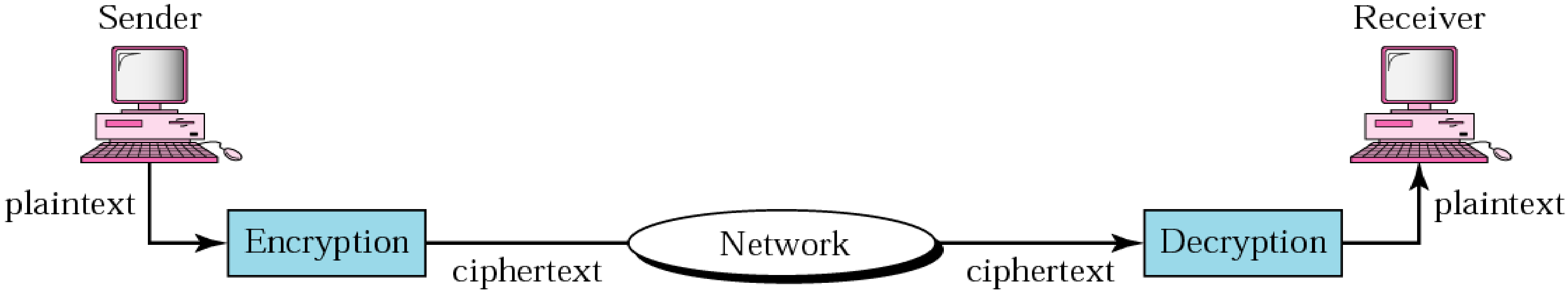
Cryptography

Introduction

- In Greek means secret writing
- Today referred as the science and art of transforming messages to make them secure and immune to attacks



Basic Terminology

- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - the field of both cryptography and cryptanalysis

Plain Text and Cipher Text

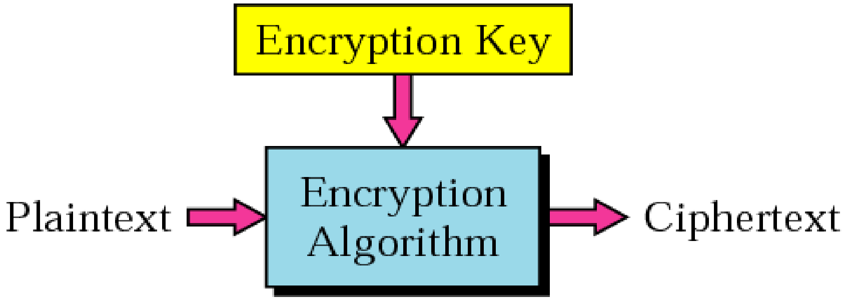
- Plain Text: Language that can be easily understood

- Cipher Text: Language that cannot be understood

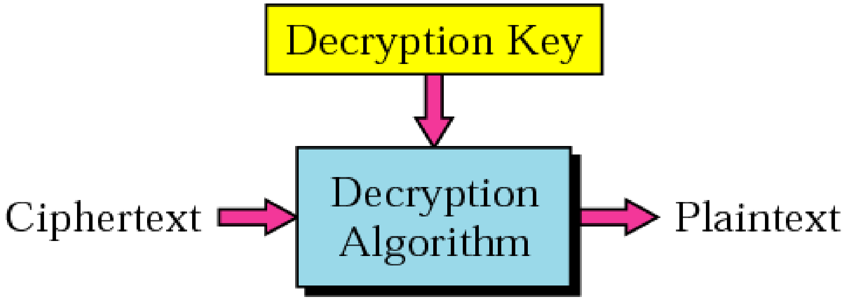
- To achieve security, plain text is transformed into cipher text

- Cipher is a term refers to different categories of algorithms in cryptography
- Sender-receiver needs own unique cipher fro secure communication
- Key is a number that the cipher operates on
- To encrypt you require
  - Encryption algo
  - Encryption key and
  - plaintext

