

Block cipher cryptanalysis and usage

Prepared by Dr. Ayman Khallel

IT373

Information Security

Lecture 4



Course content

1. Overview of security concepts and definitions
2. Symmetric cryptography; modern encryption algorithms (DES, AES)
3. modern data encryption standards;
4. block cipher cryptanalysis and usage
5. modern stream ciphers
6. Asymmetric cryptography; public key cryptography, key certificates and management
7. message authentication and hash functions
8. hash algorithms
9. digital signature and authentication protocols
10. electronic mail security, IP security, web security.

Agenda/Outline

- Definitions
- Cryptanalysis and Brute-Force Attack
- Strong Encryption
- Substitution Ciphers:
 - Caesar Cipher
 - Monoalphabetic Cipher
 - Playfair Cipher
 - Hill Cipher.
 - Vigenère Cipher
- Transposition Ciphers:
 - Rail Fence Cipher
- Summary

Definitions

- Cryptanalysis is the art of breaking or analysing codes to uncover hidden information. It finds vulnerabilities in encryption systems and decodes messages encoded using cryptographic techniques.
- For centuries, cryptanalysis has played a crucial role in revealing hidden information in secret messages conveyed through basic codes.
- Cryptanalysis advanced with the emergence of computers & internet, evolving into a more sophisticated field with new techniques & tools to break complex encryption.
- Cryptanalysis is vital in information security, playing a critical role in attacking and defending against cyber threats.



Symmetric Cipher Model

- There are two requirements for secure use of conventional encryption:
 - 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



