HTTPS, the browser and server perform a public-key handshake to agree on a symmetric key, then use AES to protect web traffic.

7 Summary and Exam Pointers

Key Points to Remember

- Difference between computer, information and network security.
- CIA triad: meaning and examples of confidentiality, integrity, availability.
- Definitions of cryptography, cryptosystem, cryptanalysis, key.
- Types of threats and distinction between passive and active attacks; details of release of message contents, traffic analysis, replay and DoS.
- Security services: authentication, access control, nonrepudiation and related mechanisms.
- Structure and working of classical ciphers:
  - Caesar and Hill (monoalphabetic);
  - Vigenère, Vernam, one-time pad, Playfair (polyalphabetic);
  - Rail Fence (transposition).
- Concepts of block vs stream ciphers and symmetric vs asymmetric cryptography.

Part A: Short-Answer Questions

1. Define: (a) asset, (b) vulnerability, (c) threat, and (d) attack.
2. Distinguish between computer security, information security and network security with suitable examples.
3. State the three components of the CIA triad. Give one example of each property.
4. What is cryptography? What are the basic goals of cryptography?
5. Define the following terms:

   a) plaintext

   b) ciphertext

   c) encryption

   d) decryption

   e) key
6. What is a cryptosystem? Write the 5-tuple notation of a symmetric cryptosystem and explain each symbol briefly.
7. What do you mean by key space? Why is large key space desirable?
8. Define cryptanalysis and cryptanalyst. Mention any two types of cryptanalytic attacks.
9. Differentiate between passive and active attacks with examples.
10. Explain the following passive attacks:

    a) release of message contents

    b) traffic analysis
11. Explain the following active attacks:

    a) replay attack

    b) denial-of-service (DoS) attack
12. What is authentication? Distinguish between entity authentication and data-origin authentication.

13. Define access control. Give two examples of access-control mechanisms used in computer systems.
14. What is nonrepudiation? How do digital signatures help in achieving nonrepudiation?
15. What is meant by a security service? What is a security mechanism? How are they related to a security policy?
16. Classify classical ciphers into substitution and transposition ciphers with suitable examples.
17. State the differences between monoalphabetic and polyalphabetic substitution ciphers.
18. Define the following classical ciphers (one or two lines each):

    a) Caesar cipher

    b) Hill cipher

    c) Vigenère cipher

    d) Vernam cipher / one-time pad

    e) Playfair cipher

    f) Rail fence cipher
19. Distinguish between block cipher and stream cipher.
20. Distinguish between symmetric-key and asymmetric-key cryptography with suitable examples.

Part B: Long-Answer Questions

1. Explain in detail the goals of computer security. Discuss how the CIA triad helps in formulating security requirements.
2. Describe different types of security threats and attacks in network security. Classify them as passive or active attacks with examples.
3. What are security services? Explain in detail the services of confidentiality, integrity, authentication, access control and nonrepudiation. Also mention suitable mechanisms for each.
4. Explain the concepts of security policy and security mechanism. How do they together enforce security in an organisation? Illustrate with an example of a university examination system.

5. Discuss classical substitution techniques in detail. Explain Caesar cipher, monoalphabetic cipher, Hill cipher and Vigenère cipher with suitable examples.

6. Explain polyalphabetic substitution ciphers. Describe Vigenère cipher and Vernam cipher (one-time pad). Show that one-time pad provides perfect secrecy under ideal assumptions.

7. Explain the Playfair cipher. Describe the procedure for constructing the key matrix, preparing the plaintext and performing encryption and decryption, with a worked example.

8. Describe transposition techniques. Explain the working of the Rail fence cipher and a general columnar transposition cipher with neat examples.

9. Write short notes on:

   a) cryptanalysis and types of cryptanalytic attacks

   b) brute-force attack and key space

   c) confusion and diffusion

10. Explain the basic ideas of modern block ciphers and stream ciphers. Compare their characteristics and typical application areas.

Part C: Classical Cipher Problems (Question List)

C1. Caesar Cipher

C1.1 Encrypt the plaintext `MEET ME AFTER CLASS` using Caesar cipher with key $k = 3$.

C1.2 Decrypt the ciphertext `KHOORZRUOG` that was produced by a Caesar cipher. Find the key used.

C2. Vigenère Cipher

C2.1 Encrypt the plaintext `CRYPTOGRAPHYISFUN` using the keyword `MATH` in Vigenère cipher.

C2.2 Decrypt the ciphertext `LXFOPVEFRNHR` produced by Vigenère cipher using keyword `LEMON`.

