Chapter Five
Crypto Concepts

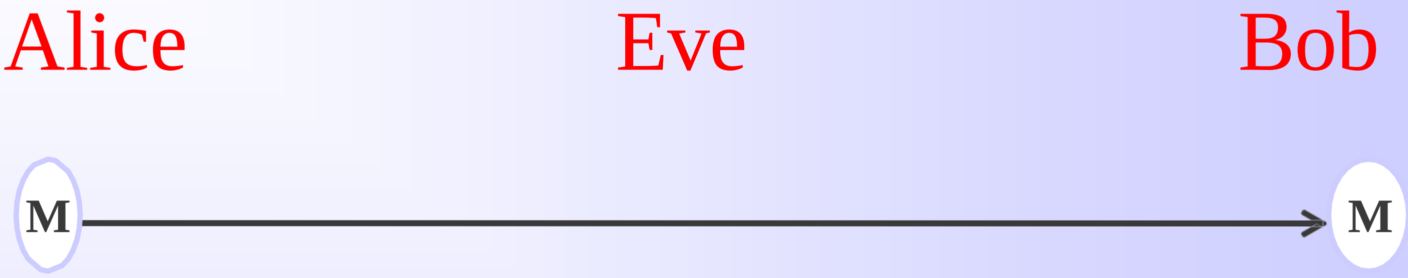
Outline

- What is cryptography?
- Application of cryptography
- Symmetric key cryptography
- Public Key Cryptography

Basic Security Properties (Revision)

- **Confidentiality:** to prevent unauthorized disclosure of the information
- **Integrity:** to prevent or detect unauthorized modification of the information
- **Authentication:** to prove the person/computer is who she/it claims to be (verify the identity of a user)
- **Availability:** to guarantee access to information
- **Privacy:** to prevent disclosure of personal information
- **Access control:** The limitation and control of access through identification and authentication.

Problem 1:Secure communication



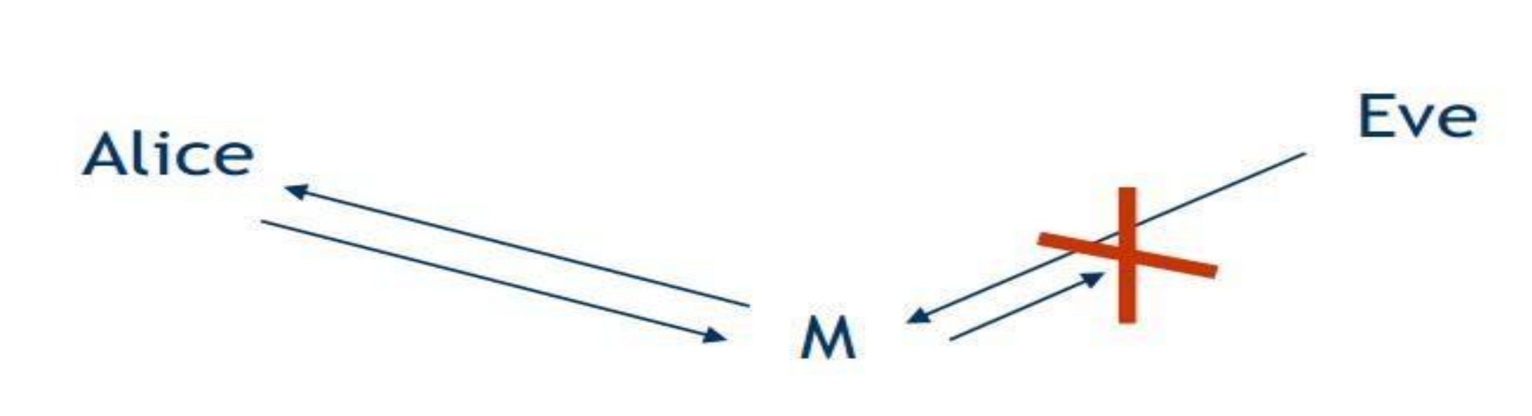
Alice Eve Bob

M M

Secure communication over unsecure channel

- **Secure channel :**an adversary does not have the ability to reorder, insert, or read.
- **Unsecure channel :** parties other than those for which the information is intended can reorder, delete, insert, or read.

Problem 2: Secure Storage



Secure storage on un-trusted hosts

- **Secure storage** one from which only authorized users can have access (read) to its information.
- **Un-trusted host (and storage)** one which unauthorized users can have access to with the intent to read, delete, modify protected information.

1-What is Cryptography?

- **Cryptography** is the science and study of secret writing (practice and study of hiding information)

A	D
B	E
C	F
...	...
X	A
Y	B
Z	C

Rotors
Lampboard
Keyboard
Plugboard
1001110111000100001101010111000010101 1010

- **Encryption** :is the process of converting data into meaningless form.
- **Decryption** :the translation of encrypted data into original text.

Crypto-analysis

- **Crypto-analysis**(from the Greek kryptós, "hidden", and analýein, "to loosen" or "to untie") is
  - The study of methods for obtaining the meaning of encrypted information without access to the secret key which is normally required to do so.
- Typically, this involves finding the secret key

2-Applications of Cryptography

1 File encryption

- „Files are stored in encrypted form on disk
- „Only owner and other authorized users has the secret key for decrypting the file

☞ Attacks on standard file protection:

- „Boot computer with a new operating system CD
- „Steal hard drive

2 Communication Encryption:

- Alice and Bob communicate over the internet
  - „Communication between browser and web server
  - „Remote shell connection

2-Applications of Cryptography…

3 **Digital right management :** refers to hardware and software systems providing access control for digital content (e.g., music and video files)

- **Encrypting music**
    - Software music players (e.g., iTunes) encrypt purchased songs
    - Songs are stored encrypted on disk and decryption keys stored within player which is shared with a limited number of trusted devices

4-E-cash

- Encryption is used in electronic money schemes to protect conventional transaction data like account numbers and transaction amounts.
- Digital signatures can replace handwritten signatures or a credit-card authorizations.

Cryptographic systems

- Cryptographic systems are generically classified along three independent dimensions.

1. Based on the type of operations used for transforming plaintext to ciphertext.
   - **Substitutions:** changing the plaintext one piece at a time.
   - **Transformations:** encrypt plaintext by moving small pieces of the message around.
   - Fundamental requirement is that no information be lost
2. Based on the number of keys used for encryption and decryption
   - **Using a single key for encryption and decryption**
     - Called Symmetric/Conventional encryption
     - The same key is used to encrypt and decrypt a message

       P = DK [EK (P)]

Cryptographic systems…

- **A pair of keys are used for encryption and decryption**
  - Called Asymmetric/Public key encryption
  - **keys for encryption and decryption are different but form a unique pair**
  - **$P = D_{KD} [E_{KE} (P)]$**
  - **Only one of the keys need to be private while the other can be public**

3. Based on the way in which the plaintext is processed

- **Stream cipher:** processes the input elements continuously, producing output one element at a time.
- **Block cipher:** processes the input one block of elements at a time, producing an output block for each input block.

Cryptosystem Elements

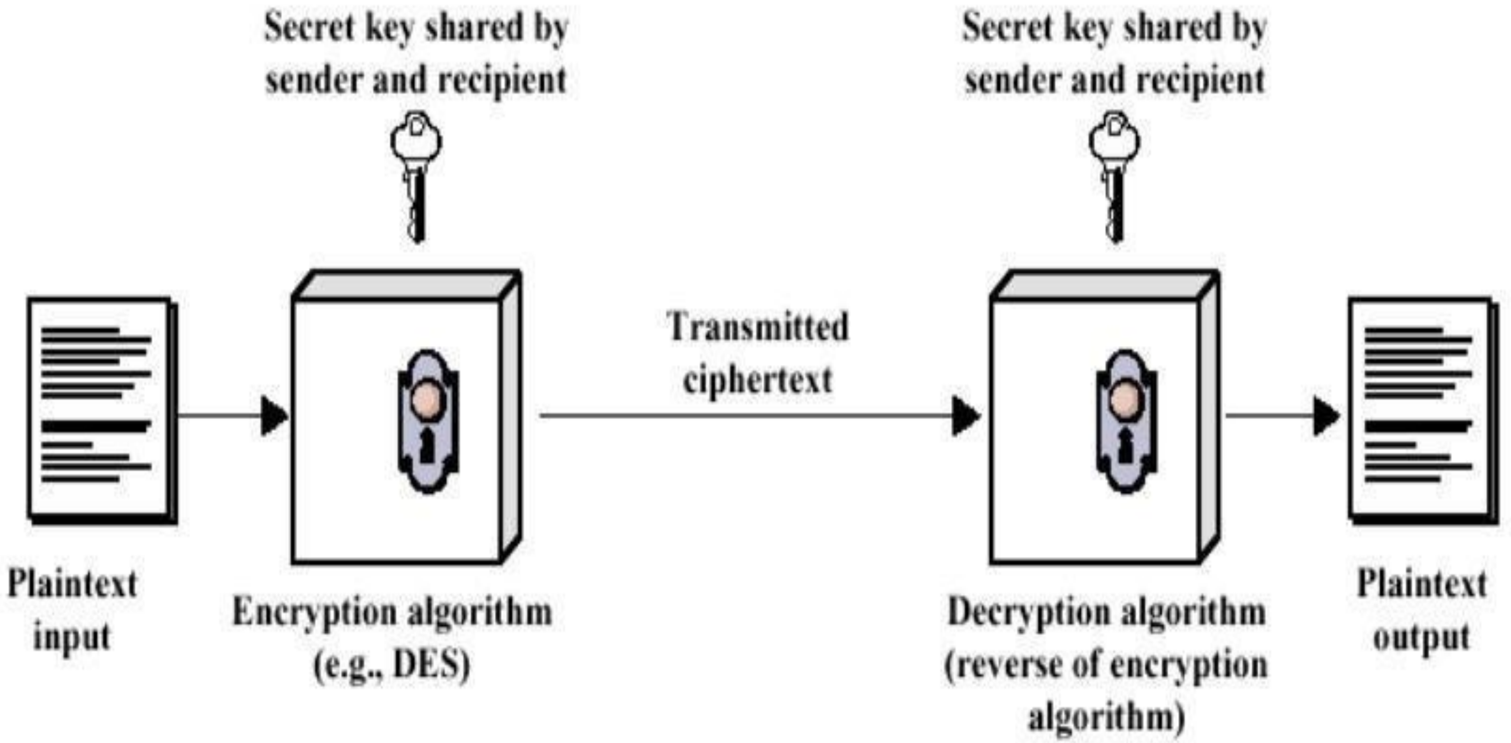
- **Quintuple(E, D, M, K, C)**
  - **M:**set of plaintexts
  - **K:**set of keys
  - **C:**set of ciphertexts
  - **E:**set of encryption functions
    - e: $M_xK \rightarrow C$
  - **D:**set of decryption functions
    - d: $C_xK \rightarrow M$

