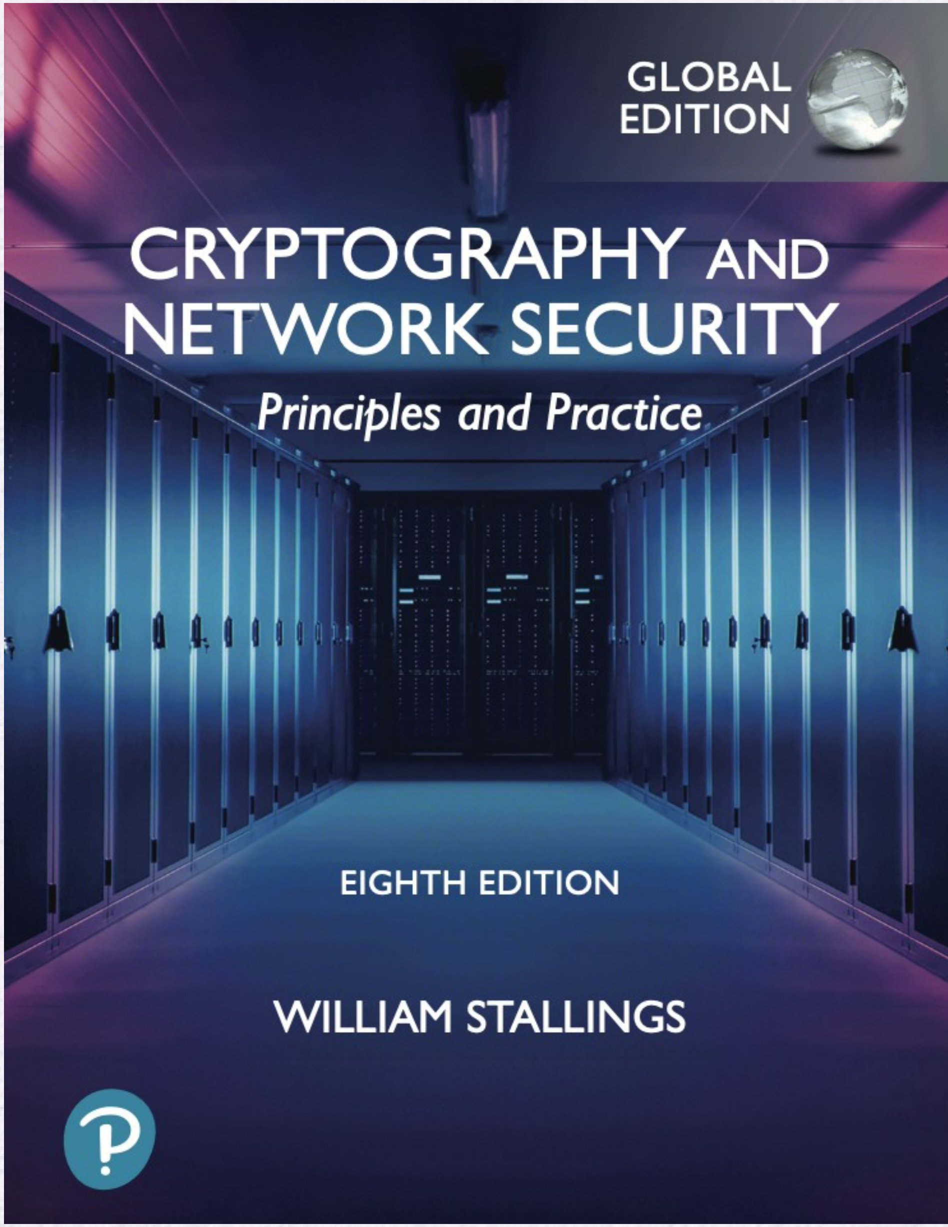
University of Nevada – Reno
Computer Science & Engineering Department