C3. Vernam Cipher / One-Time Pad

C3.1 Encrypt the binary plaintext `10110010 01101100` using one-time pad key `01010101 11001010`.

C3.2 Explain why one-time pad provides perfect secrecy. List its practical limitations.

C4. Hill Cipher

C4.1 Using a 2×2 Hill cipher with key matrix

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix},$$

encrypt the plaintext `HI`.

C4.2 Using the same key matrix K as above, decrypt the ciphertext `TC`.

C4.3 Construct a 2×2 key matrix for Hill cipher and explain how to check that it is invertible modulo 26.

C5. Playfair Cipher

C5.1 Using Playfair cipher with keyword `NEPAL`, encrypt the plaintext `YOU ARE AWESOME`.

C5.2 Using the same keyword `NEPAL`, decrypt the ciphertext `HEGMTIFYKHPQCIQSMRZY`.

C6. Rail Fence Cipher

C6.1 Encrypt the plaintext `MEET ME AFTER NOON` using a two-rail Rail fence cipher.

C6.2 The ciphertext `MEMATRONETEFENO` was produced by a two-rail Rail fence cipher. Recover the original plaintext.

C6.3 Explain how Rail fence cipher can be viewed as a special case of a transposition cipher.

Part D: Solved Cipher Problems

D1. Hill Cipher – Solved Examples

Example H1 (Encryption)

Question: Using a 2×2 Hill cipher with key

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix},$$

encrypt the plaintext `HI`. Use the mapping A=0, B=1, ..., Z=25.

Solution:

1. Convert letters to numbers:
   H $\to$ 7, I $\to$ 8.
   Plaintext vector:
   $$P = \begin{bmatrix} 7 \\ 8 \end{bmatrix}.$$

2. Compute ciphertext vector
   $$C = KP \bmod 26 = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 3 \cdot 7 + 3 \cdot 8 \\ 2 \cdot 7 + 5 \cdot 8 \end{bmatrix} = \begin{bmatrix} 45 \\ 54 \end{bmatrix}.$$
   Take modulo 26:
   $$45 \equiv 19 \pmod{26}, \qquad 54 \equiv 2 \pmod{26}.$$
   Hence
   $$C = \begin{bmatrix} 19 \\ 2 \end{bmatrix}.$$

3. Convert numbers back to letters:
   19 $\to$ T, 2 $\to$ C.
   Therefore ciphertext is **TC**.

Example H2 (Decryption)

Question: Using the same Hill cipher key

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix},$$

decrypt the ciphertext `TC`.

Solution:

1. First we need the inverse matrix K^{-1} modulo 26.

   Determinant:

   $$\det(K) = 3 \cdot 5 - 3 \cdot 2 = 9.$$

   Since $\gcd(9, 26) = 1$, the matrix is invertible mod 26.

   The inverse of 9 modulo 26 is 3 because

   $$9 \times 3 = 27 \equiv 1 \pmod{26}.$$

   The adjoint matrix of K is

   $$\begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}.$$

   Multiply by 3 and reduce modulo 26:

   $$K^{-1} \equiv 3 \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix} = \begin{bmatrix} 15 & -9 \\ -6 & 9 \end{bmatrix} \equiv \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \pmod{26}.$$

2. Convert ciphertext to numbers: T $\to$ 19, C $\to$ 2, so

   $$C = \begin{bmatrix} 19 \\ 2 \end{bmatrix}.$$

3. Compute plaintext vector

   $$P = K^{-1}C \bmod 26 = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 19 \\ 2 \end{bmatrix} = \begin{bmatrix} 15 \cdot 19 + 17 \cdot 2 \\ 20 \cdot 19 + 9 \cdot 2 \end{bmatrix} = \begin{bmatrix} 319 \\ 398 \end{bmatrix}.$$

   Take modulo 26:

   $$319 = 26 \cdot 12 + 7 \Rightarrow 319 \equiv 7, \qquad 398 = 26 \cdot 15 + 8 \Rightarrow 398 \equiv 8.$$

   Thus

   $$P = \begin{bmatrix} 7 \\ 8 \end{bmatrix}.$$

4. Convert to letters: 7 $\to$ H, 8 $\to$ I.
   Therefore plaintext is **HI**.

D2. Rail Fence Cipher – Solved Examples

Example R1 (Encryption, 2 Rails)

Question: Encrypt the plaintext `MEET ME AFTER NOON` using a two-rail Rail fence cipher (write letters in two rows alternately and then read row-wise).