3- Symmetric / Conventional Encryption

- The only form of encryption prior to late 1970s
- **Plaintext:** The original message or data
- **Encryption algorithm:** Performs various substitutions and transformations on the plaintext.
  - **Substitutions:** changing the plaintext one piece at a time.
  - **Transformations:** encrypt plaintext by moving small pieces of the message around.
- **Secret key:** Input to the encryption algorithm.
- **Ciphertext:** Scrambled message produced as output.
  - Depends on the plaintext and the secret key
- **Decryption algorithm:** Encryption algorithm run in reverse.
  - Uses ciphertext and the secret key to produce the original plaintext

Symmetric Encryption Cont..

Simplified Encryption Model:


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

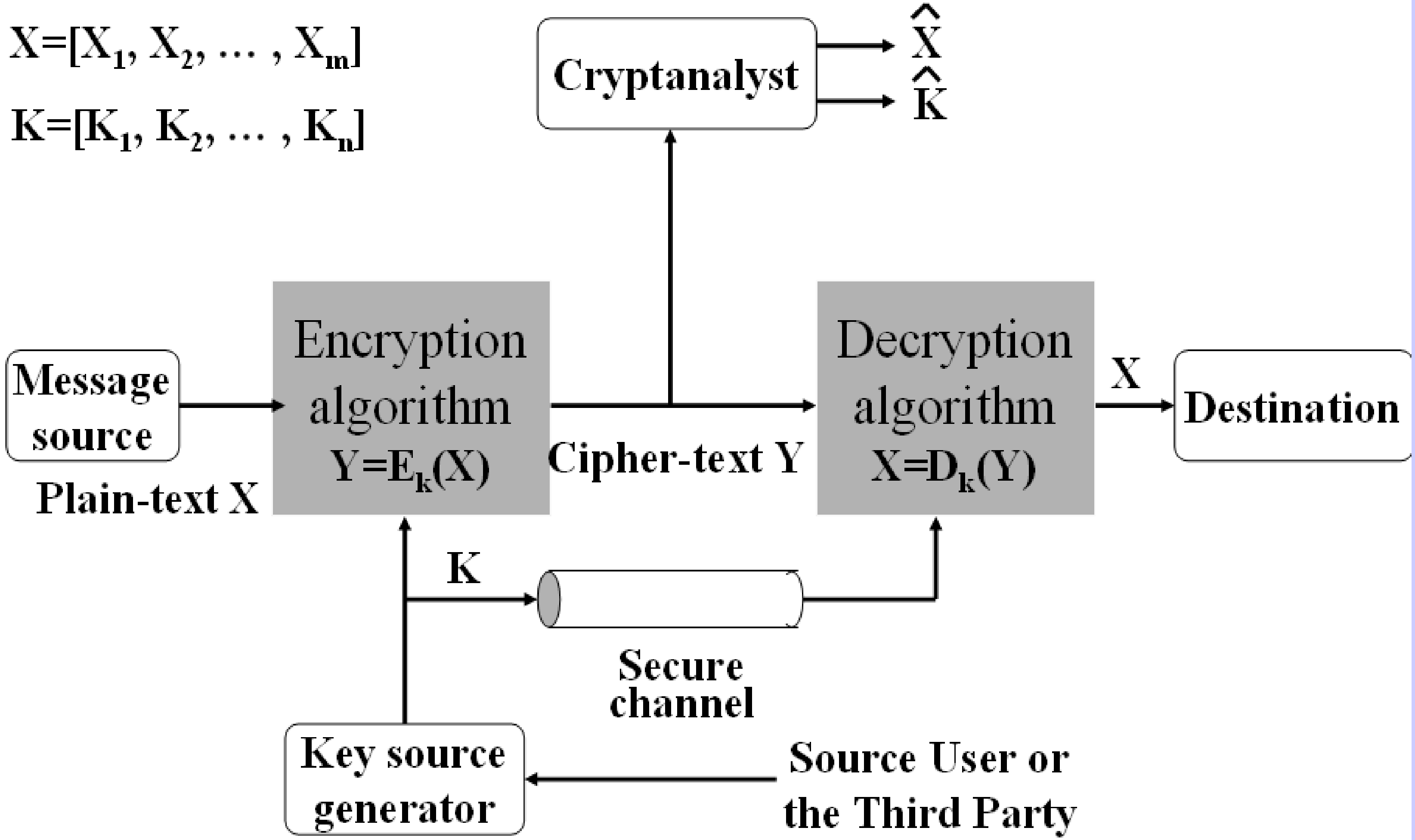
Enc(plaintext, key)=ciphertext

Dec(ciphertext, key)=plaintext

Symmetric Encryption Cont..

$X=[X_1, X_2, \ldots , X_m]$

$K=[K_1, K_2, \ldots , K_n]$



Symmetric Encryption Cont..

- A source produces a message in plaintext, $X = [x_1, x_2, \ldots, x_M]$
- The M elements of X are letters in some finite alphabet.
- For encryption, a key of the form $K = [K_1, K_2, \ldots, K_J]$ is generated.
  - The key should be provided to receiver by means of some secure channel.
  - The third party can generate and securely deliver the key for both.

Symmetric Encryption Cont..

- With the message and the encryption key as input, the encryption algorithm forms the ciphertext $Y = [Y_1, Y_2, \ldots, Y_N]$

  $Y = E_K(X)$, where Y is ciphertext, E is encryption algorithm.
- Receiver inverts $X = D_K(Y)$, where D is decryption algorithm.
- An opponent attempts to recover X or K or both.

Attacks on Symmetric encryption

- Objective of an attack is to recover the key in use rather than simply to recover the plaintext of a single ciphertext.

- There are two general approaches to attacking a conventional encryption scheme:

a) **Cryptanalysis:** rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs.

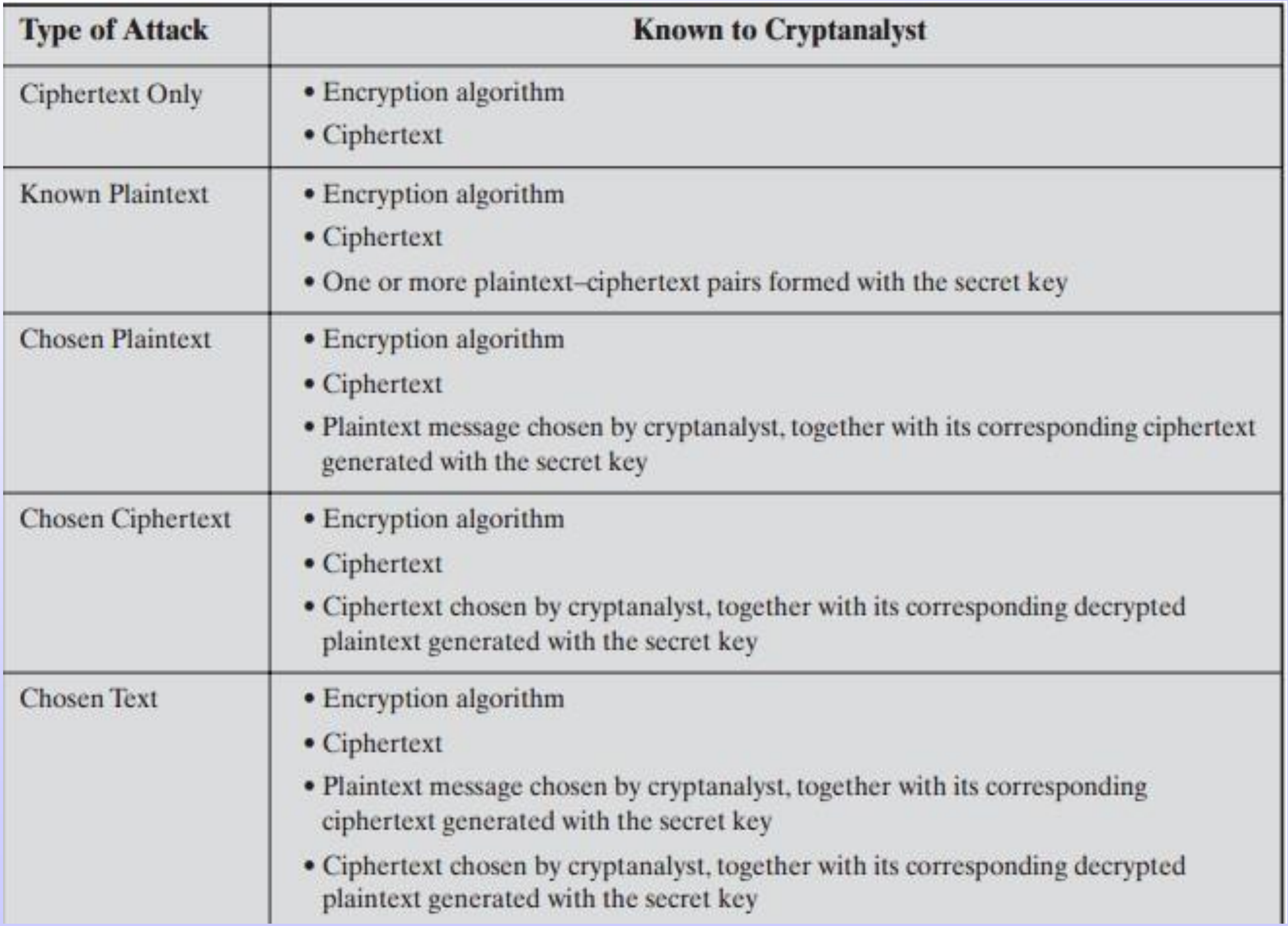
  - Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

