

Classical Encryption Techniques

Prepared by Dr. Sumaya Alkubaisi

FNT625
Cybersecurity Concepts

Lecture 3



Lecture

3

Learning Goals

By the end of this lecture, you will be able to:

- Define the concept of classical cryptography and explain why it is important.
- Describe the symmetric cipher model and different types of attacks.
- Explain and apply substitution techniques such as Caesar, Monoalphabetic, Playfair, Hill, Vigenère, and One-Time Pad.
- Explain and apply transposition techniques such as Rail Fence.
- Compare steganography vs encryption and recognize their differences.
- Understand the role of cryptanalysis and brute-force attacks in breaking ciphers.
- Evaluate the strengths and weaknesses of classical ciphers and link them to modern cryptographic systems.

Lecture

3

Why Study Classical Ciphers?

They are the foundation of modern cryptography.

- Show the evolution of ideas: from simple letter shifts to complex algorithms.
- Teach basic concepts: keys, encryption, decryption, cryptanalysis.
- Even if insecure today, they explain why strong encryption is needed.

What is Cryptography?

- Science of protecting information by transforming it so only authorized parties can understand it.
- Two main goals: **Confidentiality** and **Integrity**.

Example: Sending a secret message during war → encrypted so enemies can't read it.

What is Cryptography?

Plaintext: An original message

Ciphertext: The coded message

Enciphering/encryption: The process of converting from plaintext to ciphertext

Deciphering/decryption: Restoring the plaintext from the ciphertext

Cryptography: The area of study of the many schemes used for encryption

Cryptographic system/cipher: A scheme

Cryptanalysis: Techniques used for deciphering a message without any knowledge of the enciphering details

Cryptology: The areas of cryptography and cryptanalysis

Cryptographic Systems (Dimensions)

A system is defined by:

Type of operation – substitution or transposition.

Number of keys – symmetric (1 key) or asymmetric (2 keys).

Processing – block (chunks) or stream (one symbol at a time).

Lecture

3

The Symmetric Cipher Model (Symmetric Encryption)

Used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords

Same secret key is used for encryption and decryption.

Two requirements:

- A strong encryption algorithm.
- Sender and receiver must have obtained copies of the
 - secret key in a secure fashion and must keep the key secure

Example: Caesar cipher (shift by 3).



Symmetric Cipher Model Diagram

-Plaintext $\rightarrow$ Encryption Algorithm
(with Key) $\rightarrow$ Ciphertext.

-Receiver applies same Key with
Decryption Algorithm $\rightarrow$ Plaintext.