CS454/654 Reliability and Security of Computing Systems - Fall 2024

Lecture 4

Dr. Batyr Charyyev
bcharyyev.com



PART TWO: SYMMETRIC CIPHERS

CHAPTER 3

CLASSICAL ENCRYPTION TECHNIQUES

Symmetric Cipher Model

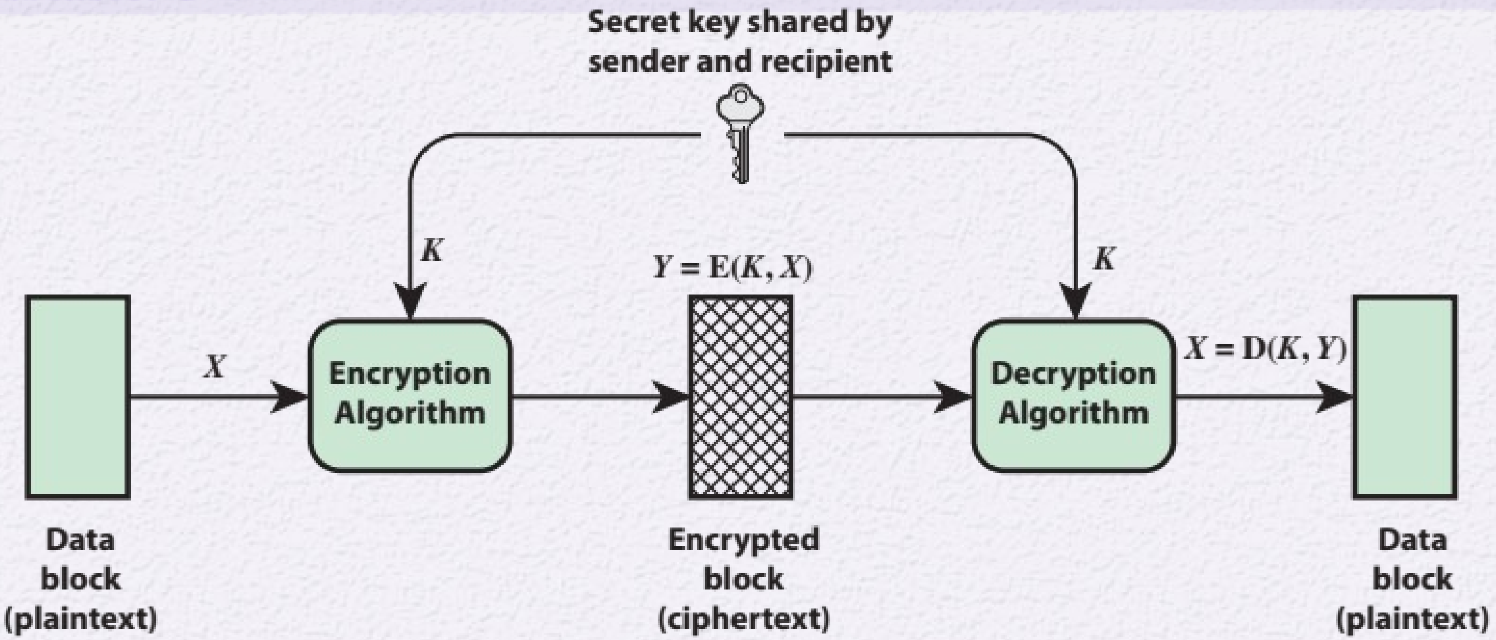
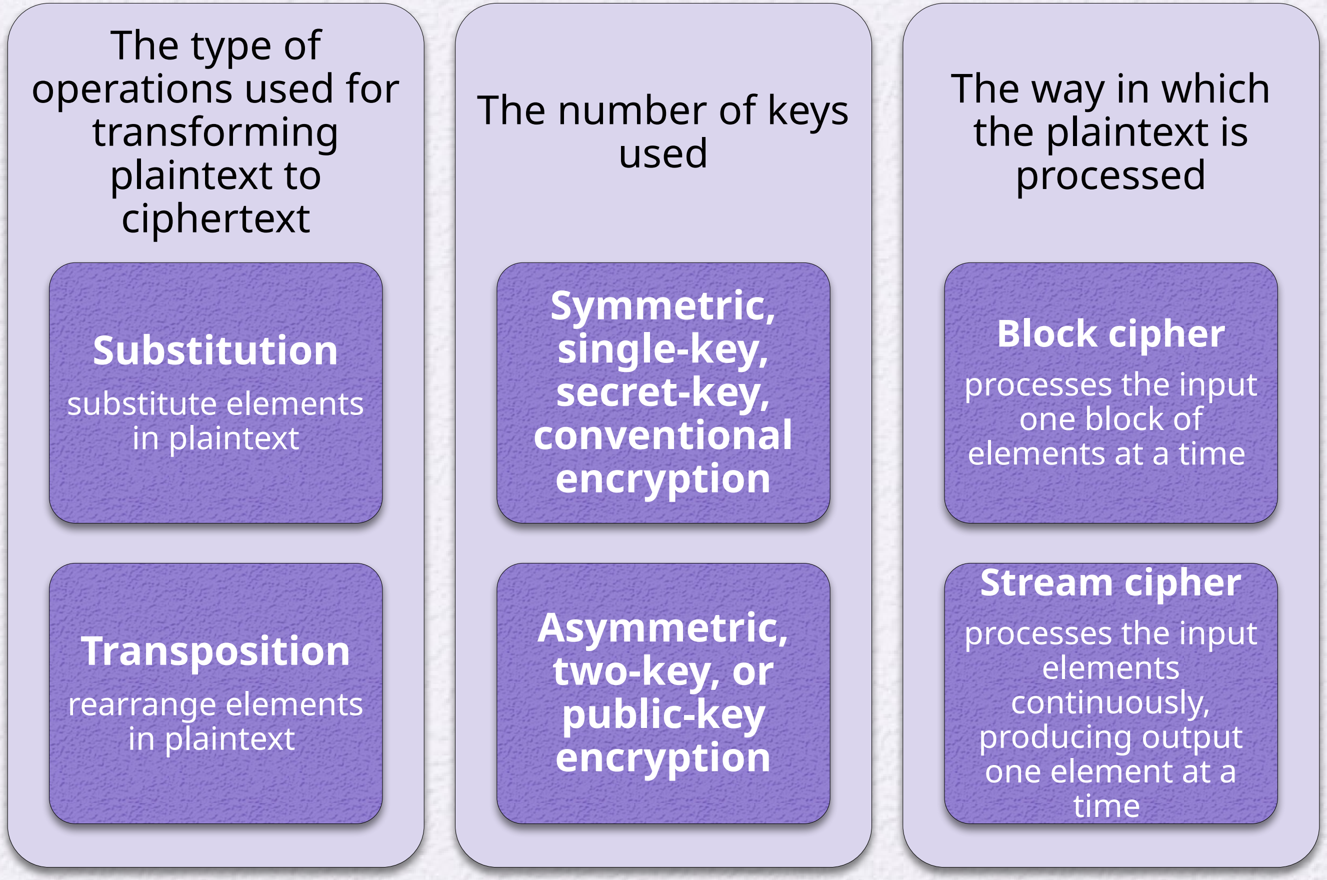