Attacks on Symmetric encryption

b) Brute-force attack: The 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.

Crytoanalysis attack



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

- Only relatively weak algorithms fail to withstand a known plaintext attack.
- Generally an encryption algorithm is designed to withstand a known-plaintext attack.
- An encryption algorithm meets one or both of the following:
  - 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.

- An encryption scheme is:
  - **Unconditionally secure**
    - If the ciphertext generated does not contain enough information to determine uniquely the corresponding plaintext.
    - The required information doesn’t exist.
    - Except **one-time pad** scheme, there is no encryption algorithm that is unconditionally secure.
  - **Computationally secure**
    - The amount of cost and time exceeds the value and lifetime of the information required to cryptanalyze ciphertext successfully.

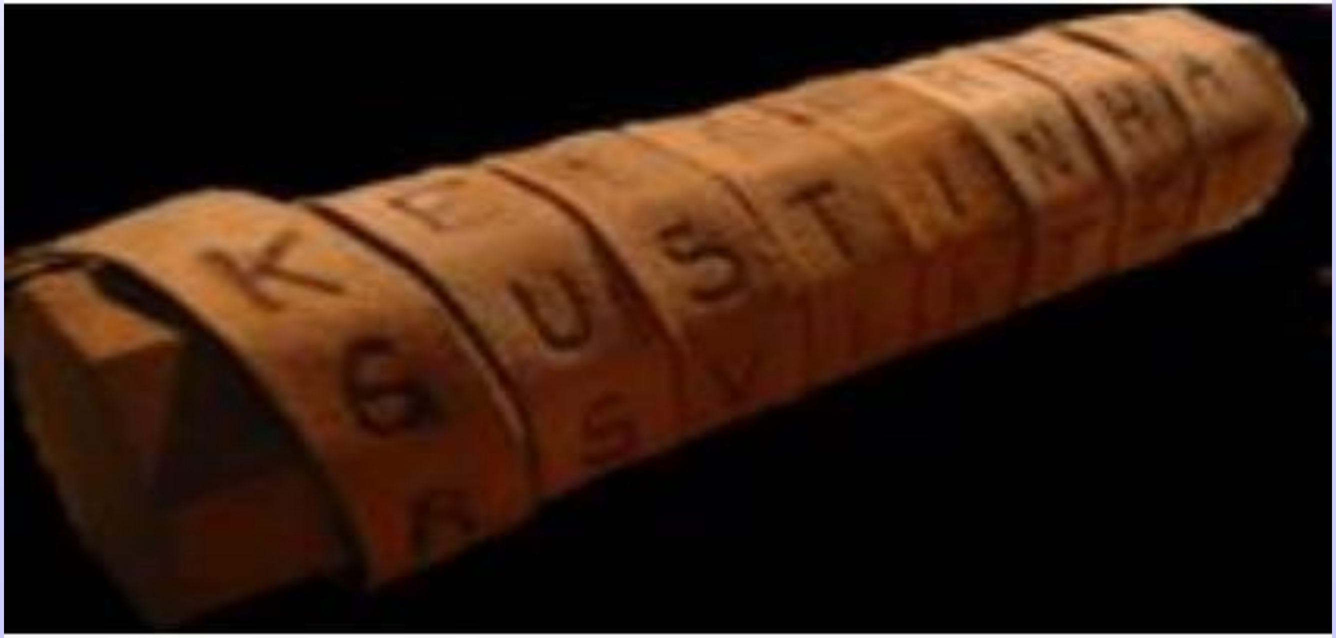
Substitution and transposition techniques

1. Substitution techniques
   - Letters of plaintext are replaced by other letters or by numbers or symbols.
2. Transposition Techniques
   - Performing some sort of permutation on the plaintext letters.

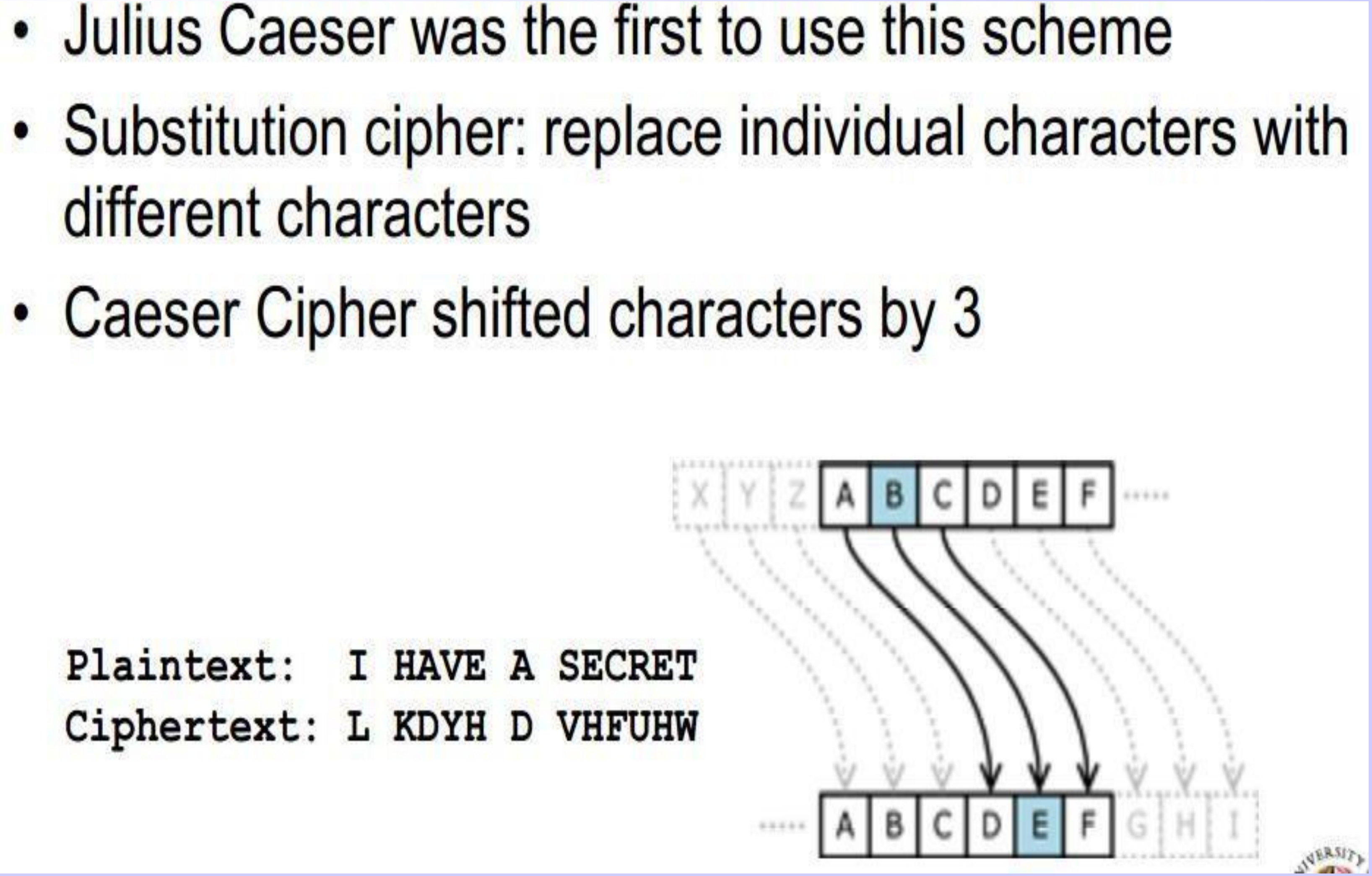
A-Substitution Techniques

i) Spartan SCYTALE (c 500 B.C.)

- It was used by the Spartan Military for encoding message sent between commanders.