Encryption and Decryption



a. Encryption



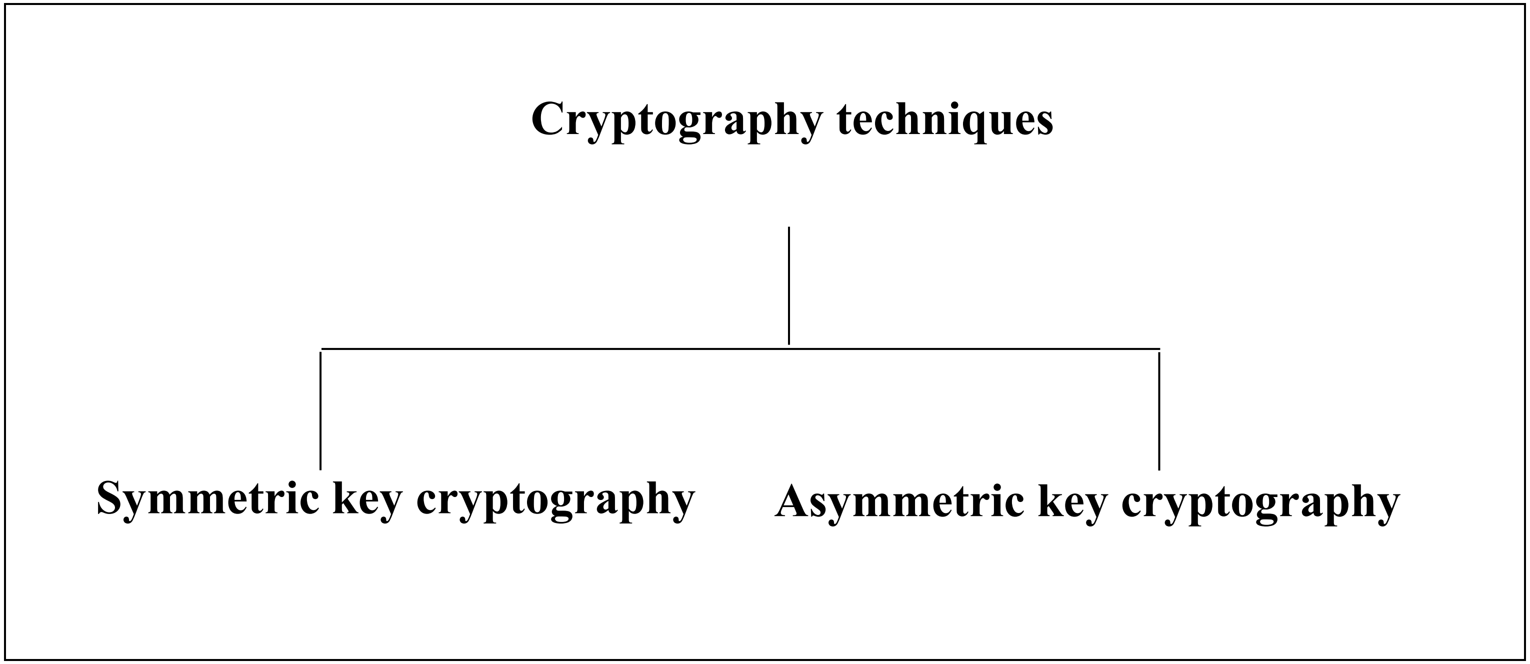
b. Decryption

- Algorithms are public
- Anyone can access them
- Keys are secret
- Need to be protected
- Alice, Bob and Eve

Cryptography

- can characterize by:
  - – type of encryption operations used
    - substitution / transposition / product
  - – number of keys used
    - single-key or private / two-key or public
  - – way in which plaintext is processed
    - block / stream

Types of Cryptography



Cryptography techniques

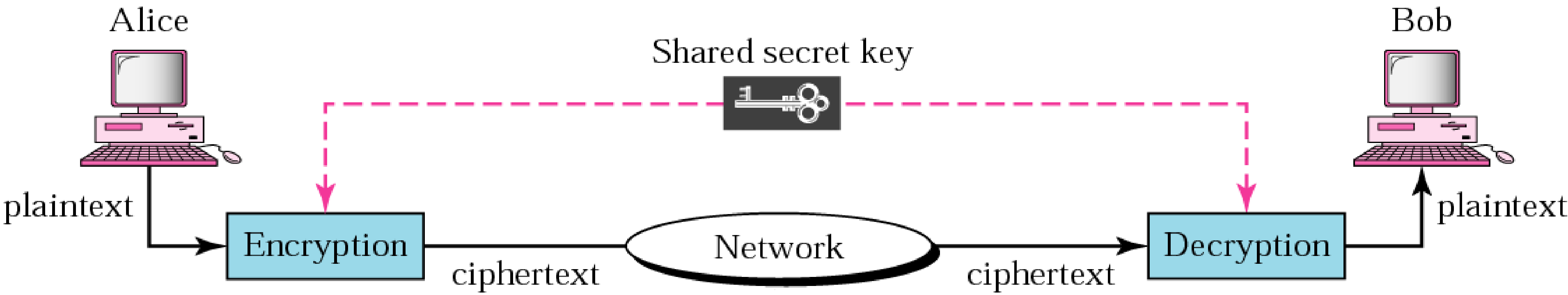
Symmetric key cryptography

Asymmetric key cryptography

Symmetric Encryption

- or conventional / private-key / single-key
- sender and recipient share a common key
- all classical encryption algorithms are private-key
- was only type prior to invention of public-key in 1970's

Symmetric Cipher Model



In symmetric-key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.

In symmetric-key cryptography, the same key is used in both directions.

Advantages

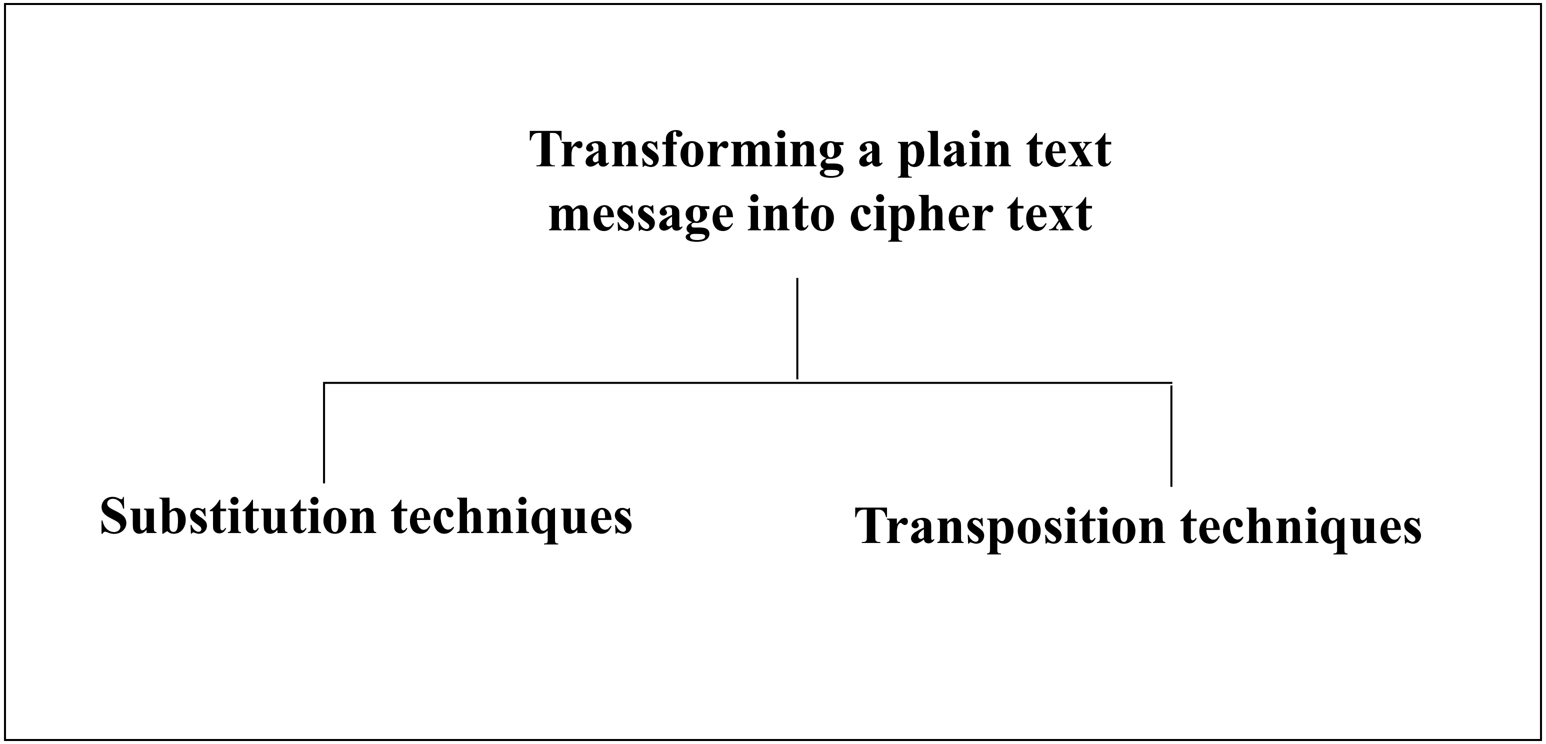
- Algorithm used for decryption is reverse of encryption
- i.e if encryption uses a combination of addition and multiplication decryption is combination of division and subtraction
- Symmetric algorithms are efficient
- Take less time to encrypt than asymmetric