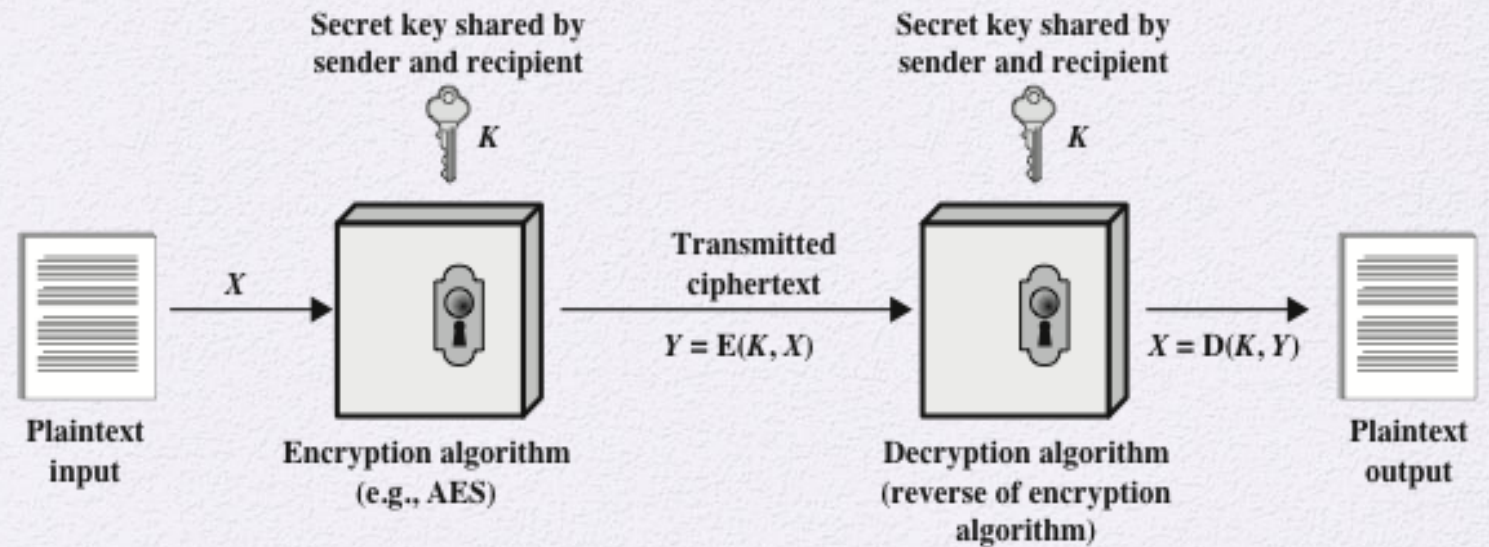


Figure 3.1 Simplified Model of Symmetric Encryption

Attacks on Symmetric Ciphers

Lecture

1

Cryptanalysis – exploiting weaknesses in the algorithm.

Brute Force – trying all possible keys until message is revealed.

Example: Caesar cipher has only 25 possible keys → easily brute-forced.