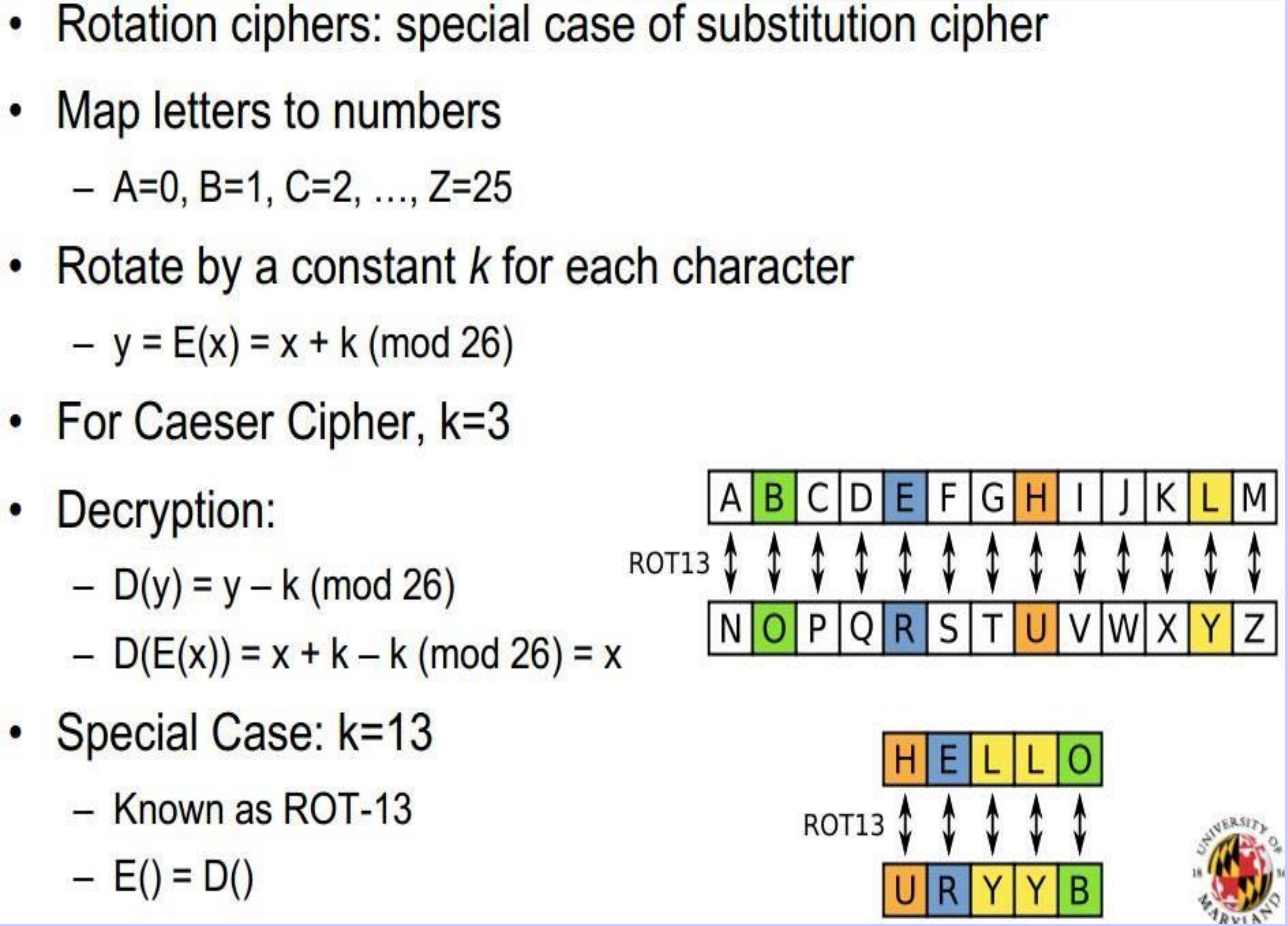
ii) CEASAR Cipher



- Julius Caeser was the first to use this scheme
- Substitution cipher: replace individual characters with different characters
- Caeser Cipher shifted characters by 3

Plaintext: I HAVE A SECRET
Ciphertext: L KDYH D VHFUHW

ii) CEASAR Cipher…



- Rotation ciphers: special case of substitution cipher
- Map letters to numbers
  - A=0, B=1, C=2, …, Z=25
- Rotate by a constant *k* for each character
  - y = E(x) = x + k (mod 26)
- For Caeser Cipher, k=3
- Decryption:
  - D(y) = y – k (mod 26)
  - D(E(x)) = x + k – k (mod 26) = x
- Special Case: k=13
  - Known as ROT-13
  - E() = D()