Symmetric-key cryptography is often used for long messages.

Disadvantages

- Each pair must have a unique symmetric key
- If N people want to use there need n(n-1)/2 keys
- Distribution of keys between two parties can be difficult

Techniques for Plain Text to Cipher Text Conversion – Traditional Ciphers

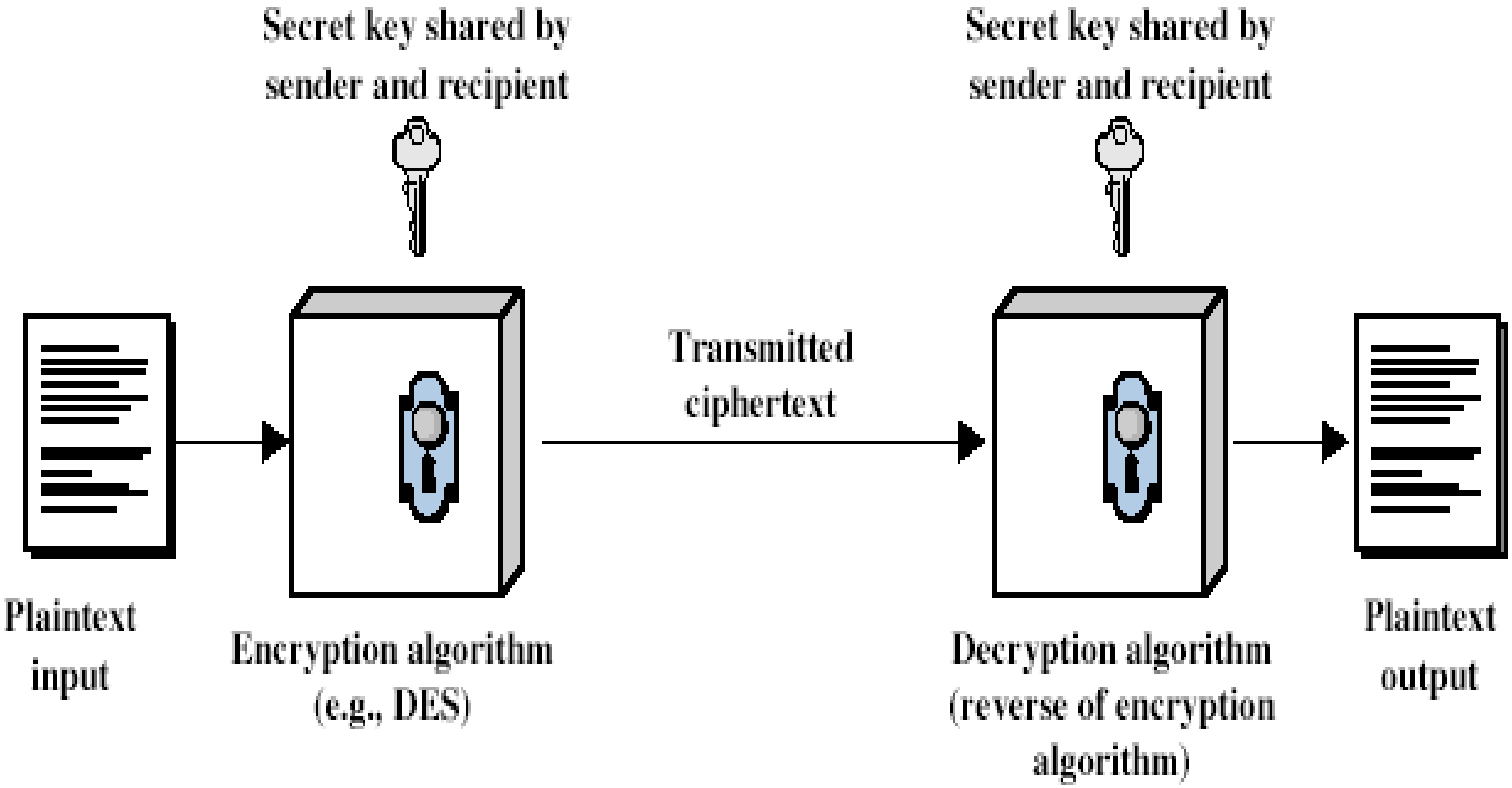


Transforming a plain text message into cipher text

Substitution techniques

Transposition techniques

Symmetric Cipher Model



Requirements

- two requirements for secure use of symmetric encryption:
  - a strong encryption algorithm
  - a secret key known only to sender / receiver
- mathematically have:

  $Y = \mathrm{E}_K(X)$

  $X = \mathrm{D}_K(Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Cryptography