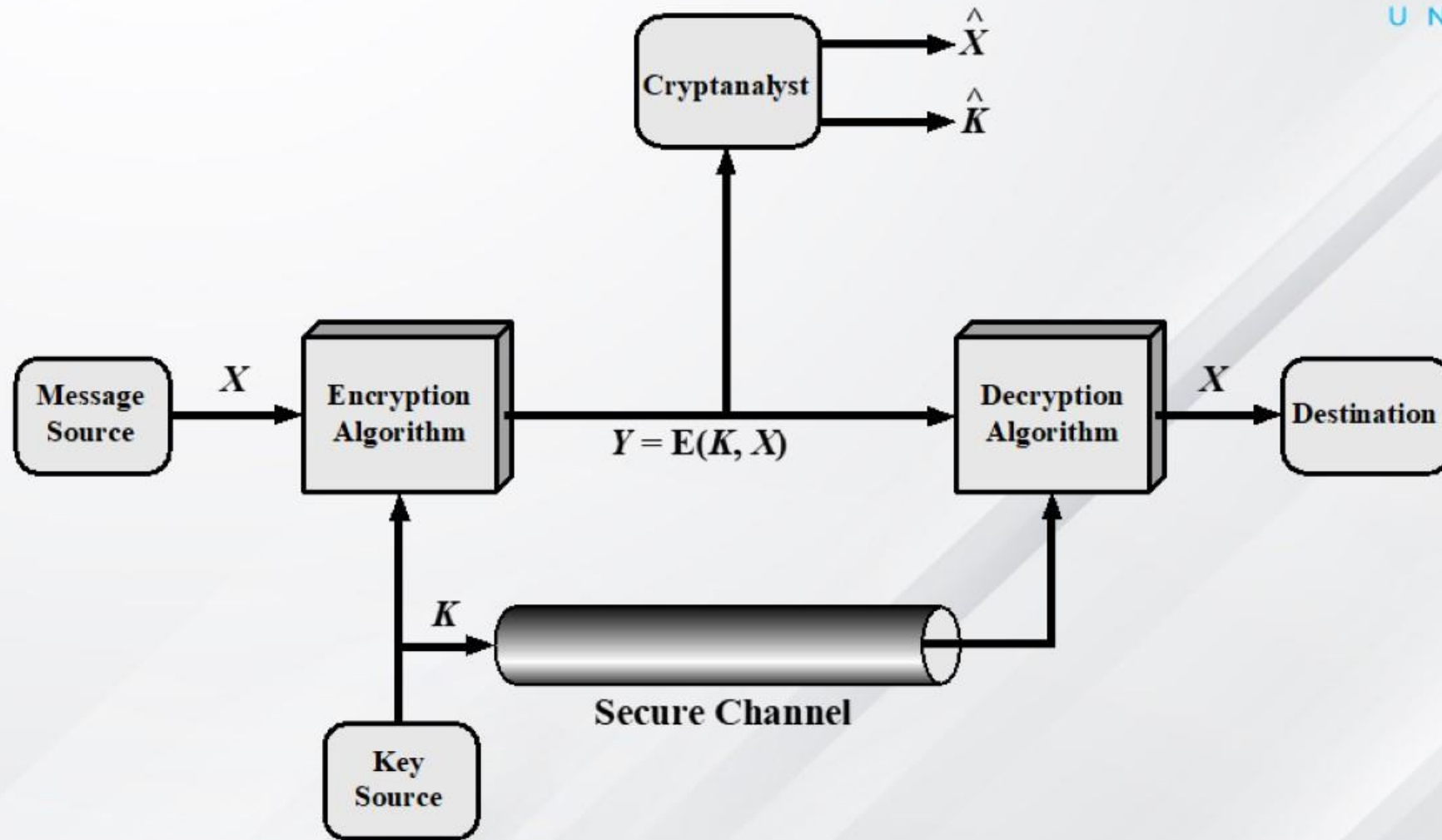
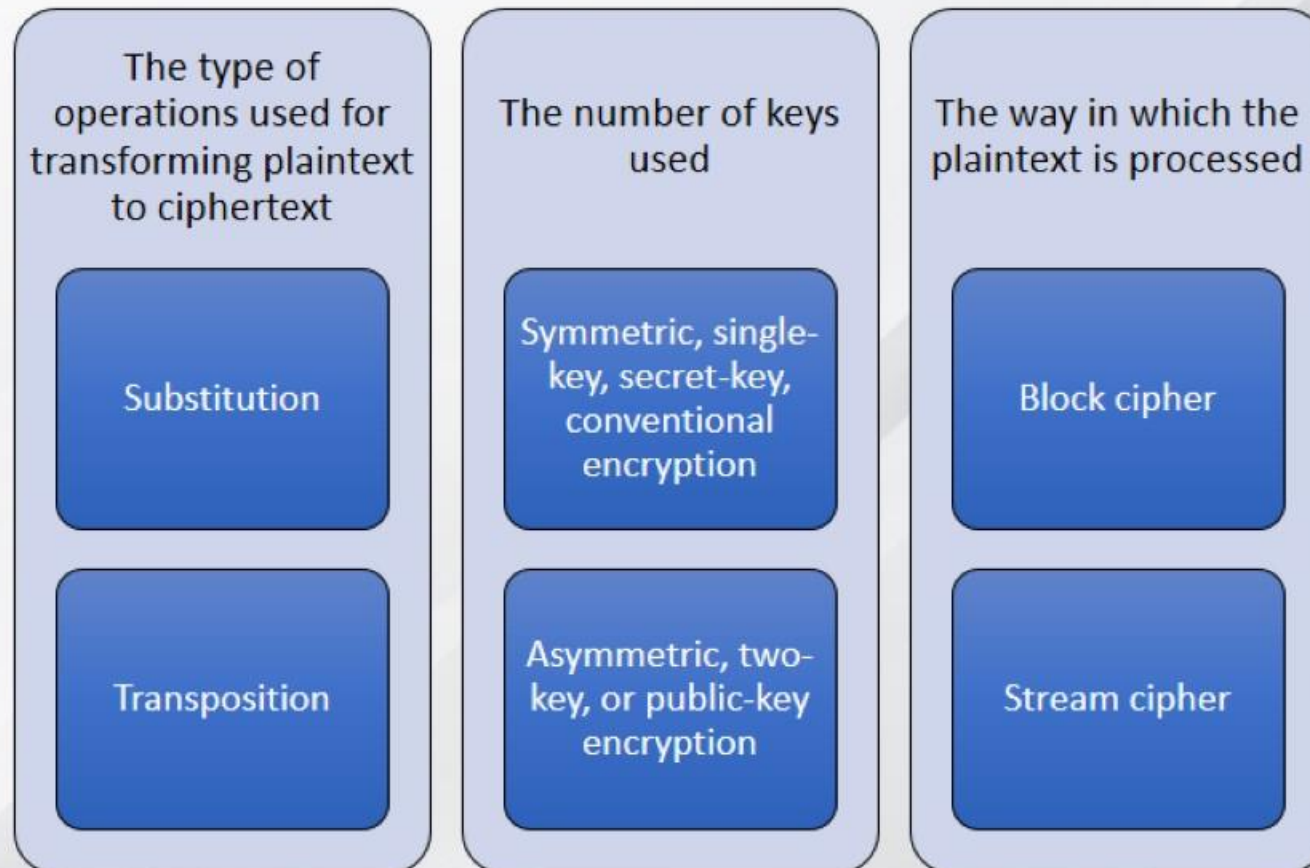