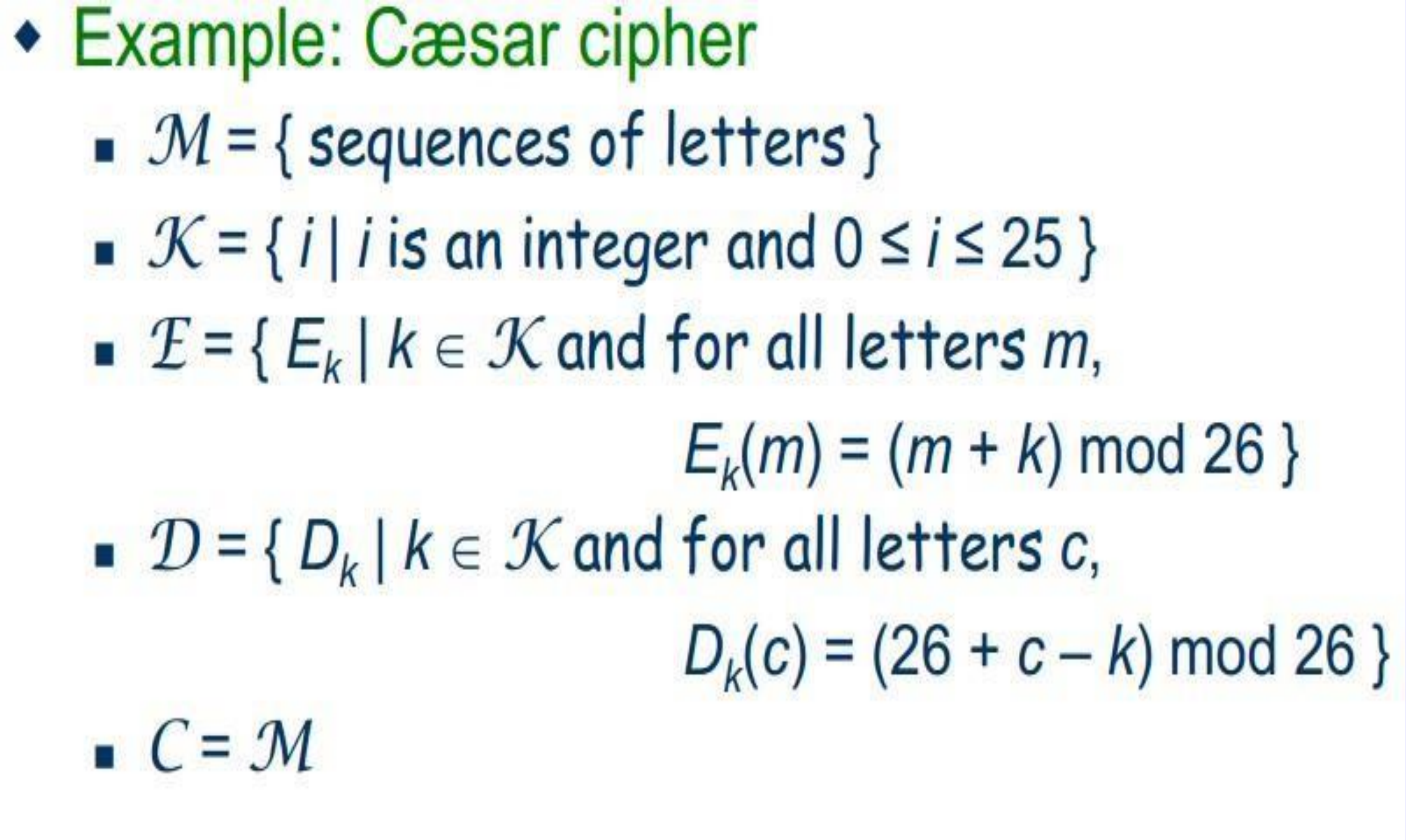
ROT13

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

ROT13

H	E	L	L	O
U	R	Y	Y	B

ii-CEASAR Algorithm

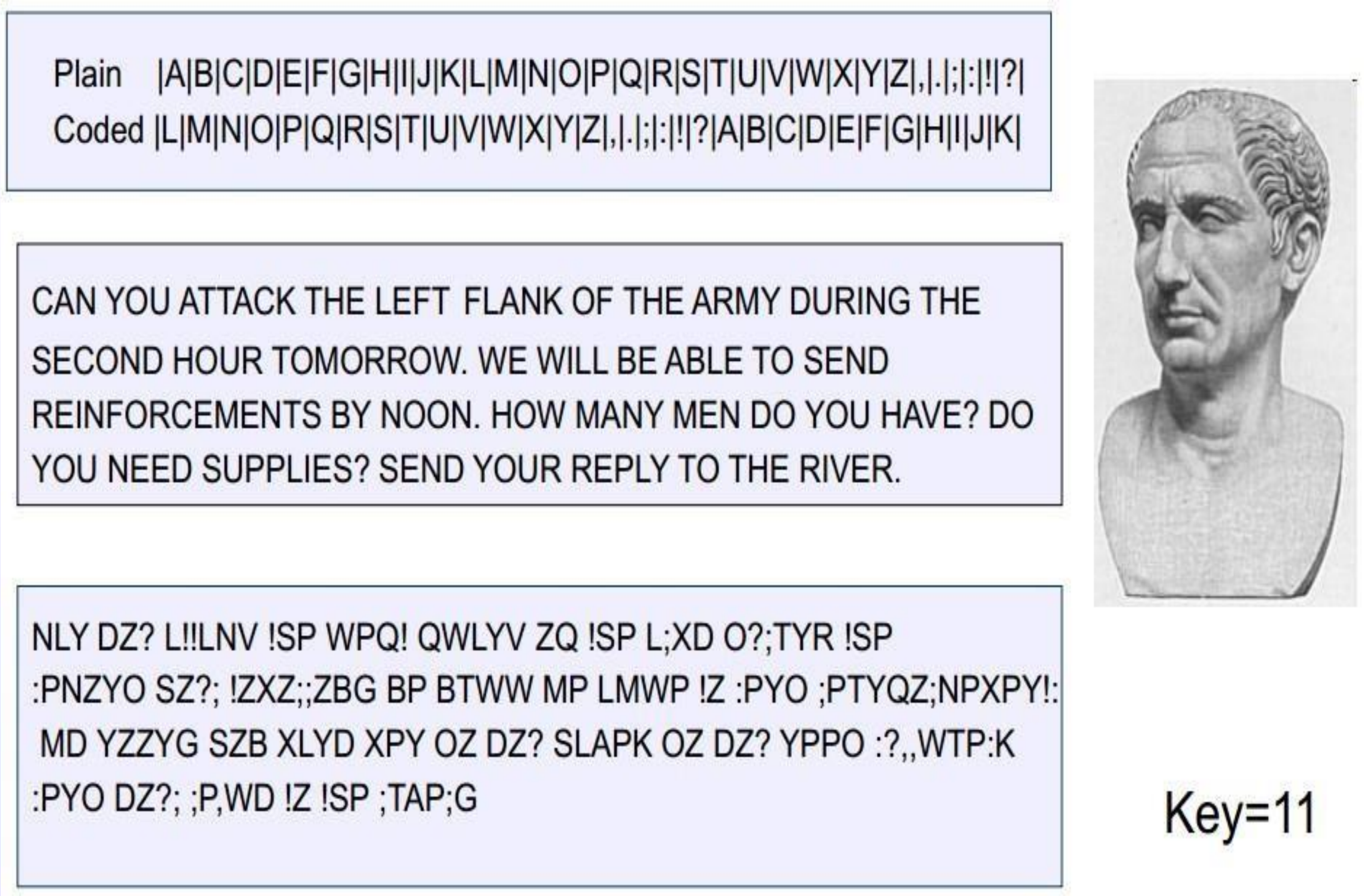


- Example: Cæsar cipher
  - $\mathcal{M} = \{$ sequences of letters $\}$
  - $\mathcal{K} = \{ i \mid i$ is an integer and $0 \leq i \leq 25 \}$
  - $\mathcal{E} = \{ E_k \mid k \in \mathcal{K}$ and for all letters m,

    $E_k(m) = (m + k) \bmod 26 \}$
  - $\mathcal{D} = \{ D_k \mid k \in \mathcal{K}$ and for all letters c,

    $D_k(c) = (26 + c - k) \bmod 26 \}$
  - $\mathcal{C} = \mathcal{M}$

Example



Plain	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	,	.	;	:	!	?
Coded	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	,	.	;	:	!	?	A	B	C	D	E	F	G	H	I	J	K

CAN YOU ATTACK THE LEFT FLANK OF THE ARMY DURING THE SECOND HOUR TOMORROW. WE WILL BE ABLE TO SEND REINFORCEMENTS BY NOON. HOW MANY MEN DO YOU HAVE? DO YOU NEED SUPPLIES? SEND YOUR REPLY TO THE RIVER.

NLY DZ? L!!LNV !SP WPQ! QWLYV ZQ !SP L;XD O?;TYR !SP :PNZYO SZ?; !ZXZ;;ZBG BP BTWW MP LMWP !Z :PYO ;PTYQZ;NPXPY!: MD YZZYG SZB XLYD XPY OZ DZ? SLAPK OZ DZ? YPPO :?,,WTP:K :PYO DZ?; ;P,WD !Z !SP ;TAP;G

Key=11

ii-CEASAR’s Problem

- Key is too short, can be found by exhaustive search.
- Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet
- Countermeasure
  - Homophonic Cipher-provide multiple substitutes for a single character.
  - Polyalphabetic cipher-change the substitution pattern (key) on a character basis

iii-Playfair Cipher

- Best-known multiple-letter encryption
- Algorithm is based on the use of a 5 x 5 matrix of letters
- Constructed by using keyword
- Example

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

iii-Playfair Cipher …

- The keyword is monarchy.
- The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order.
- The letters I and J count as one letter.

iii-Playfair Cipher-Encryption

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

☞ 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.

iii-Playfair Cipher-Encryption

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

Example, **MU** is encrypted as **CM**.

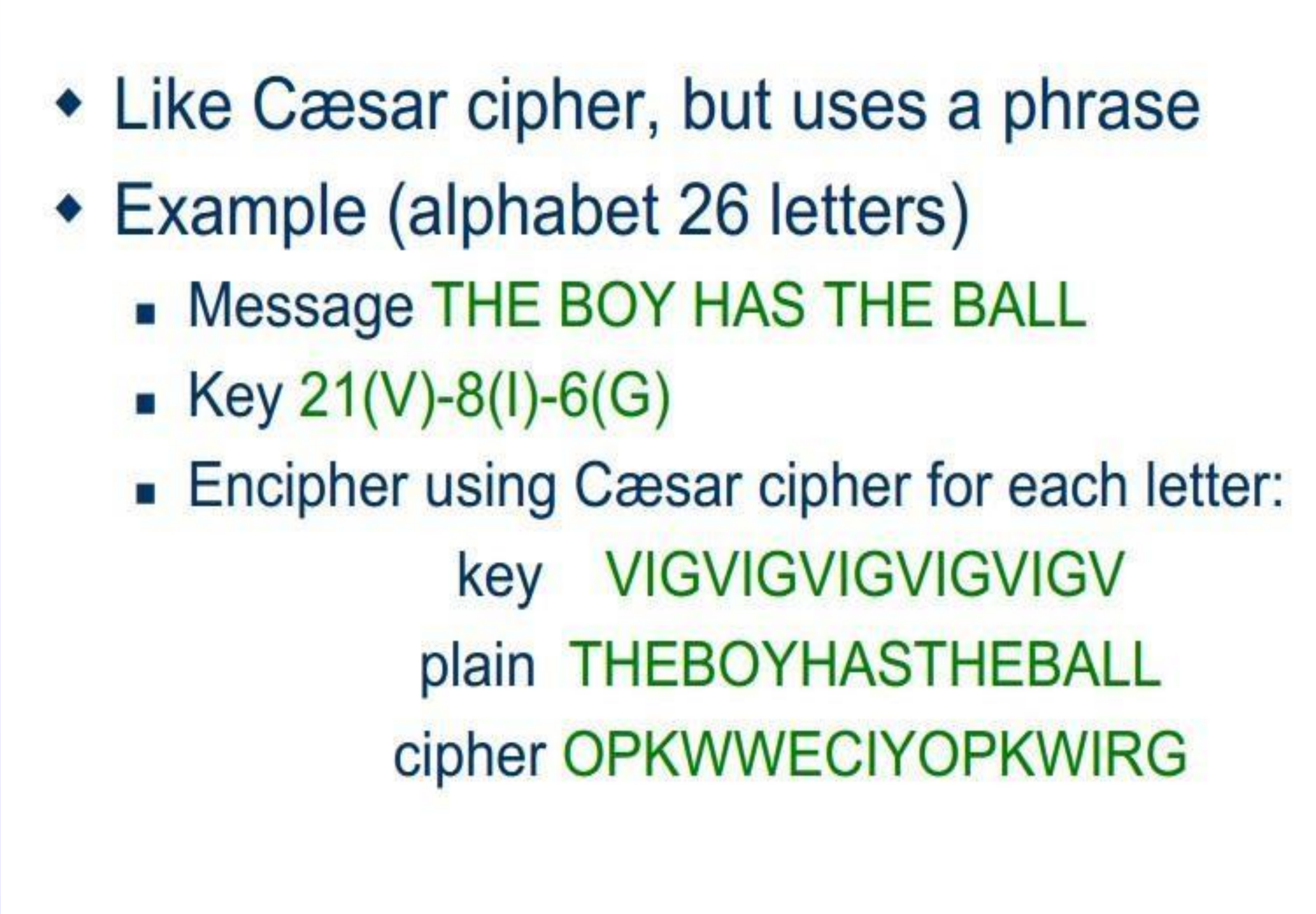
4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

Example. HS becomes BP and ea becomes IM (or JM, as the encipherer wishes).

iii-Playfair Cipher …

- Great advancement over monoalphabetic cipher.
- There are about 26 x 26 = 676 diagrams.
- More difficult to identify individual diagrams and relative frequencies of letters, so the playfair cipher was unbreakable for a long.