- characterize cryptographic system by:
  - type of encryption operations used
    - substitution / transposition / product
  - number of keys used
    - single-key or private / two-key or public
  - way in which plaintext is processed
    - block / stream

Cryptanalysis

- objective to recover key not just message
- general approaches:
  - cryptanalytic attack
  - brute-force attack

Cryptanalytic Attacks

- **ciphertext only**
  - only know algorithm & ciphertext, is statistical, know or can identify plaintext
- **known plaintext**
  - know/suspect plaintext & ciphertext
- **chosen plaintext**
  - select plaintext and obtain ciphertext
- **chosen ciphertext**
  - select ciphertext and obtain plaintext
- **chosen text**
  - select plaintext or ciphertext to en/decrypt

Brute Force Search

- always possible to simply try every key
- most basic attack, proportional to key size
- assume either know / recognise plaintext

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/µs	Time required at 10^6 decryptions/µs
32	$2^{32} = 4.3 \times 10^9$	2^{31} µs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} µs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} µs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} µs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} µs = 6.4×10^{12} years	6.4×10^6 years

Classical Substitution Ciphers

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

Caesar Cipher

- earliest known substitution cipher
- by Julius Caesar
- first attested use in military affairs
- replaces each letter by 3rd letter on
- example:

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```

Caesar Cipher

- 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

- then have Caesar cipher as:

$$c = \mathrm{E}(p) = (p + k) \bmod (26)$$

$$p = \mathrm{D}(\mathrm{c}) = (\mathrm{c} - k) \bmod (26)$$

Cryptanalysis of Caesar Cipher

- only have 26 possible ciphers
  - A maps to A,B,..Z
- could simply try each in turn
- a **brute force search**
- given ciphertext, just try all shifts of letters
- do need to recognize when have plaintext
- eg. break ciphertext "GCUA VQ DTGCM"

Monoalphabetic Cipher

- rather than just shifting the alphabet
- could shuffle (jumble) the letters arbitrarily
- each plaintext letter maps to a different random ciphertext letter
- hence key is 26 letters long