Figure 3.2 Model of Symmetric Cryptosystem



Cryptographic Systems

- Characterized along three independent dimensions:



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



Table 3.1

Types of
Attacks
on
Encrypted
Messages

Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key



Encryption Scheme Security

- Unconditionally secure
 - No matter how much time an opponent has, it is impossible for him or her to decrypt the ciphertext simply because the required information is not there
- Computationally secure
 - The cost of breaking the cipher exceeds the value of the encrypted information
 - The time required to break the cipher exceeds the useful lifetime of the information



Brute-Force Attack

Involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained



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



To supplement the brute-force approach, some degree of knowledge about the expected plaintext is needed, and some means of automatically distinguishing plaintext from garble is also needed



Strong Encryption

- The term *strong encryption* refers to encryption schemes that make it impractically difficult for unauthorized persons or systems to gain access to plaintext that has been encrypted
- Properties that make an encryption algorithm strong are:
 - Appropriate choice of cryptographic algorithm
 - Use of sufficiently long key lengths
 - A well-engineered implementation
 - Absence of deliberately introduced hidden flaws



Substitution Technique

- Is one in which 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

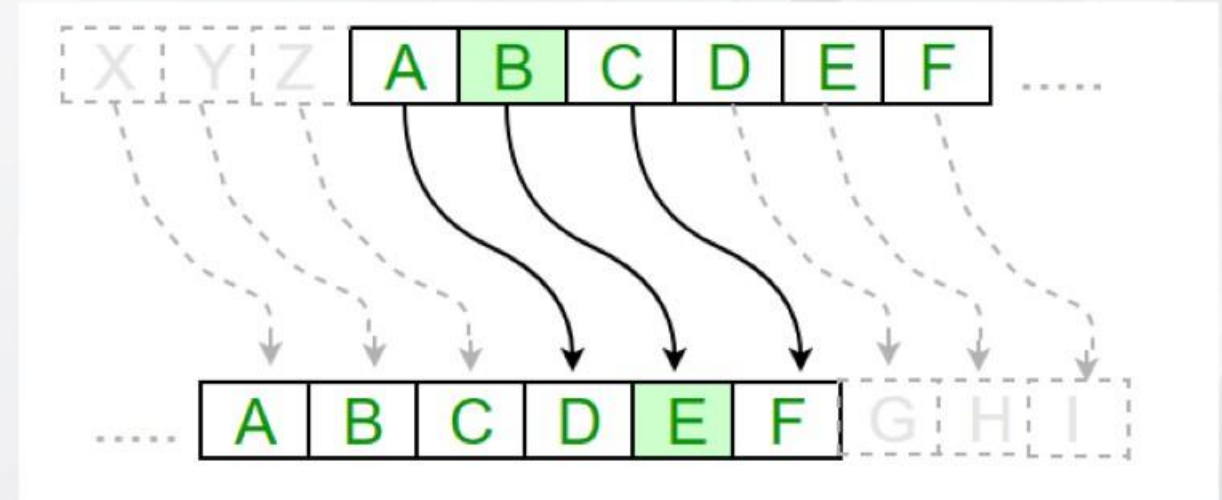


Caesar Cipher

- Simplest and earliest known use of a substitution cipher
- Used by Julius Caesar
- Involves replacing each letter of the alphabet with the letter standing three places further down the alphabet
- Alphabet is wrapped around so that the letter following Z is A

plain: meet me after the
toga party

cipher: PHHW PH DIWHU WKH
WRJD SDUWB



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

- Algorithm can be expressed as:

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

ex:

$$c = E(3, 'a') = (0 + 3) \bmod 26 = 3 \bmod 26 = 3 \Rightarrow (d)$$

$$c = E(3, 'z') = (25 + 3) \bmod 26 = 28 \bmod 26 = 2 \Rightarrow (c)$$

- 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:

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



Figure 3.3

Brute-Force Cryptanalysis of Caesar Cipher

(This chart can be found on page 71 in the textbook)

KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vgic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrpc	rfe	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	objv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	unmb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzcx	znk	zung	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc



Figure 3.3 Brute-Force Cryptanalysis of Caesar Cipher

Sample of Compressed Text

~+Wμ"- Ω-0)≤4{∞‡, ë~Ω%ràu.~í ◇-z-
Ú≠2Ò#Åæð æ«q7,Ωn.®3NÔÚ Œz'Y-f∞Í[±Ũ_ èΩ,<NO¬±«~xã Åä£èü3Å
x}ö§k°Â
_yÍ ^ΔÉ] ,κ J/°iTê&1 'c<uΩ-
ÄD(G WÄC~y_iöÄW PÔ1«ÎÜ†ç],κ;~Ï^üÑπ~≈~L~9OgflO~&Œ≤ ¬≤ ØÔ§":
~Œ!SGqèvo^ ú\,S>h<-*6ø‡%x'"|fiÓ#≈~my%~≥ñP<,fi Áj ÅÔ¿"Zù-
Ω"Ö-6Œÿ{%, „ΩÊó ,i π÷Áî°úO2çSÿ'O-
2Äflßi /@^"ΠK°ªPŒπ,úé^'3Σ~ö~ÔZÌ"Y¬ÿΩæY> Ω+eô/·<K£¿*÷~"≤û~
B ZøK~Qßÿüf,!ÒflîzsS/]>ÈQ ü

Figure 3.4 Sample of Compressed Text



Monoalphabetic Cipher

- Permutation
 - Of a finite set of elements S is an ordered sequence of all the elements of S , with each element appearing exactly once
ex: $S = \{a, b, c\}$
abc acb bac bca cab cba
- If the “cipher” line can be any permutation of the 26 alphabetic characters, then there are $26!$ or greater than 4×10^{26} possible keys
 - This is 10 orders of magnitude greater than the key space for DES
 - Approach is referred to as a *monoalphabetic substitution cipher* because a single cipher alphabet is used per message



Monoalphabetic Cipher

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

Encrypting the plaintext: **HELLO**

1. H $\rightarrow$ I
2. E $\rightarrow$ T
3. L $\rightarrow$ S
4. L $\rightarrow$ S
5. O $\rightarrow$ G

So, the ciphertext would be: **ITSSG**

Decrypting the plaintext: **ITSSG**

1. I $\rightarrow$ H
2. T $\rightarrow$ E
3. S $\rightarrow$ L
4. S $\rightarrow$ L
5. G $\rightarrow$ O

So, the ciphertext would be: **HELLO**



Step 1: Calculate Letter Frequencies

- Count how often each letter appears in the ciphertext.
- Example frequencies:
 - **P**: 13.33%
 - **Z**: 11.67%
 - **S, U**: 8.33%
 - **O**: 7.50%

Step 2: Compare with English Letter Frequencies

- "In English, 'e' and 't' are the most frequent letters."
- "P and Z are likely 'e' and 't,' but we're not certain yet."

Step 3: Analyze the Remaining Letters

- "High-frequency letters S, U, O, M, H could correspond to common English letters like a, h, i, n, o, r, s."
- "Less frequent letters A, B, G, Y might correspond to rare letters like b, j, k, q, v, x, z."

Next Steps

- "We can make tentative assignments for some letters and begin constructing a possible plaintext."
- "Alternatively, we can look for repeating letter sequences or known words."