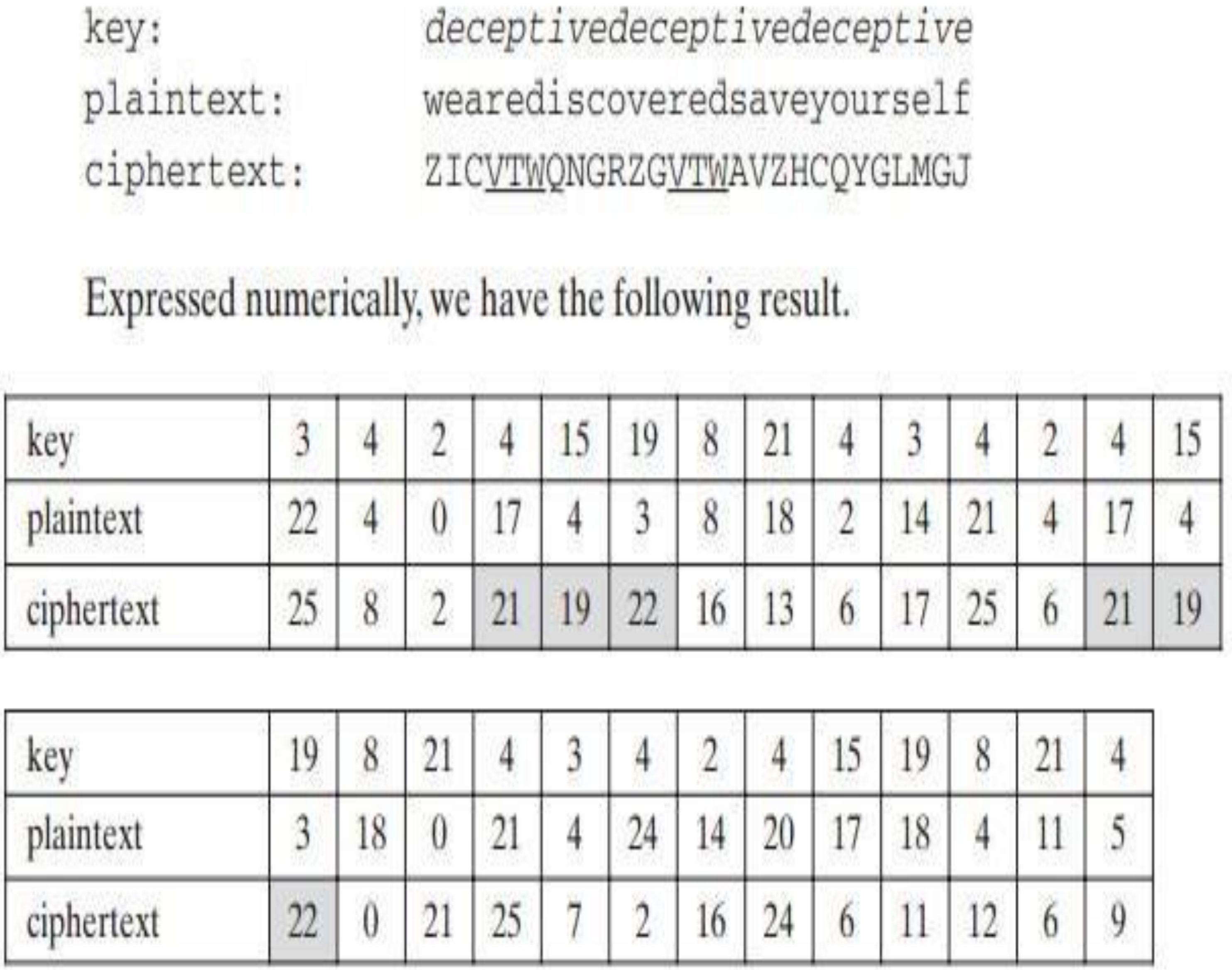
iv-Vigènere Cipher



- Like Cæsar cipher, but uses a phrase
- Example (alphabet 26 letters)
  - Message THE BOY HAS THE BALL
  - Key 21(V)-8(I)-6(G)
  - Encipher using Cæsar cipher for each letter:

key VIGVIGVIGVIGVIGV
plain THEBOYHASTHEBALL
cipher OPKWWECIYOPKWIRG

iv-Vigènere Cipher-Example



key:	*deceptivedeceptivedeceptive*
plaintext:	wearediscoveredsaveyourself
ciphertext:	ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Expressed numerically, we have the following result.

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

key	19	8	21	4	3	4	2	4	15	19	8	21	4
plaintext	3	18	0	21	4	24	14	20	17	18	4	11	5
ciphertext	22	0	21	25	7	2	16	24	6	11	12	6	9

iv-Cryptanalysis of Vigenere

- On polyalphabetic ciphers we need
  - Number of alphabets used
  - Key for each one
- Cryptanalysis is harder since it is not only a matters to check how the frequency has shifted

iv’-One-time Pad

- A Vigenère cipher with a random key at least as long as the message so that the key need not be repeated.
- Probably unbreakable
- Why?

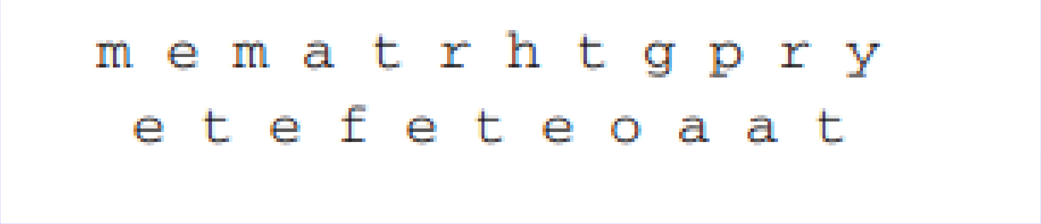
  Look at ciphertext DXQR. Equally likely to correspond to plaintext DOIT (key AJIY) and to plaintext DONT (key AJDY) and any other 4 letters.
- The key is to be used to encrypt and decrypt a single message, and then is discarded.

iv’-One-time Pad …

- **Warning:** keys must be random, or you can attack the cipher by trying to regenerate the key
- Very large number of alphabets: one time pad (large non-repeating keys on a pad)
- Each different, each used once and discarded
- **Problems:** Printing, distribution, storage

B-Transposition Techniques

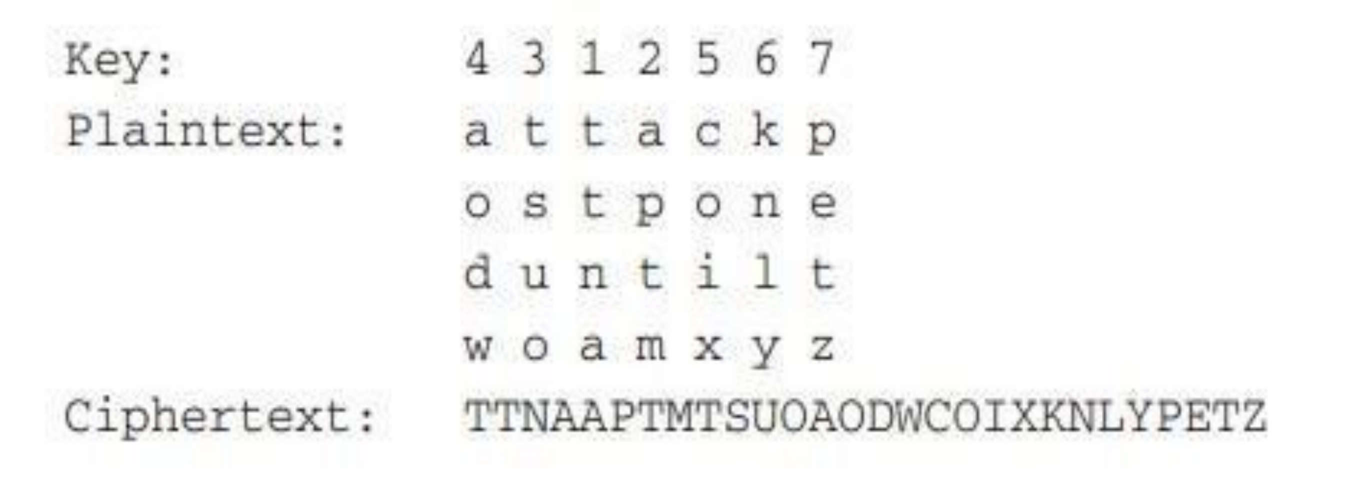
- Performing some sort of permutation on the plaintext letters.
- The simplest such cipher is the **rail fence** technique
- ***Plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.***
- Example with **k=2.**
- Plaintext: *“meet me after the toga party”*
- Encryption using railfence cipher



```
m e m a t r h t g p r y
 e t e f e t e o a a t
```