Figure 3.1 Simplified Model of Symmetric Encryption

- 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

Cryptographic Systems

- Characterized along three independent dimensions:



The type of operations used for transforming plaintext to ciphertext

Substitution

substitute elements in plaintext

Transposition

rearrange elements in plaintext

The number of keys used

Symmetric, single-key, secret-key, conventional encryption

Asymmetric, two-key, or public-key encryption

The way in which the plaintext is processed

Block cipher

processes the input one block of elements at a time

Stream cipher

processes the input elements continuously, producing output one element at a time

Most product systems involve multiple stages of substitutions and transpositions.

Cryptanalysis and Brute-Force Attack

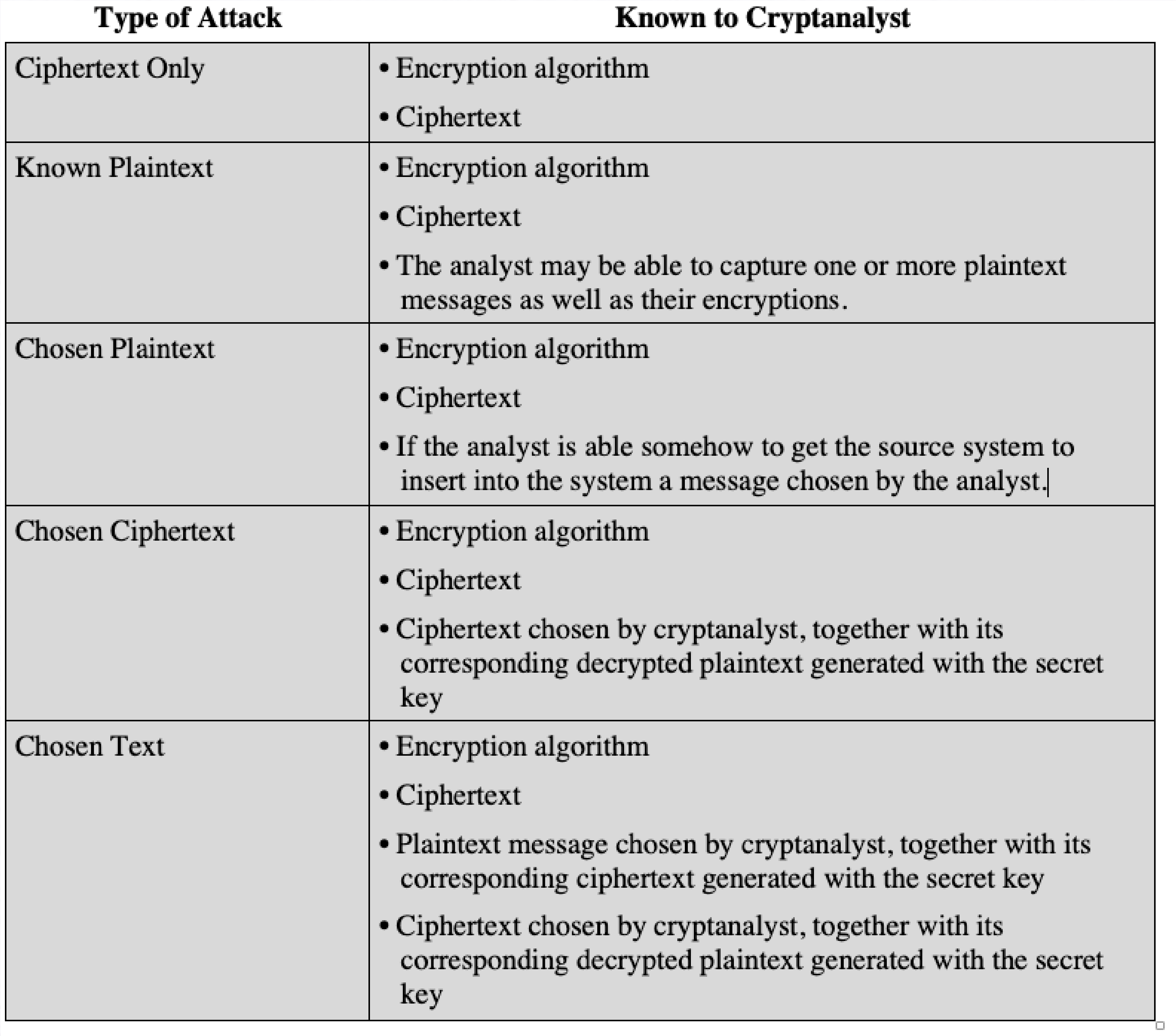
Cryptanalysis

- 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

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

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



Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • The analyst may be able to capture one or more plaintext messages as well as their encryptions.
Chosen Plaintext	• Encryption algorithm • Ciphertext • If the analyst is able somehow to get the source system to insert into the system a message chosen by the analyst.
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