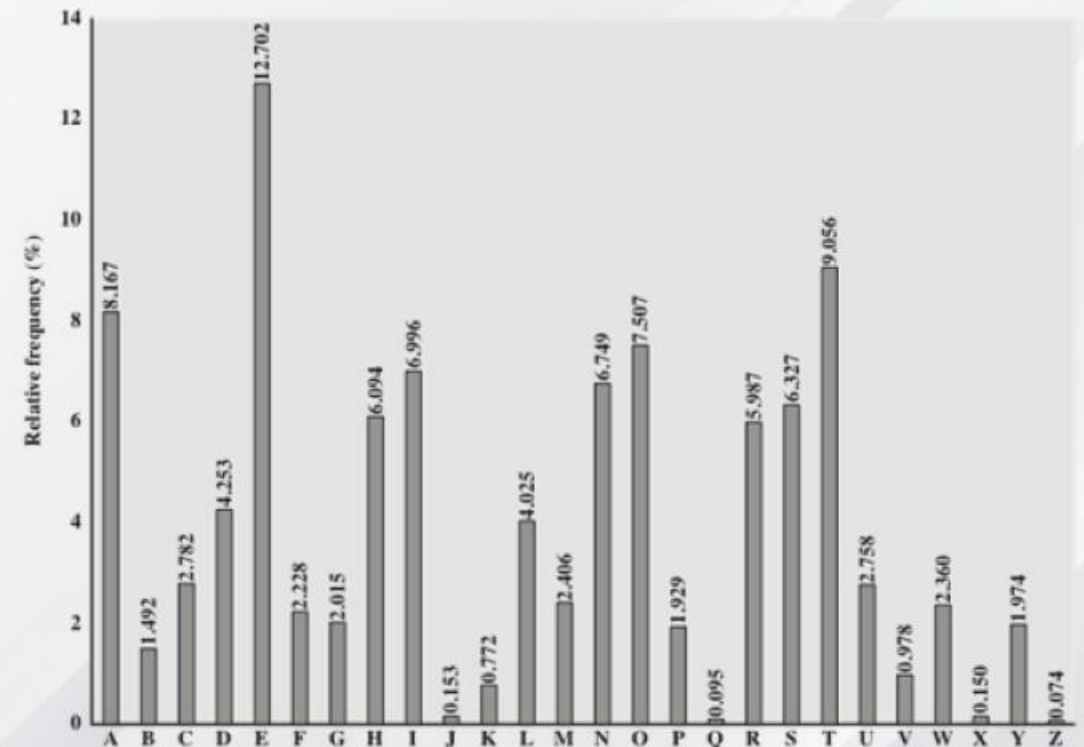


Figure 3.5 Relative Frequency of Letters in English Text



Monoalphabetic Ciphers

- Easy to break because they reflect the frequency data of the original alphabet
- Countermeasure is to provide multiple substitutes (homophones) for a single letter
- Digram
 - Two-letter combination
 - Most common is *th*
- Trigram
 - Three-letter combination
 - Most frequent is *the*



Playfair Cipher

- Best-known multiple-letter encryption cipher
- Treats digrams in the plaintext as single units and translates these units into ciphertext digrams
- Based on the use of a 5 x 5 matrix of letters constructed using a keyword
- 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



Playfair Cipher

- Multiple letter encryption cipher
- Digraphs
- 5x5 matrix constructed using a keyword (Ex Monarchy)

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



Rules for encryption using Playfair Cipher

- Step 1 Generating Digraphs for Playfair Cipher
- Prepare the Plaintext
 - Remove non-alphabetic characters (punctuation, numbers).
 - Convert letters to uppercase (optional).
Example: "HELLO"
- Handle Repeated Letters
 - Replace consecutive identical letters with a filler (e.g., 'X').
Example: "LL" → "LX"
"HELLO" → "HE", "LX", "LO"
- Add Filler for Odd-Length Text
 - Add a filler letter (e.g., 'X') if there is an odd number of letters.
Example: "HELLO" (no filler needed) or "HELLOX" (if no repeated letters).
- Create Digraphs
 - Split the text into pairs of two letters.
Example: "HELLO" → "HE", "LX", "LO"



Rules for encryption using Playfair Cipher

- Example
- Plaintext: attack
Digraphs: at ta ck
- Plaintext: Neso academy
- Digraphs: Ne so ac ad em yx
- Plaintext: ballon
- Digraphs: ba ll oo n
- Digraphs: ba lx lo on