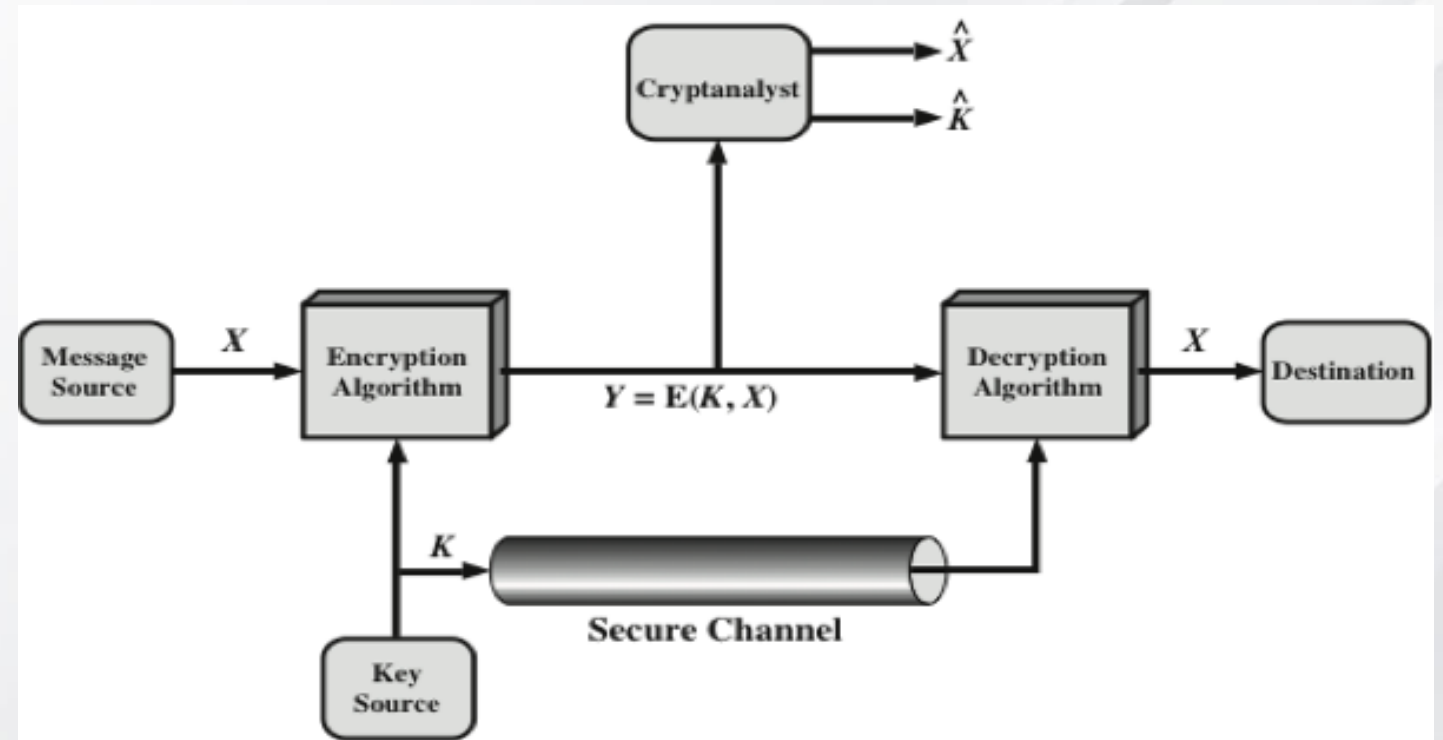


Figure 3.2 Model of Symmetric Cryptosystem

Security Levels

Unconditionally Secure (Perfect Security)

Even with unlimited computing power, the cipher cannot be broken (e.g., One-Time Pad)

Key is random, as long as the message, and never reused.

Attacker sees ciphertext but cannot know the plaintext.

Problem: Not practical → requires huge random keys, difficult to share securely.

Computationally Secure (Practical Security)

The cipher can be broken in theory, but would take billions of years with today's computers.

Example: Modern ciphers (AES, DES in early days).

AES with a 128-bit key → 2^{128} possible keys (too many to brute force).

Widely used today because it's "secure enough" in practice.

Classical Ciphers (Caesar, Vigenère, etc.)

Very weak by modern standards.

Example: Caesar cipher only has 25 keys → brute force takes seconds.

Not secure today → used only for learning or puzzles, not real protection

Cryptanalysis and Brute-Force Attack

Cryptanalysis: Attack relies on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext.

Attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used

Brute-force attack: Attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.

On average, half of all possible keys must be tried to achieve success

Lecture

3

Substitution Techniques

the letters of plaintext are replaced by other letters or by numbers or symbols
If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns

Examples: Caesar, Monoalphabetic, Playfair, Hill, Vigenère, One-Time Pad.



Caesar Cipher

- Oldest known substitution cipher.
- Invented by Julius Caesar to protect military messages.
- Each letter shifted by 3 positions in the alphabet.
- Alphabet is wrapped around so that the letter following Z is A.

Example:

Plaintext: MEET ME

Ciphertext: PHHW PH

Lecture

3

Caesar Cipher Algorithm

Can define transformation as:

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

Mathematically give each letter a number

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 Algorithm

Algorithm can be expressed as:

$$c = E(3, p) = (p + 3) \bmod (26)$$

A shift may be of any amount, so that the general Caesar algorithm is:

$$C = E(k, p) = (p + k) \bmod 26$$

Where k takes on a value in the range 1 to 25; the decryption algorithm is simply:

$$p = D(k, C) = (C - k) \bmod 26$$

Lecture

3

Caesar Cipher Algorithm

Example

Plaintext: **HELLO**

Key: **k = 3**

H → K

E → H

L → O

L → O

O → R

Ciphertext: **KHOOR**

Monoalphabetic Cipher

- Each letter is substituted by any other letter, you decide the mapping (shifted, keyword-based, or random).
 - Same mapping must be used for the whole message.
 - You can change the mapping for a new message.
 - Easy to break: Because the cipher still shows the same letter frequency as normal English.
- Digram: A pair of letters. Example: “th” (very common).
- Trigram: A group of three letters. Example: “the” (most frequent).
- Attackers use these patterns to guess the hidden message.