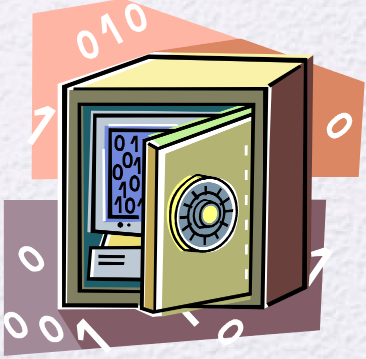
(Table is on page 68 in the textbook)

Encryption Scheme Security

- **Unconditionally secure**
  - No matter how much time and ciphertext an opponent has, it is impossible for him or her to decrypt the ciphertext.
  - With the exception of a scheme known as the one- time pad (described later in this chapter), there is no encryption algorithm that is unconditionally secure.

- **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



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
  - Appropriate choice of protocols
  - A well-engineered implementation
  - Absence of deliberately introduced hidden flaws

CHAPTER 3

CLASSICAL ENCRYPTION TECHNIQUES

Substitution Technique

- The letters (bits) of plaintext are replaced by other letters (bits) or by numbers or symbols

Substitution Techniques

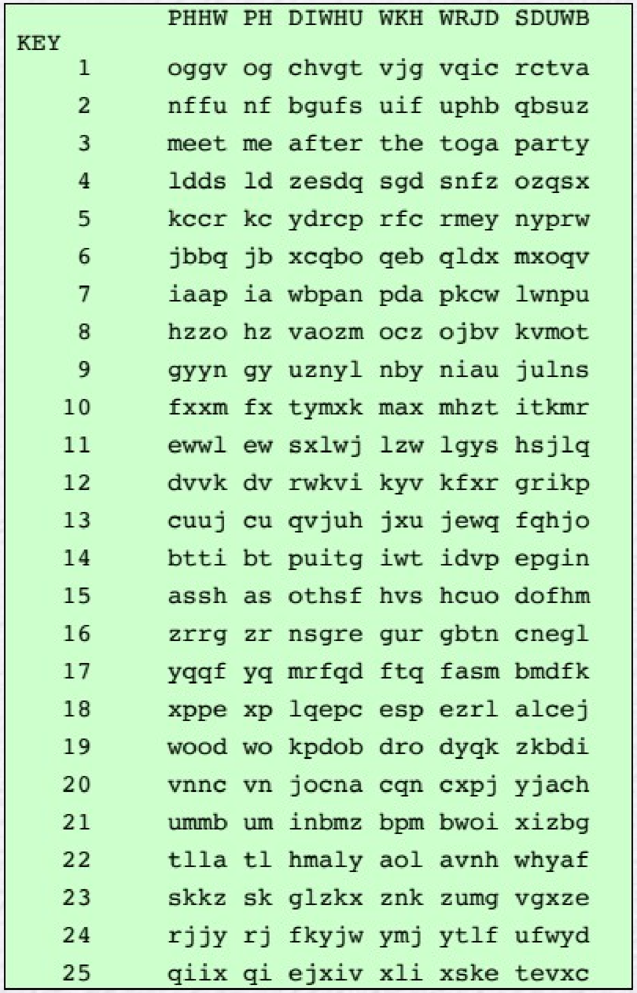
- Caesar Cipher
- Monoalphabetic Ciphers
- Playfair Cipher
- Hill Cipher
- Polyalphabetic Ciphers
- One-Time Pad

Caesar Cipher

- Simplest and earliest known use of a substitution cipher
- 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



KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic 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 ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv 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	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

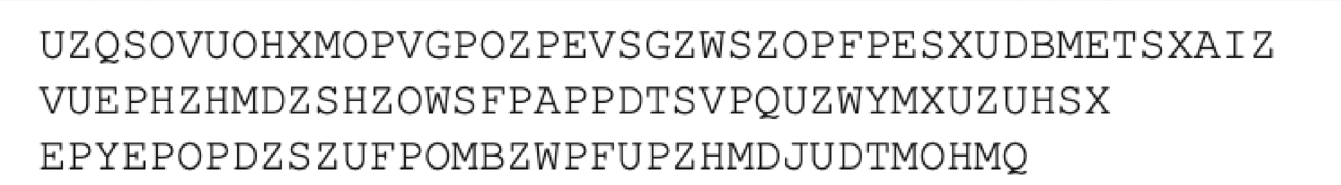
Figure 3.3 Brute-Force Cryptanalysis of Caesar Cipher