Rules for encryption using Playfair Cipher

- **Rule 2: Same Row:** If both letters in the digraph appear on the same row of the key square, replace them with the letters immediately to their right (wrap around if needed).
- **Rule 3: Same Column:** If both letters in the digraph are in the same column, replace them with the letters immediately below (wrap around if needed).
- **Rule 4: Rectangle Rule** (Different Row and Column): If the two letters form a rectangle (i.e., they are not in the same row or column), swap the letters in the same row but in 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



Rules for encryption using Playfair Cipher

- Example
- Plaintext: attack
Digraphs: at ta ck
- Cyphert.: rs sr ed

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



Rules for encryption using Playfair Cipher

- Example
- Plaintext: Mosque
- Digraphs: Mo sq ue
- Cyphert.: on ts ml

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



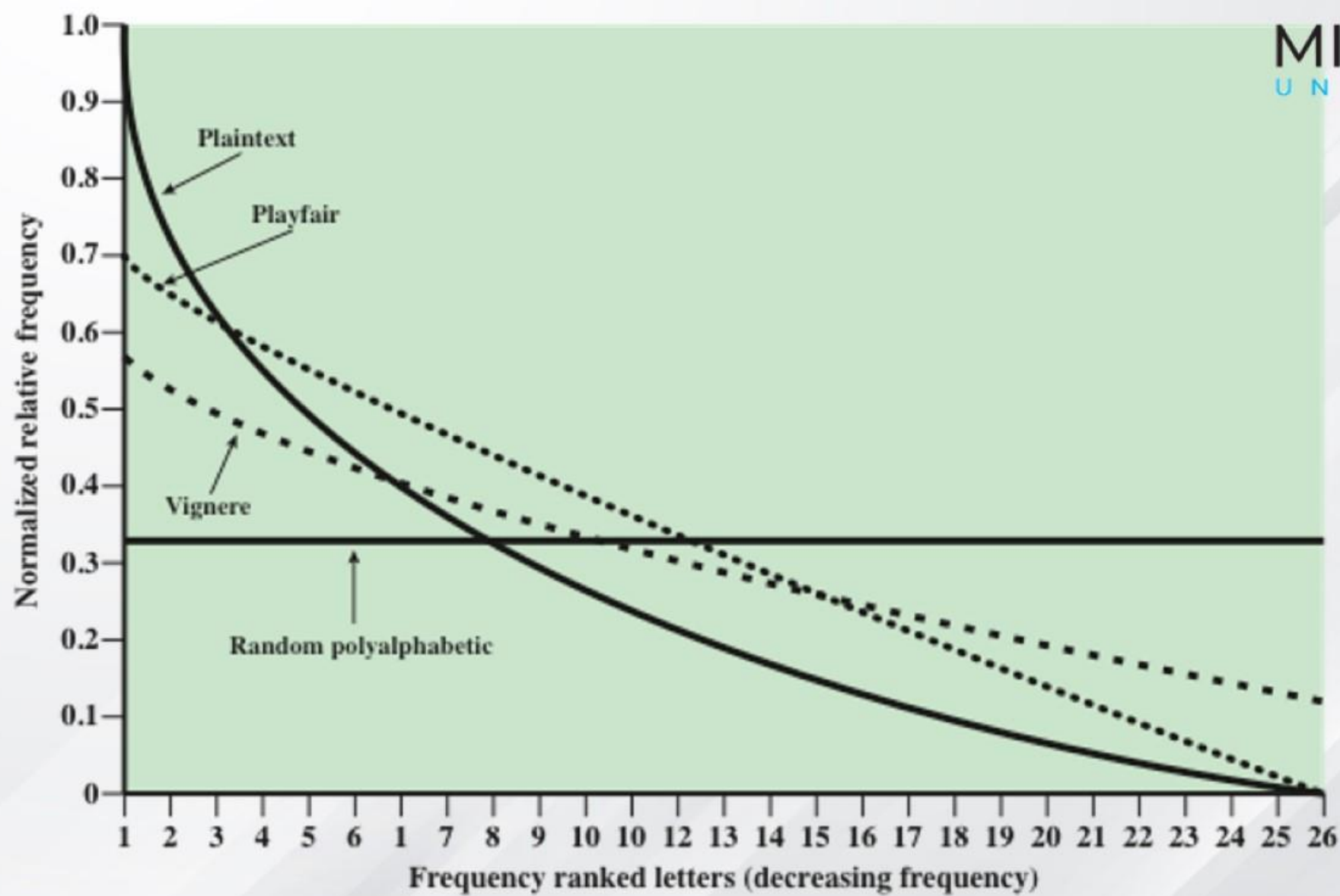


Figure 3.6 Relative Frequency of Occurrence of Letters



Hill Cipher

- Developed by the mathematician Lester Hill in 1929
- 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