Monoalphabetic Cipher

Plaintext → Ciphertext Mapping (random mapping)

A→Q B→W C→E D→R E→T F→Y G→U H→I I→O J→P
K→A L→S M→D N→F O→G P→H Q→J R→K S→L T→Z
U→X V→C W→V X→B Y→N Z→M

Example:

HELLO → ITSSG

Playfair Cipher

- Encrypts pairs (digrams) of letters using a 5×5 matrix.
- Fill in letters of keyword (minus duplicates) from left to right and from top to bottom, then fill in the remainder of the matrix with the remaining letters in alphabetic order
- Invented by British scientist Sir Charles Wheatstone in 1854
- Used as the standard field system by the British Army in World War I and the U.S. Army and other Allied forces during World War II

Lecture

3

Playfair Cipher (Example)

1. Create a 5×5 matrix using a keyword

Keyword: MONARCHY

Remove duplicates: M O N A R C H Y

Fill the rest of the alphabet

(combine I/J to fit 25 letters):

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

2. Prepare the plaintext

Plaintext: HELLO

Break into pairs (digrams). If a letter repeats in a pair or a pair is incomplete, add a filler (usually X):

HE LL O

Rule: no double letters in the same pair → fix LL by inserting X:

→ HE LX LO

Now we have 3 valid pairs: **HE – LX – LO**

Playfair Cipher (Example)

3. Encrypt each pair using the Playfair rules

Rule 1: If letters are in the same row, replace each with the letter to its right (wrap around if needed).

Rule 2: If letters are in the same column, replace each with the letter below (wrap around if needed).

Rule 3: If letters form a rectangle (different row and column), replace each with the letter in the same row but the column of the other letter.

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

4. Encrypt each pair

Pair 1: HE

H → row2 col2

E → row3 col1

Result: HE → CY

Rectangle rule → swap columns:

H → C (row2 col1)

E → Y (row3 col2)

Lecture

3

Playfair Cipher (Example)

Pair 2: LX

L → row4 col1 X → row5 col4

Rectangle rule → swap columns:

L → S (row4 col4)

X → U (row5 col1)

LX → SU

Pair 3: LO

L → row4 col1 O → row1 col2

Rectangle rule → swap columns:

L → P (row4 col2)

O → M (row1 col1)

LO → PM

4. Final Ciphertext → Combine: CY + SU + PM = CYSUPM

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

Lecture

3

Hill Cipher

- Strength is that it completely hides single- letter frequencies
 - The use of a larger matrix hides more frequency information
 - A 3 x 3 Hill cipher hides not only single-letter but also two-letter frequency information
 - Strong against a ciphertext-only attack but easily broken with a known plaintext attack
 - Uses matrix multiplication on letter values (A=0,...,Z=25).
 - you can use different matrix sizes: 2x2, 3x3, 4x4, ... depending on how many letters you want to encrypt at a time.
- If your key matrix is 2x2 → you encrypt 2 letters (a digram) at a time.
- If it's 3x3 → you encrypt 3 letters (a trigram) at a time, etc.

Lecture

3

Hill Cipher

Example:

Key Matrix 2×2:

3 3

2 5

Plaintext: HI → H=7, I=8

$3 \times 7 + 3 \times 8, 2 \times 7 + 5 \times 8 = 45, 54 \rightarrow \text{mod } 26 \rightarrow (19, 2)$

= T, C

Ciphertext: TC

Lecture

3

Vigenère Cipher

- In this scheme the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25
- Each letter of the key corresponds to a shift value. For instance, if the key letter is “A,” that means no shift. If it’s “B,” that means a shift of 1, and so on, up to “Z,” which would mean a shift of 25.
- To encrypt a longer message, you repeat the key so that each plaintext letter has a corresponding key letter.
- Each letter of the plaintext is shifted by the amount determined by the corresponding key letter. This means that each letter in the message can have a different shift, creating a more complex encryption than a single Caesar cipher.
- Vigenère can be broken using frequency analysis or statistical patterns, because the key repeats.