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN

Plaintext:  ifwewishtoreplaceletters
Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA
```

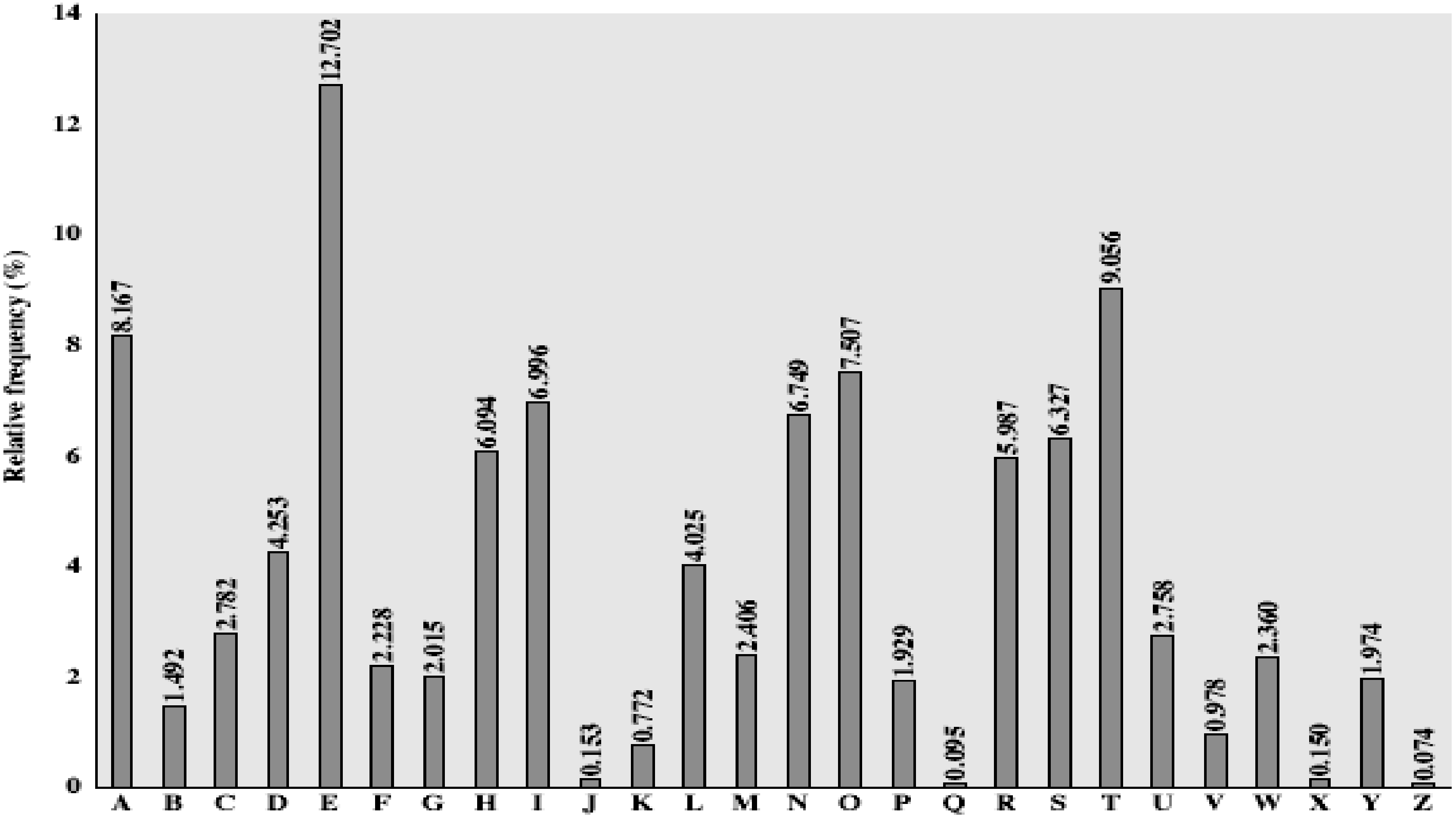
Monoalphabetic Cipher Security

- now have a total of 26! = 4 x 10 raise to 26 keys
- with so many keys, might think is secure
- but would be **!!!WRONG!!!**
- problem is language characteristics

Language Redundancy and Cryptanalysis

- human languages are **redundant**
- eg "th lrd s m shphrd shll nt wnt"
- letters are not equally commonly used
- in English E is by far the most common letter
  - followed by T,R,N,I,O,A,S
- other letters like Z,J,K,Q,X are fairly rare
- have tables of single, double & triple letter frequencies for various languages

English Letter Frequencies



Playfair Cipher

- not even the large number of keys in a monoalphabetic cipher provides security
- one approach to improving security was to encrypt multiple letters
- the **Playfair Cipher** is an example
- invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair

Playfair Key Matrix

- a 5X5 matrix of letters based on a keyword
- fill in letters of keyword (sans duplicates)
- fill rest of matrix with other letters
- eg. using the keyword 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

Encrypting and Decrypting

- plaintext is encrypted two letters at a time
  1. if a pair is a repeated letter, insert filler like 'X’
  2. if both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
  3. if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)
  4. otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair

Security of Playfair Cipher

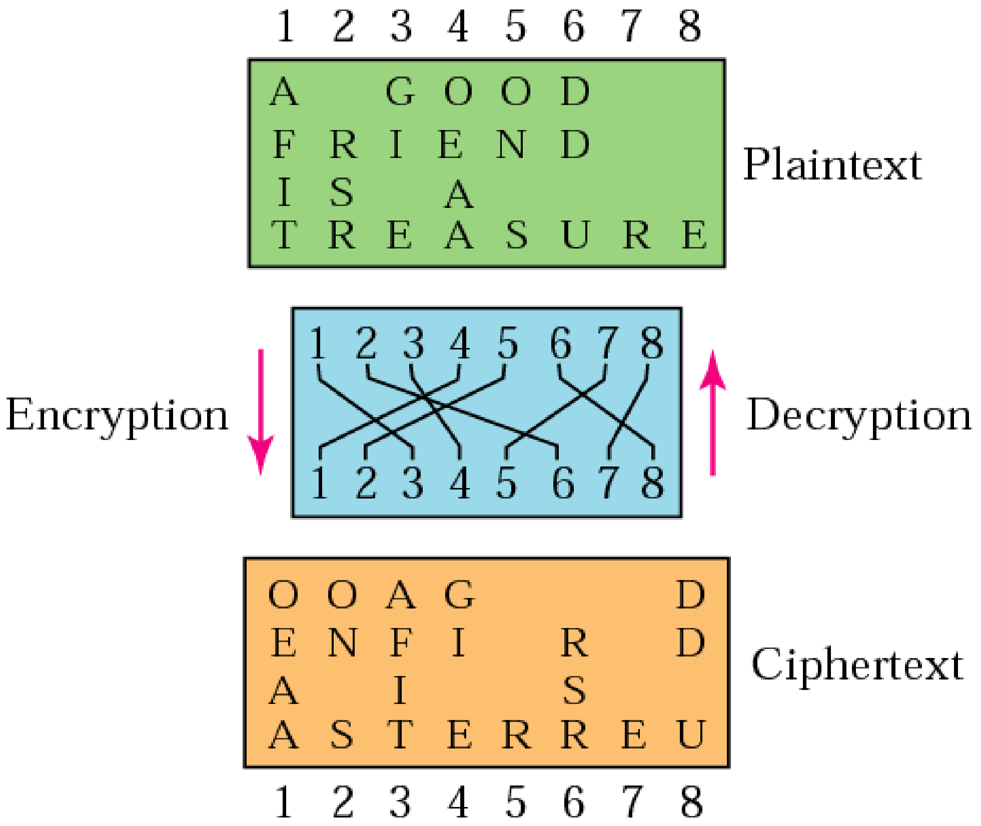
- security much improved over monoalphabetic