Hill Cipher

- $C = E(K,P) = \mathbf{PK} \bmod 26$
- $P = D(K,C) = CK^{-1} \bmod 26 = \mathbf{PK} K^{-1} = P$

- $(C_1 \ C_2 \ C_3) = (P_1 \ P_2 \ P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$



Hill Cipher Example

Question: Encrypt "pay" using Hill cipher with key

Solution

p	a	y
15	0	24

17	17	5
21	18	21
2	2	19

$$(C_1 \ C_2 \ C_3) = (15, 0, 24) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \text{mode } 26$$

$$= (15*17 + 0*21 + 24*2 \quad 15*17 + 0*18 + 24*2 \quad 15*5 + 0*21 + 24*19) \text{ mod } 26$$

$$= (303 \ 303 \ 531) \text{ mod } 26$$

$$= (17 \ 17 \ 11)$$

$$= \text{RRL}$$



Hill Cipher Example

Question: decrypt "RRL" using Hill chipper with key

Solution

17	17	5
21	18	21
2	2	19

$$P = D(K,C) = C \times K^{-1} \bmod 26$$

$$(P_1 \ P_2 \ P_3) = \begin{pmatrix} 17 & 17 & 11 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$(P_1 \ P_2 \ P_3) = (15 \ 0 \ 24) = \text{pay}$$



Hill Cipher Example

Breaking the Cipher:

- Define matrices:
 - P = Matrix of plaintext pairs
 - C = Matrix of ciphertext pairs
- Equation:

$$C = P \cdot K$$

- If P is invertible, K can be determined:

$$\bullet K = P^{-1} \cdot C$$

- If P is not invertible, new plaintext-ciphertext pairs are needed to form an invertible P .



Polyalphabetic Ciphers

- Polyalphabetic substitution cipher
 - Improves on the simple monoalphabetic technique by using different monoalphabetic substitutions as one proceeds through the plaintext message

All these techniques have the following features in common:

- A set of related monoalphabetic substitution rules is used
- A key determines which particular rule is chosen for a given transformation



Vigenère Cipher

- Best known and one of the simplest polyalphabetic substitution ciphers
- In this scheme the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25
- Each cipher is denoted by a key letter which is the ciphertext letter that substitutes for the plaintext letter a



Example of Vigenère Cipher

- To encrypt a message, a key is needed that is as long as the message
- Usually, the key is a repeating keyword
- For example, if the keyword is *deceptive*, the message “we are discovered save yourself” is encrypted as:

key: deceptivedeceptivedeceptive

plaintext: wearediscoveredsaveyourself

ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ



Vigenère Autokey System

- Example:

key: deceptivewearediscoveredsav

plaintext: wearediscoveredsaveyourself

ciphertext: ZICVTWQNGKZEIIGASXSTSLVWVLA

Key	3	4	2	4	15	19	8	21	4	3	4	2	4
PT	22	4	0	17	4	3	8	18	2	14	21	4	17
CT	25	8	2	21	19	22	16	13	6	17	25	6	21

Key	15	19	8	21	4	3	4	2	4	15	19	8	21	4
PT	4	3	18	0	21	4	24	14	20	17	18	4	11	5
CT	19	22	0	21	25	7	2	16	24	6	11	12	6	9