Lecture

3

Vigenère Cipher

Example:

Plaintext: ATTACKATDAWN

Key: LEMON (repeated $\rightarrow$ LEMONLEMONLE)

$A (0) + L (11) = 11 \rightarrow L$

$T (19) + E (4) = 23 \rightarrow X$

$T (19) + M (12) = 31 \bmod 26 = 5 \rightarrow F$

$A (0) + O (14) = 14 \rightarrow O$

$C (2) + N (13) = 15 \rightarrow P \dots$

Ciphertext: LXFOPVEFRNHR

Lecture

3

Vigenère Autokey System

- A keyword is concatenated with the plaintext itself to provide a running key

Example:

key: deceptivewearediscoveredsav

plaintext: wearediscoveredsaveyourself

ciphertext: ZICVTWQNGKZEIIGASXSTSLVWLA

- Even this scheme is vulnerable to cryptanalysis
 - Because the key and the plaintext share the same frequency distribution of letters, a statistical technique can be applied

Lecture

3

Vernam Cipher

It's very similar to the Vigenère cipher, but with two key differences:

- The key is as long as the plaintext.
- The key is completely random (no patterns, no repetitions).

Encryption rule:

Classical Vernam (text/letters): $C_i = (P_i + K_i) \bmod 26$ (Works on letters A–Z.)

Binary Vernam (modern form, one-time pad / stream cipher): Uses XOR ($\oplus$), which is the same as addition modulo 2.

$C_i = P_i \oplus K_i$ (Works on bits (0 and 1))

One-Time Pad

- Improvement to Vernam cipher proposed by an Army Signal Corp officer, Joseph Mauborgne
- Uses a truly random key as long as the message.
- Key is never repeated → used once then discarded.
- Each new message → needs a new random key of equal length.
- Unbreakable: ciphertext has no link to plaintext, giving perfect secrecy.

One-Time Pad – Difficulties

- The one-time pad provides perfect security, but it has two main problems in practice:
 1. Generating random keys – Huge amounts of true random keys are needed. A busy system may require millions of random characters regularly, which is very hard to produce.
 2. Distributing keys – Each message needs a key of the same length. Both sender and receiver must securely share these large keys, creating a serious key distribution problem.
- Because of these difficulties, the one-time pad is not practical for everyday use. It is mainly used in special cases with small communication channels but very high security needs.
- It remains the only encryption method with perfect secrecy.

Lecture

3

Rail Fence

- The Rail Fence Cipher is one of the simplest transposition ciphers.
- In this method, the plaintext is written in a zig-zag pattern (diagonals), then read row by row.

Example with depth = 2 (two rails):

Plaintext:

meet me after the toga party

Write letters in 2 rows:

m e m a t r h t g p r y

e t e f e t e o a a t

Encrypted message is: MEMATRHTGPRYETEFETEOAAT

Steganography

- the art of hiding a secret message inside another medium so that its existence isn't obvious. It can be done in text, images, audio, video, or even physical objects.
- A classic literary example comes from “The Silent World of Nicholas Quinn” by Colin Dexter (an Inspector Morse novel):

Steganography

3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours,

A Puzzle for Inspector Morse
(from *The Silent World of Nicholas Quinn*, by Colin Dexter)

Steganography

3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours,

A Puzzle for Inspector Morse
(from *The Silent World of Nicholas Quinn*, by Colin Dexter)

Other Steganography Techniques (Physical)

Character Marking

Certain letters in printed or typed text are lightly marked with pencil. Marks are usually invisible unless the paper is held at an angle to bright light.

Invisible Ink

Special substances write messages that cannot be seen until heat or a chemical is applied.

Pin Punctures

Tiny holes are made on selected letters. Invisible unless the paper is held up to a light source.

Typewriter Correction Ribbon

Used between typed lines with a black ribbon. Marks become visible only under strong light.



Lecture

3

Recap

- Cryptography basics: Protects confidentiality and integrity through encryption.
- Symmetric Cipher Model: Uses the same secret key for encryption and decryption.
- Substitution Ciphers: Replace letters (Caesar, Monoalphabetic, Playfair, Hill, Vigenère, Vernam, One-Time Pad).
- Transposition Ciphers: Rearrange letters (Rail Fence).
- Steganography: Hides the existence of a message, not just its content.
- Cryptanalysis & Brute-force: Show why classical ciphers are insecure today.
- Key lesson: Classical methods are broken, but they form the foundation of modern cryptography (AES, RSA).

References

- Stallings, “Cryptography and Network Security”, Pearson, (7th Edition, 2017).