- since have 26 x 26 = 676 digrams
- would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic)
- and correspondingly more ciphertext
- was widely used for many years
  - eg. by US & British military in WW1
- it **can** be broken, given a few hundred letters
- since still has much of plaintext structure

Polyalphabetic Cipher

- Each occurrence of a character can have a different substitute
- Relationship is one to many
- Char A can be replaced D once and Y the other
- Eg. Vigenere cipher

Transpositional Cipher

- The characters retain their plaintext form but change their positions to create the plaintext
- Text is organized as a two dimensional matrix
- The columns are interchanged according to the key



1	2	3	4	5	6	7	8
A		G	O	O	D		
F	R	I	E	N	D		
I	S		A				
T	R	E	A	S	U	R	E

Plaintext

1	2	3	4	5	6	7	8
O	O	A	G				D
E	N	F	I		R		D
A		I			S		
A	S	T	E	R	R	E	U

Ciphertext

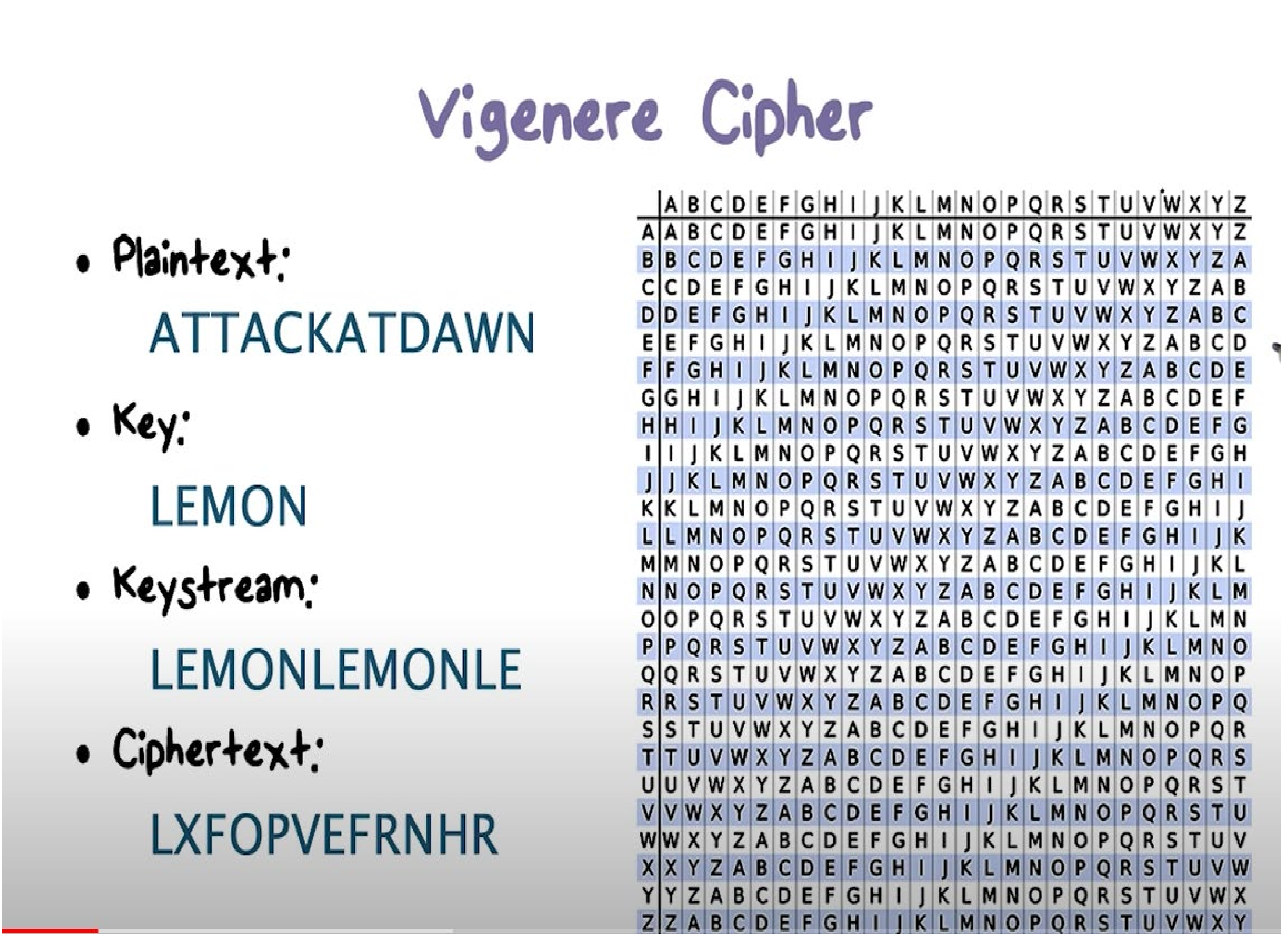
Vigenere Cipher

- Character in the ciphertext is chosen form a 2 dimensional table (26*26)
- Each row is permutation of 26 characters (A to Z)
- To encrypt algo finds the character to be replaced in the first row
- Finds the position of the character in the text (mod 26) and uses it as the row number
- then replaces the character with the character found in the table

Plaintext

Key

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



Vigenere Cipher

- Plaintext:

  ATTACKATDAWN

- Key:

  LEMON

- Keystream:

  LEMONLEMONLE

- Ciphertext:

  LXFOPVEFRNHR

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

Vernam Cipher

- Vernam Cipher, also known as the one-time-pad.Gilbert Vernam invented and patented his cipher in 1917 while working at AT&T.
- Vernam cipher Also known as One-time-pad.