Monoalphabetic Cipher

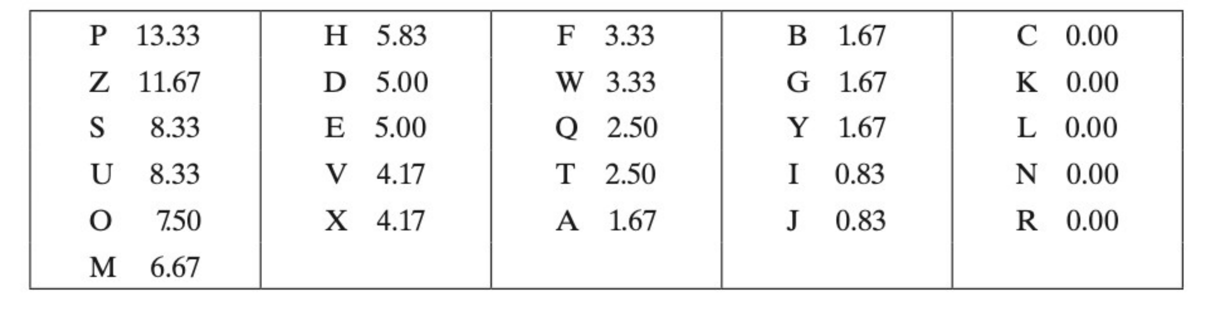
- Compared to Caesar Cipher, Monoalphabetic Cipher allows an arbitrary substitution.

- The cipher line can be any permutation of the 26 alphabetic characters
  - Q: How many possible keys?
  - 26! possible keys.