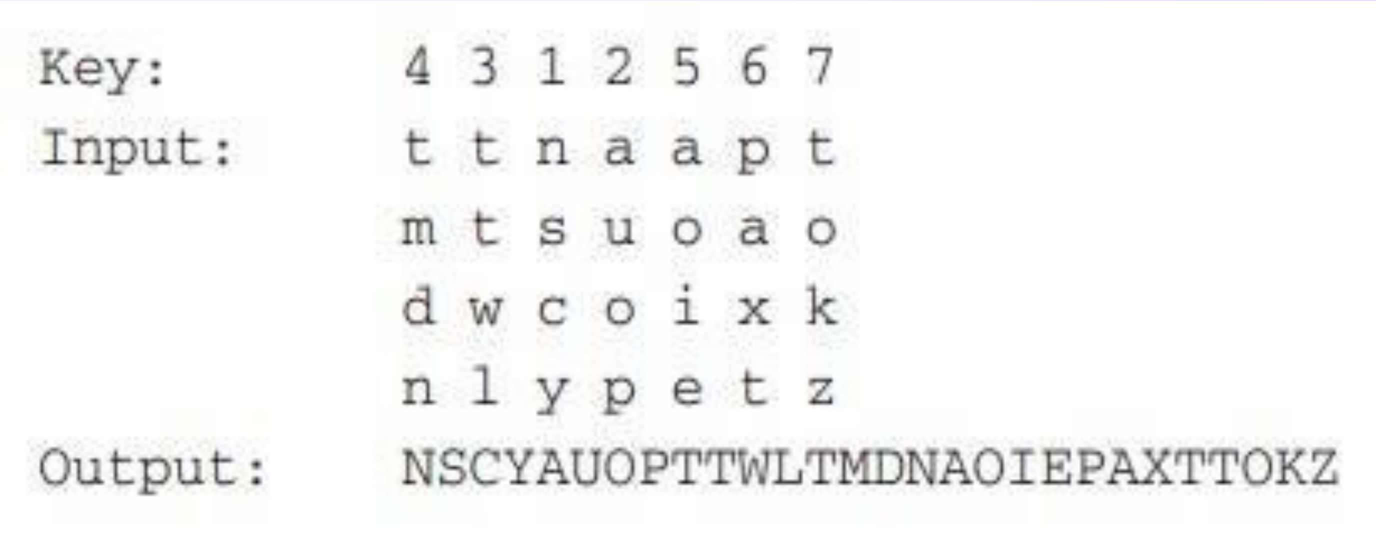
- Ciphertext:“MEMATRHTGPRYETEFETEOAAT”

- A more complex scheme is to 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.
- For example: key=4312567



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.
- Transposition of previous output (TTNAAPTMTSUOAODWCOIXKNLYPETZ) with the same key



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

Shannon theory

- **Confusion (K↔ C)**
  - Confusion makes the relation between the key and the ciphertext as complex as possible.
  - Ideally, every letter in the key influences every letter of the ciphertext block.
    - Replacing every letter with the one next to it on the typewriter keyboard is a simple example of confusion by substitution.
  - Good confusion can only be achieved when each character of the ciphertext depends on several parts of the key, and this dependence appears to be random to the observer.
  - Ciphers that do not offer much confusion (such as Vigenère cipher) are vulnerable to frequency analysis.

Shannon theory

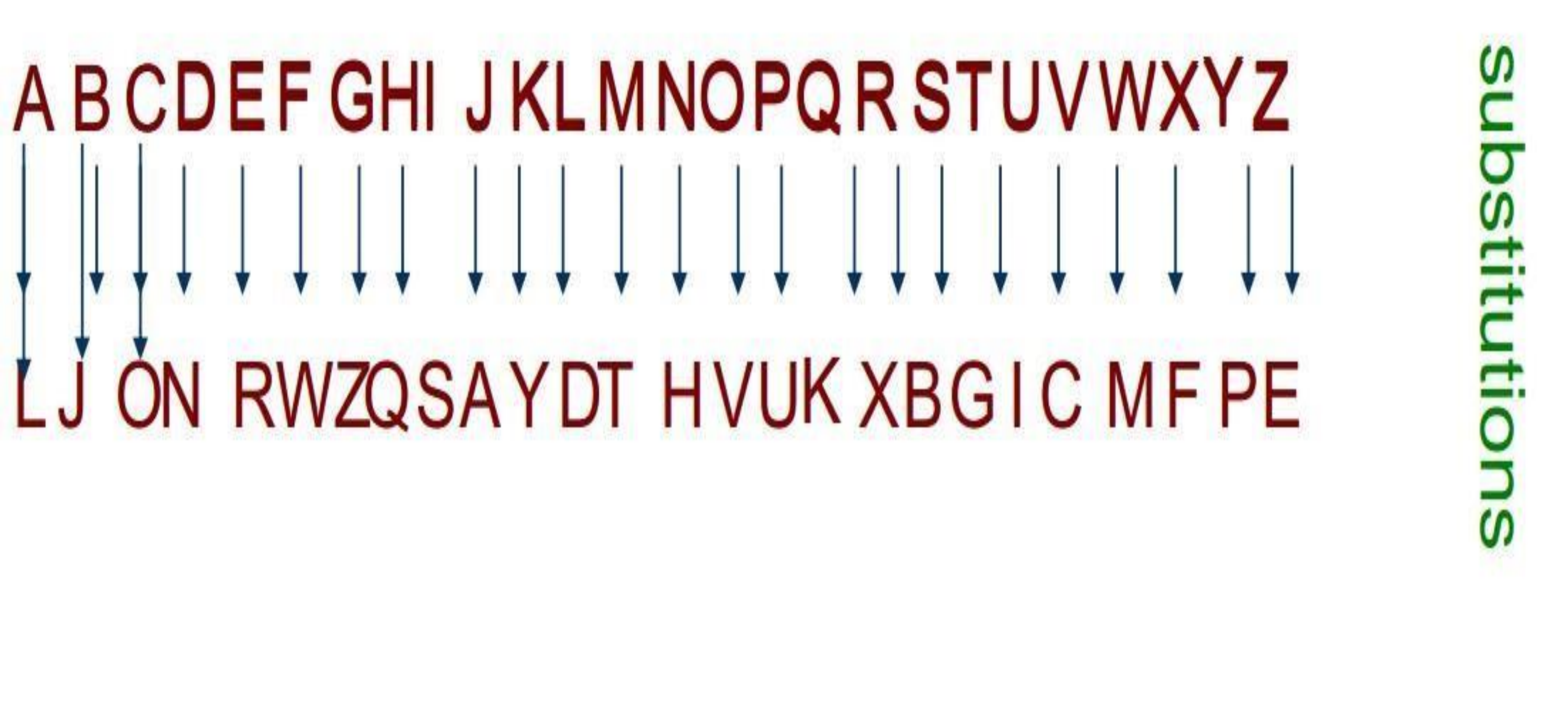
☞ Diffusion (M ↔ C)

- A fixed transformation can show good encryption at the first iterations but it can fail in the long run.
- Diffusion refers to the property that the statistics structure of the plaintext is dissipated into long range statistics of the ciphertext.
- In contrast to confusion, diffusion spreads the influence of a single plaintext letter over many ciphertext letters.
- In terms of the frequency statistics of letters, digrams, etc in the plaintext, diffusion randomly spreads them across several characters in the ciphertext.
- This means that much more ciphertexts are needed to do a meaningful statistical attack on the cipher.

Shannon theory

- ☞ **Unconditional security**
  - Unconditionally secure systems can not be broken even if all possible keys could be tried within short time.