What Is One-Time pad?

- In cryptography, the one-time pad is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key the same size as the message being sent.
- In this technique, a plaintext is paired with a random secret key (also referred to as a **one**-**time pad**)

Encryption Formula:

- plaintext + key = cipher text

Decryption Forumla:

- cipher text-key=plain-text

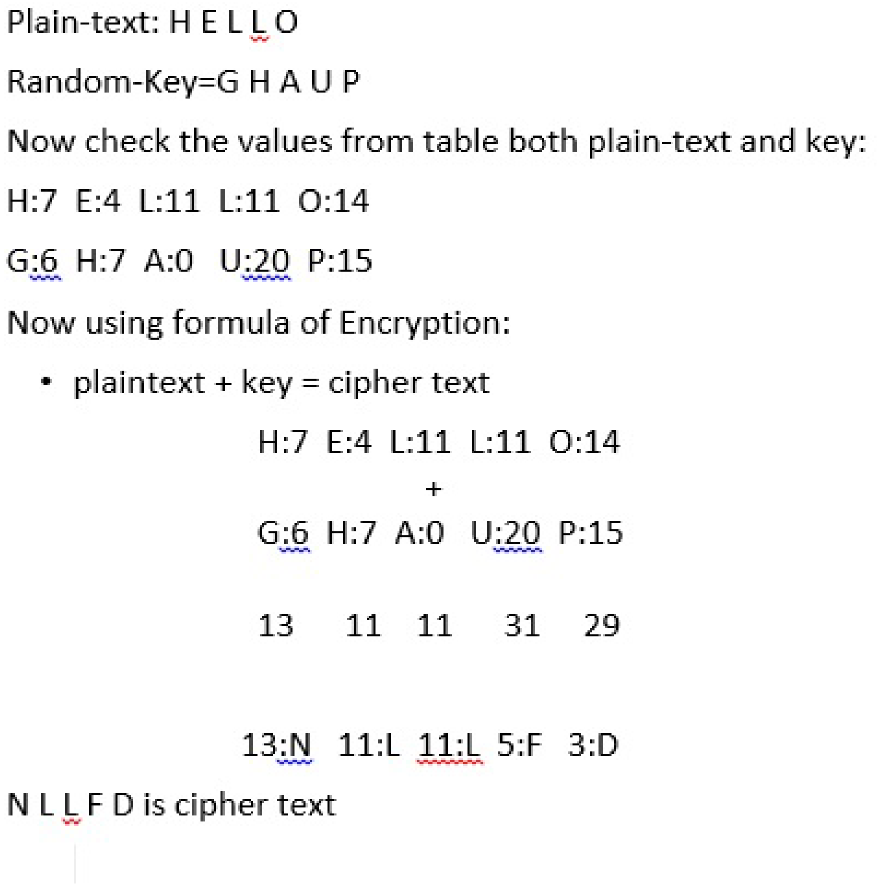
Some Rules for Encryption

- First We chose plain text which we want to convert into cipher text.
- We can chose random key.
- Key length is always equal to length of cipher text.
- After adding plain text and keys .If num is $\geq \mathbf{26}$ then we subtract 26 from cipher text in Encryption.
- Keys have two copies One for sender and one for receiver.
- Keys is discarded after one time use.

TABLE ALPHABET

A	0	I	8	Q	16	Y	24
B	1	J	9	R	17	Z	25
C	2	K	10	S	18		
D	3	L	11	T	19		
E	4	M	12	U	20		
F	5	N	13	V	21		
G	6	O	14	w	22		
H	7	P	15	X	23		

Encryption Example



Plain-text: H E L L O

Random-Key=G H A U P

Now check the values from table both plain-text and key:

H:7 E:4 L:11 L:11 O:14

G:6 H:7 A:0 U:20 P:15

Now using formula of Encryption:

- plaintext + key = cipher text

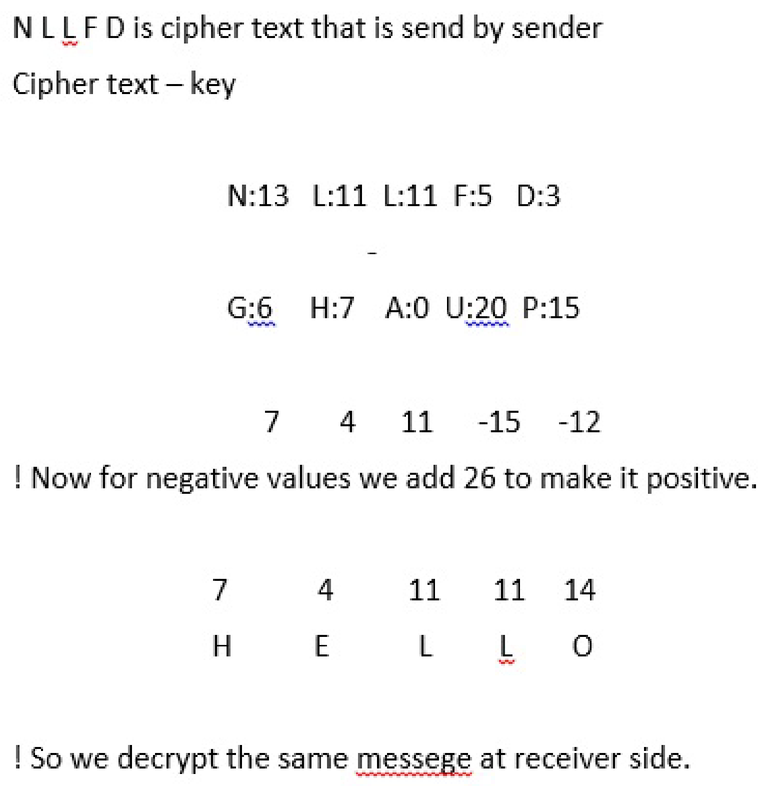
H:7 E:4 L:11 L:11 O:14
+
G:6 H:7 A:0 U:20 P:15

13 11 11 31 29

13:N 11:L 11:L 5:F 3:D

N L L F D is cipher text

Decryption



N L L F D is cipher text that is send by sender

Cipher text – key

N:13 L:11 L:11 F:5 D:3

-

G:6 H:7 A:0 U:20 P:15

7 4 11 -15 -12

! Now for negative values we add 26 to make it positive.

7 4 11 11 14

H E L L O

! So we decrypt the same messege at receiver side.

Another Example “same message” but now this time key is different.

Encyption