Solution:

1. Remove spaces and convert to uppercase:
   MEETMEAFTERNOON (15 letters).

2. Write letters alternately on Rail 1 and Rail 2:

Position	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Letter	M	E	E	T	M	E	A	F	T	E	R	N	O	O	N
Rail 1	M		E		M		A		T		R		O		N
Rail 2		E		T		E		F		E		N		O	

3. Read characters row-wise.

   - Rail 1: M E M A T R O N ⇒ `MEMATRON`
   - Rail 2: E T E F E N O ⇒ `ETEFENO`

   Ciphertext is **MEMATRONETEFENO**.

Example R2 (Decryption, 2 Rails)

Question: Ciphertext `MEMATRONETEFENO` was produced using a two-rail Rail fence cipher as in Example R1. Recover the plaintext.

Solution:

1. Ciphertext length = 15. For two rails, first rail gets $\lceil 15/2 \rceil = 8$ letters and second rail gets the rest (7 letters).

   - Rail 1: first 8 letters ⇒ `MEMATRON`
   - Rail 2: remaining 7 letters ⇒ `ETEFENO`

2. Now read the letters alternately from Rail 1 and Rail 2:

$$\text{Rail 1: } M, E, M, A, T, R, O, N$$

Rail 2: E, T, E, F, E, N, O

Interleaving:

$$M, E, E, T, M, E, A, F, T, E, R, N, O, O, N$$

which gives plaintext `MEETMEAFTERNOON`.

3. Insert spaces as desired: **MEET ME AFTER NOON**.

D3. Playfair Cipher – Solved Examples

Example P1 (Encryption)

Question: Using Playfair cipher with keyword `NEPAL`, encrypt the plaintext `YOU ARE AWESOME`. Assume `I/J` are combined.

Solution:

1. Construct the 5×5 key matrix.

   - Keyword: NEPAL (remove duplicates).
   - Fill remaining letters of alphabet (merging I and J).

   Key matrix:

$$\begin{array}{ccccc} N & E & P & A & L \\ B & C & D & F & G \\ H & I & K & M & O \\ Q & R & S & T & U \\ V & W & X & Y & Z \end{array}$$

2. Prepare plaintext: remove spaces and form digraphs.

$$\text{YOUAREAWESOME} \Rightarrow \text{YOUAREAWESOME}$$

   Pair letters (insert X if a pair repeats, and pad final single letter with X):

$$YO \mid UA \mid RE \mid AW \mid ES \mid OM \mid EX.$$

3. Encrypt each digraph using Playfair rules.

   - YO: Y and O form a rectangle; Y$(5,4)$, O$(3,5)$ $\Rightarrow$ Z and M $\Rightarrow$ `ZM`.

- UA: U$(4,5)$, A$(1,4)$ $\Rightarrow$ T and L $\Rightarrow$ `TL`.
- RE: R$(4,2)$, E$(1,2)$, same column $\Rightarrow$ W and C $\Rightarrow$ `WC`.
- AW: A$(1,4)$, W$(5,2)$, rectangle $\Rightarrow$ E and Y $\Rightarrow$ `EY`.
- ES: E$(1,2)$, S$(4,3)$, rectangle $\Rightarrow$ P and R $\Rightarrow$ `PR`.
- OM: O$(3,5)$, M$(3,4)$, same row $\Rightarrow$ H and O $\Rightarrow$ `HO`.
- EX: E$(1,2)$, X$(5,3)$, rectangle $\Rightarrow$ P and W $\Rightarrow$ `PW`.

4. Concatenate all digraphs:

$$\text{Ciphertext} = \texttt{ZM TL WC EY PR HO PW} = \boxed{\texttt{ZMTLWCEYPRHOPW}}.$$

Example P2 (Decryption)

Question: Using the same Playfair key matrix (keyword `NEPAL`), decrypt the ciphertext

`HEGMTIFYKHPQCIQSMRZY`.

Solution (outline):

1. Use the same key matrix as in Example P1.
2. Split ciphertext into digraphs:

$$HE \mid GM \mid TI \mid FY \mid KH \mid PQ \mid CI \mid QS \mid MR \mid ZY.$$

3. For each pair apply the *inverse* Playfair rules:

   - same row: shift one position to the *left*;
   - same column: shift one position *up*;
   - rectangle: replace with letters in same row but opposite corners of rectangle.

   Working through all pairs (students should practise on the matrix), we obtain the sequence of plaintext digraphs:

$$IN \mid FO \mid RM \mid AT \mid IO \mid NS \mid EC \mid UR \mid IT \mid YX.$$

4. Combine them:

`INFORMATIONSECURITYX`.

Dropping the padding X at the end gives

INFORMATION SECURITY.