- Possible attack can be analyzing the relative frequency of letters, and compare it to frequency distribution for English.
  - Attacker should know the nature of plaintext (text is in English)
  - Should have long message to generate correct frequency distribution.



```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```



P	13.33	H	5.83	F	3.33	B	1.67	C	0.00
Z	11.67	D	5.00	W	3.33	G	1.67	K	0.00
S	8.33	E	5.00	Q	2.50	Y	1.67	L	0.00
U	8.33	V	4.17	T	2.50	I	0.83	N	0.00
O	7.50	X	4.17	A	1.67	J	0.83	R	0.00
M	6.67								

- P and Z are the equivalents of plain letters e and t

- The letters S, U, O, M, and H are all of relatively high frequency and probably correspond to plain letters from the set {a, h, i, n, o, r, s}

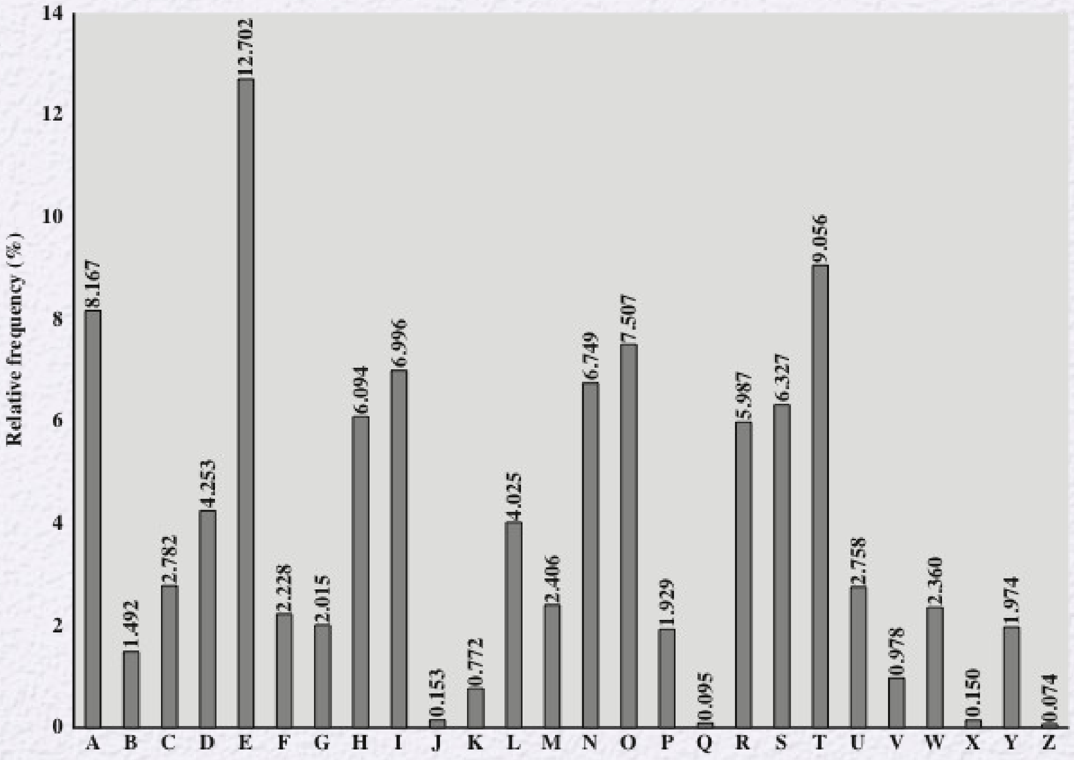
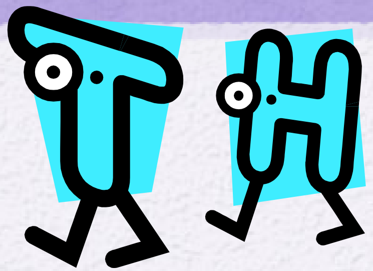
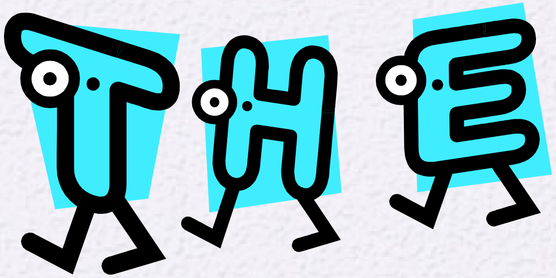


Figure 3.5 Relative Frequency of Letters in English Text

Monoalphabetic Ciphers



- Digram
  - Two-letter combination
  - Most common is *th*
  - In our ciphertext, the most common digram is ZW, which appears three times. So we make the correspondence of Z with t and W with h.



- Trigram
  - Three-letter combination
  - Most frequent is *the*
  - *ZWP is most frequent trigram thus we can assume P correspond to e*
- *Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.*

Playfair Cipher

- Best-known multiple-letter encryption cipher
- Treats digrams in the plaintext as single units and translates these units into ciphertext digrams
- 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 Key Matrix

Constructing 5x5 matrix from keyword.

1. Assume keyword is “jurisdiction”
2. Remove duplicates, keyword become “J U R I S D C T O N”
3. Treat I and J same, “J/I U R S D C T O N”
4. Fill the letters in keyword from left to right and then fill other letters in alphabetic order

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

Playfair Key Matrix

Plaintext is encrypted two letters at a time, according to the following rules:

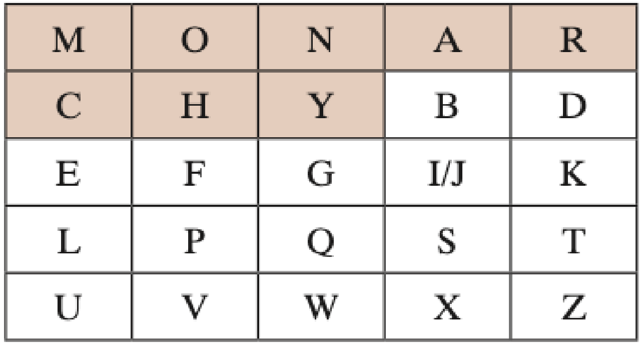
1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.
2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.
4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes). (Create rectangle).

Play pl ay => QP NB

Game ga me => IN CL

hell he lx lx =>CF SU SU

hello he lx lo =>CF SU PM



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

Substitution Technique

- The letters (bits) of plaintext are replaced by other letters (bits) or by numbers or symbols

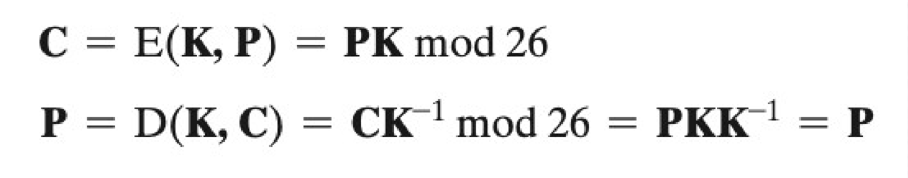
Substitution Techniques

- Caesar Cipher
- Monoalphabetic Ciphers
- Playfair Cipher
- Hill Cipher
- Polyalphabetic Ciphers
- One-Time Pad

Hill Cipher

- Take nxn (3x3, 2x2, etc.) matrix which should be invertible.

- Inverse M^{-1} of square matrix M is defined by the equation $M(M^{-1}) = (M^{-1})\ M = I$ where I is identity matrix.



$$\mathbf{C} = \mathrm{E}(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$$

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

Hill Cipher

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \quad \mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

$$\mathbf{C} = \mathrm{E}(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$$

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

Example: consider plaintext “paymoremoney” and use the encryption key above.

First three letters (pay) of the plaintext are represented by the vector (15 0 24)

Then (15 0 24) K = (303 303 531) mod 26 = (17 17 11) = RRL. And if we continue “paymoremoney” ->RRLMWBKASPDH

For decryption if we repeat the process for RRLMWBKASPDH with K^{-1} we get the ”paymoremoney”.

Substitution Technique

- The letters (bits) of plaintext are replaced by other letters (bits) or by numbers or symbols

Substitution Techniques

- Caesar Cipher
- Monoalphabetic Ciphers
- Playfair Cipher
- Hill Cipher
- Polyalphabetic Ciphers
- One-Time Pad

Polyalphabetic Ciphers

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

- Polyalphabetic Ciphers: Vigenere and Vernam