Modern symmetric key cryptography

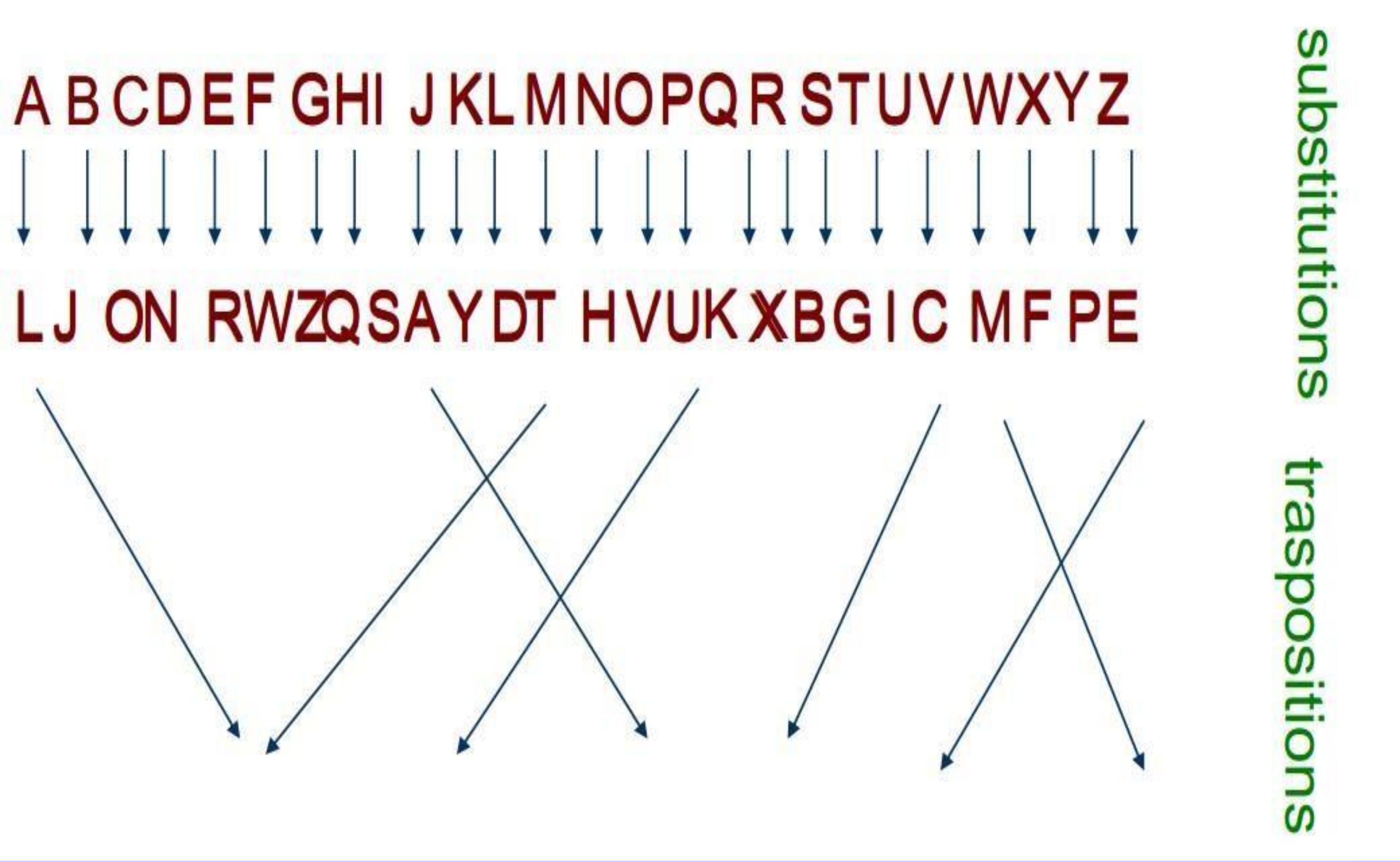


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

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

substitutions

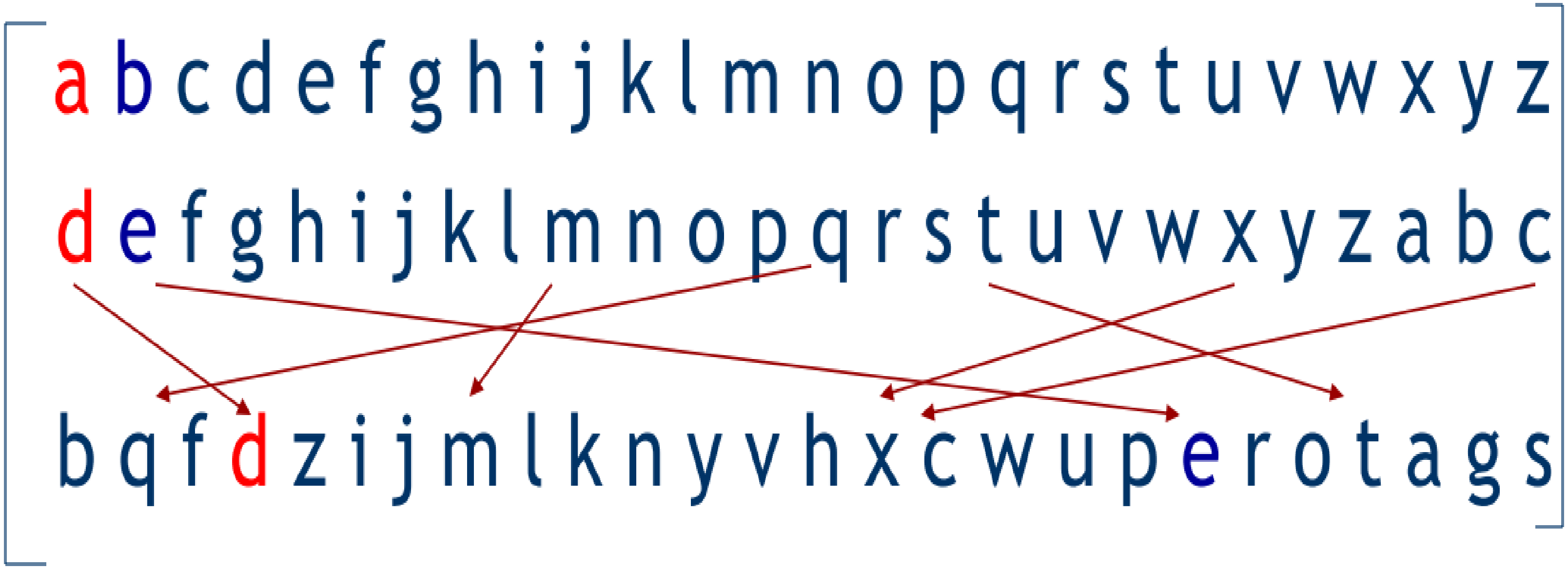
Modern symmetric key cryptography



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
L J ON RWZQSAYDT HVUKXBGIC MFPE
substitutions
traspositions

Product Cipher

- Substitution → confusion K ↔ C
- Permutation → diffusion M ↔ C



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

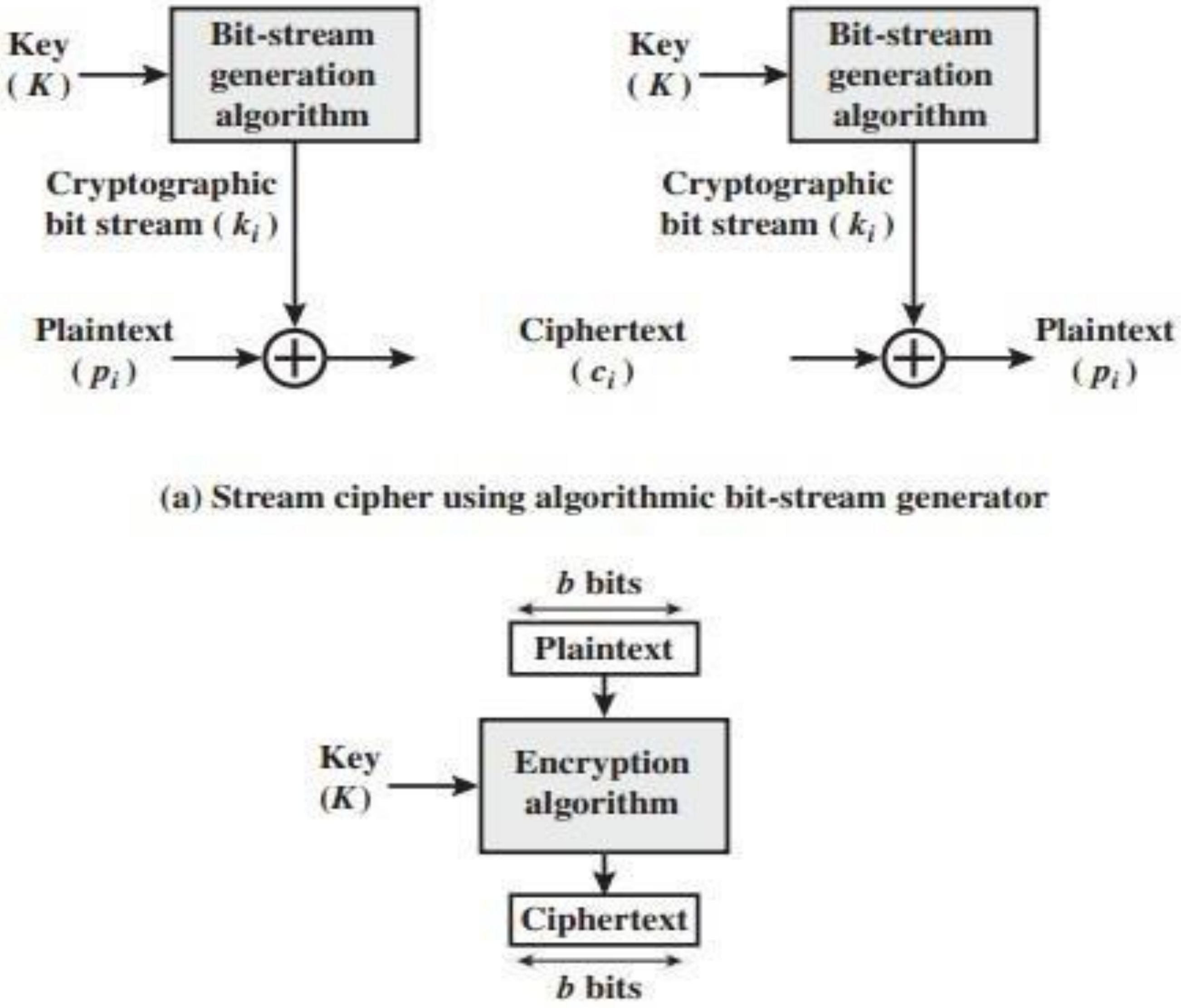
b q f d z i j m l k n y v h x c w u p e r o t a g s

Stream Ciphers and Block Ciphers

- **Stream cipher** is one that encrypts a digital data stream one bit or one byte at a time.

  E.g. Vigenère cipher and theVernam cipher.

- **Block cipher** is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.
  - Typically, a block size of 64 or 128 bits is used.
  - E.g. Feistel cipher and DES


Key
(K)
Bit-stream generation algorithm
Cryptographic bit stream (k_i)
Plaintext
(p_i)
Key
(K)
Bit-stream generation algorithm
Cryptographic bit stream (k_i)
Ciphertext
(c_i)
Plaintext
(p_i)
b bits
Plaintext
Key
(K)
Encryption algorithm
Ciphertext
b bits

(a) Stream cipher using algorithmic bit-stream generator

(b) Block cipher

Block Cipher

- A block cipher operates on a block of n bits and it produces a ciphertext block of n bits.
- There are 2^n possible different plaintext/ciphertext blocks.
- The encryption must be **reversible**. i.e. decryption to be possible each plaintext must produce a unique ciphertext block. (one-to-one correspondence)
- Such a transformation is called reversible, or nonsingular.
- The following examples illustrate nonsingular and singular transformations for n=2.