Vigenère Autokey System

- 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



Vernam Cipher

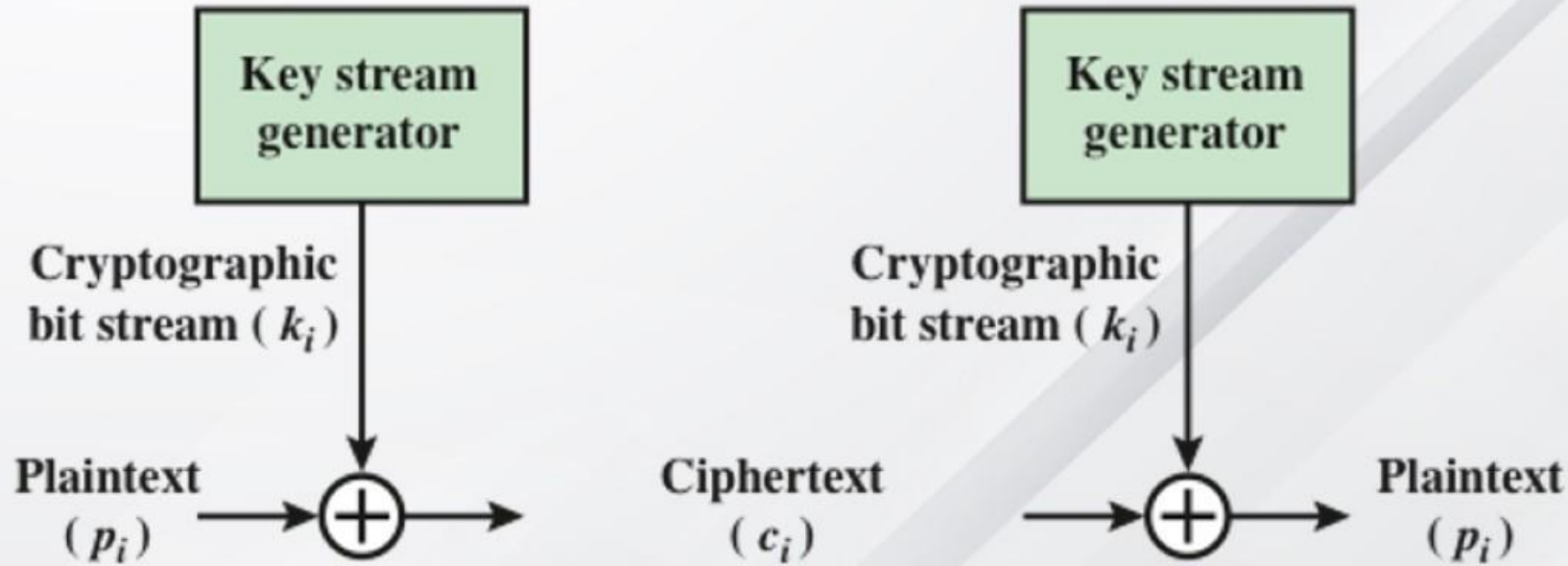


Figure 3.7 Vernam Cipher



One-Time Pad

- Improvement to Vernam cipher proposed by an Army Signal Corp officer, Joseph Mauborgne
- Use a random key that is as long as the message so that the key need not be repeated
- Key is used to encrypt and decrypt a single message and then is discarded
- Each new message requires a new key of the same length as the new message
- Scheme is unbreakable
 - Produces random output that bears no statistical relationship to the plaintext
 - Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code



Difficulties

- The one-time pad offers complete security but, in practice, has two fundamental difficulties:
 - There is the practical problem of making large quantities of random keys
 - Any heavily used system might require millions of random characters on a regular basis
 - Mammoth key distribution problem
 - For every message to be sent, a key of equal length is needed by both sender and receiver
- Because of these difficulties, the one-time pad is of limited utility
 - Useful primarily for low-bandwidth channels requiring very high security



Rail Fence Cipher



- Simplest transposition cipher
- Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows
- To encipher the message “meet me after the toga party” with a rail fence of depth 2, we would write:

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



Summary

- **Symmetric Cipher Model:**
 - Requires a strong encryption algorithm and secure key sharing.
- **Cryptographic Security:**
 - **Unconditionally secure:** Impossible to decrypt.
 - **Computationally secure:** Breaking it costs more than the encrypted data's value.
- **Substitution Ciphers:**
 - Caesar Cipher
 - Monoalphabetic Cipher
 - Playfair Cipher
 - Hill Cipher.
 - Vigenère Cipher
- **Transposition Ciphers:**
 - Rail Fence Cipher





Thank You