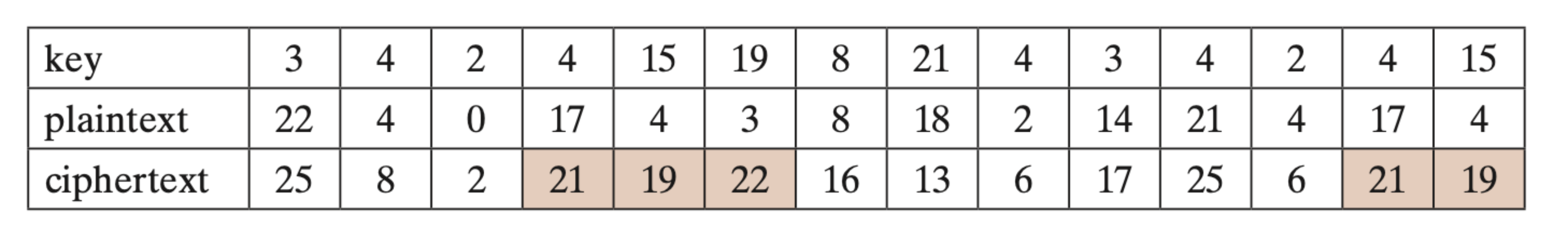
Vigenère Cipher

- 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

d+w=z   => (3+22) mod 26=25

Vigenère Cipher



key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

In the example, two instances of the sequence “red” are separated by nine character positions.

If the message is long enough, there will be a number of such repeated ciphertext sequences.

By looking for common factors in the displacements of the various sequences, the analyst should be able to make a good guess of the keyword length.

Vernam Cipher

Key can be shorter or equal to message, and can be reused.

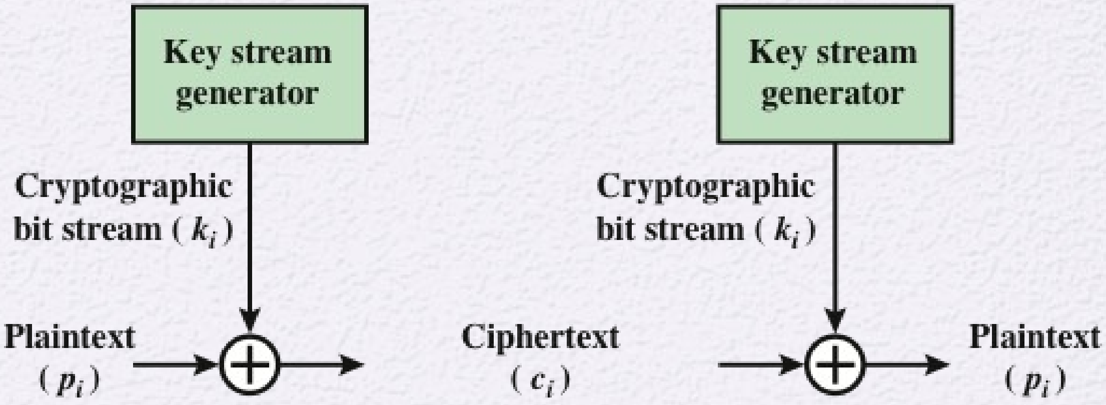
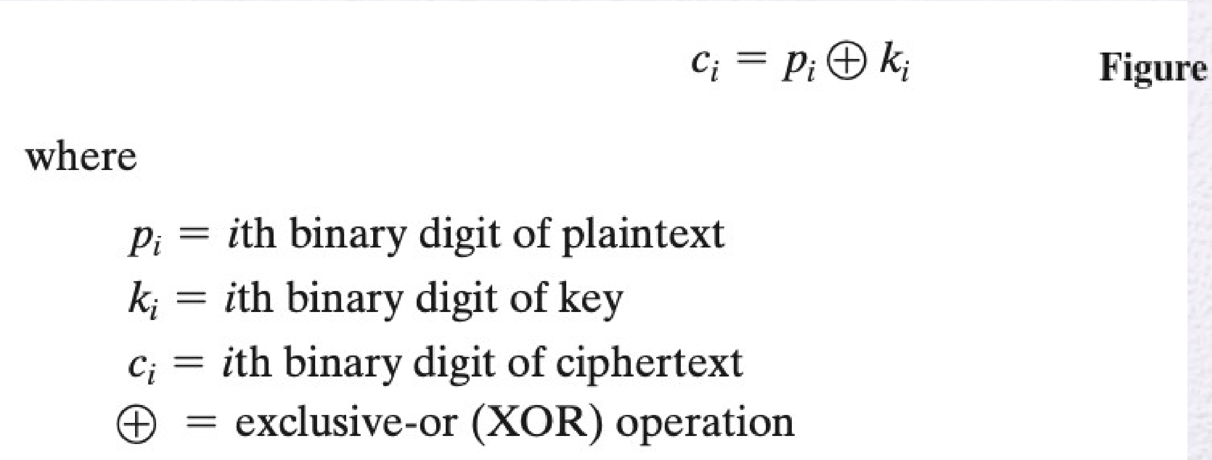


Figure 3.7 Vernam Cipher



$$c_i = p_i \oplus k_i$$

where

p_i = ith binary digit of plaintext

k_i = ith binary digit of key

c_i = ith binary digit of ciphertext

$\oplus$ = exclusive-or (XOR) operation

Key is just a random bits

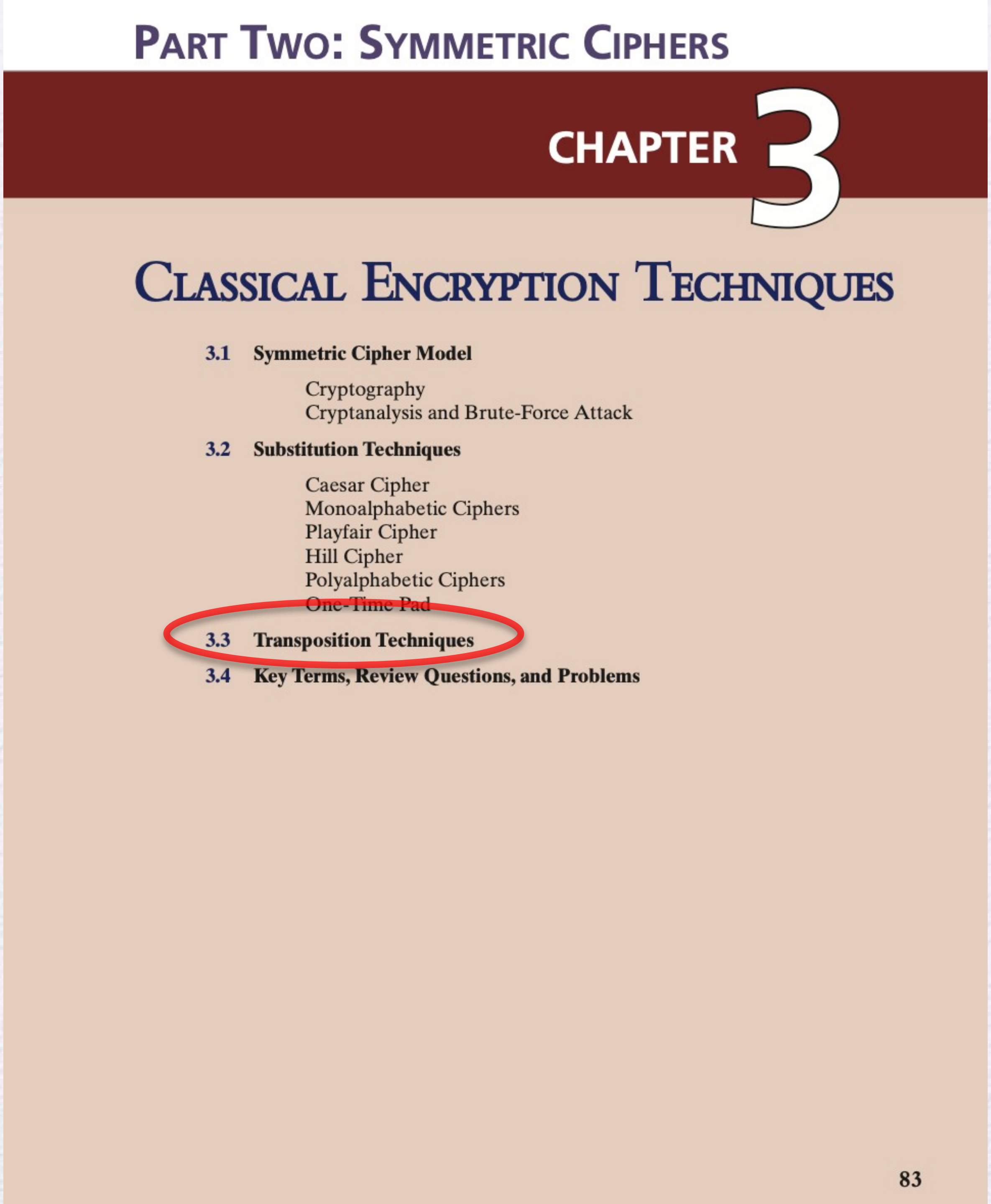
One-Time Pad

- 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
- Produces random output that bears no statistical relationship to the plaintext

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. Thus, distribution (exchanging) of keys is challenging.



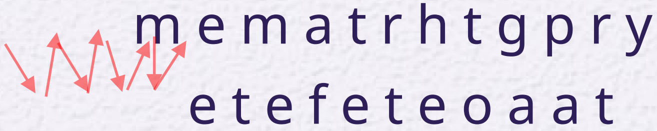
PART TWO: SYMMETRIC CIPHERS

CHAPTER 3

CLASSICAL ENCRYPTION TECHNIQUES

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

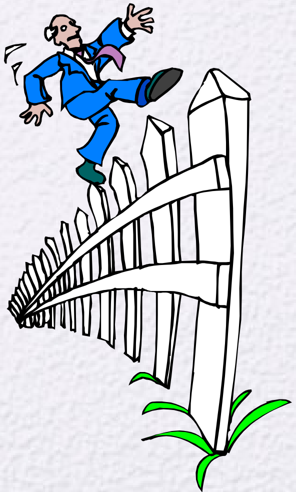
e t e f e t e o a a t

Encrypted message is:

MEMATRHTGPRYETEFETEOAAT

Q: What is key here?

The Depth: number of rows



Row Transposition Cipher

- Write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns
  - The order of the columns then becomes the key to the algorithm

Key:	4		3	1	2	5	6	7	
Plaintext:		a	t	t	a	c	k	p	
			o	s	t	p	o	n	e
			d	u	n	t	i	l	t
			w	o	a	m	x	y	z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

The transposition cipher can be made significantly more secure by performing more than one stage of transposition