```
           H E L L O
 7 (H) 4 (E) 11 (L) 11 (L) 14 (O) message

+ 23 (X) 12 (M) 2 (C) 10 (K) 11 (L) key

= 30 16 13 21 25 message + key

= 4 (E) 16 (Q) 13 (N) 21 (V) 25 (Z) (message +
key)

  E Q N V Z → ciphertext
```

Decryption:

```
E Q N V Z cipher-text

 4 (E) 16 (Q) 13 (N) 21 (V) 25 (Z) cipher-text

- 23 (X) 12 (M) 2 (C) 10 (K) 11 (L)

 key = -19 4 11 11 14

For negative value we add 26 for make it positive

7 (H) 4 (E) 11 (L) 11 (L) 14 (O) cipher-text – key

 H E L L O → message
```

- This cipher is unbreakable in a very strong sense. The intuition is that any message can be transformed into any cipher (of the same length) by a pad, and all transformations are equally likely

Modern use of the Vernam Cipher

- The Vernam Cipher can also be implemented with modern computer technology.

Why OTP is secure?

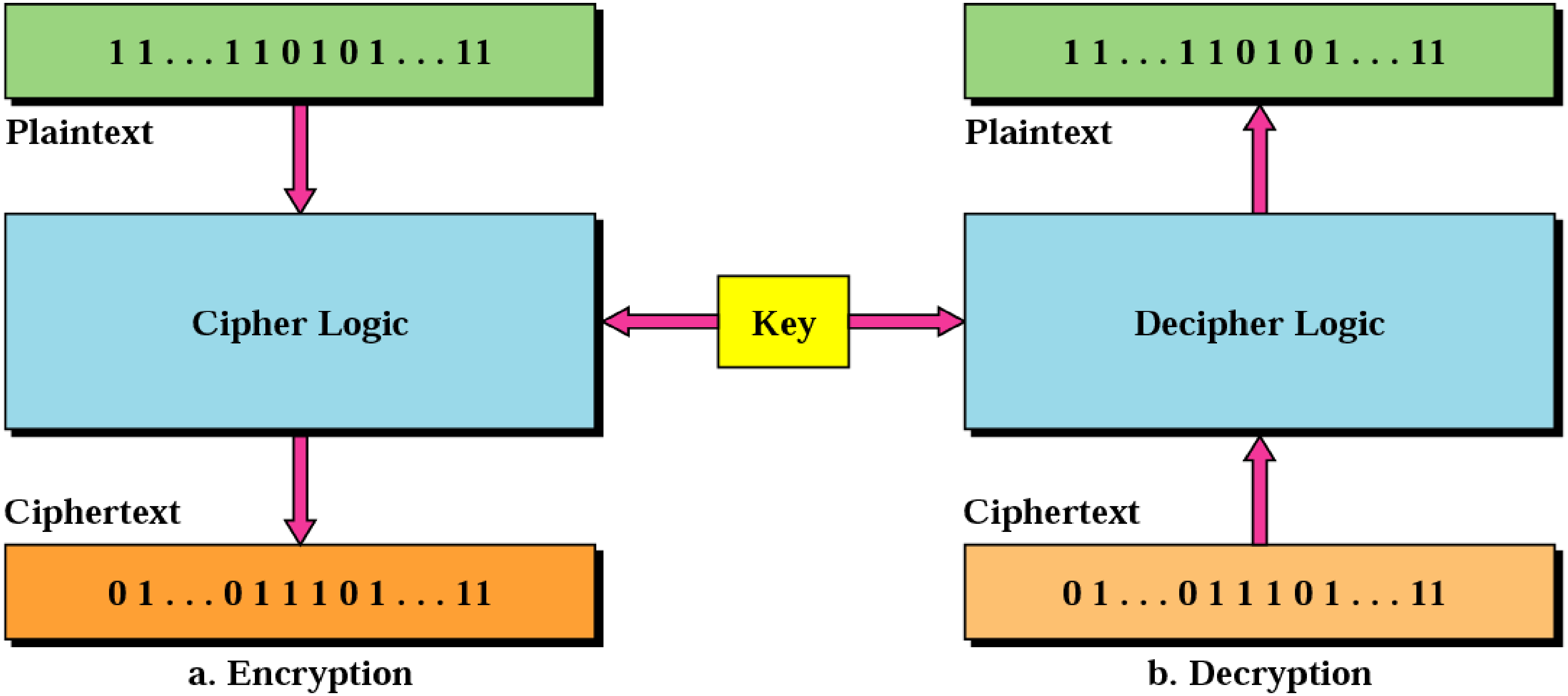
- The security depends on the randomness of the key.

Drawback in OTP

- Key-stream should be as long as plain-text.
- Key distribution & Management difficult.

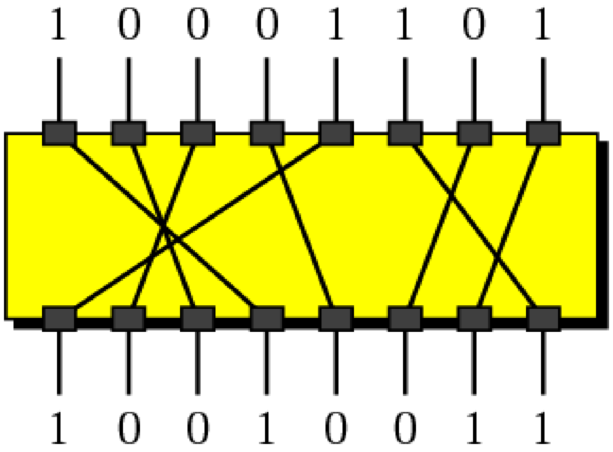
Block Cipher

- Traditional ciphers used character or symbols as he unit of encryption/decryption
- Modern ciphers use a block of bits as a unit of encryption and decryption



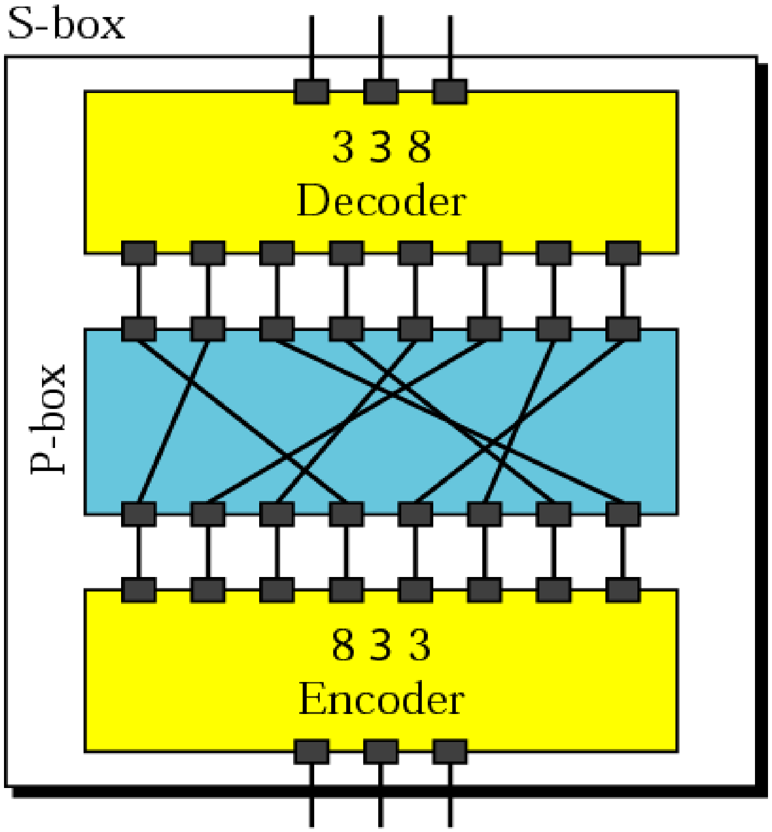
P box

- Permutation box
- Performs transposition at bit level
- Transposes bits
- The key and the encryption/decryption algo are embedded in the hardware
- Plain text and cipher text have the same number of 1s and 0s

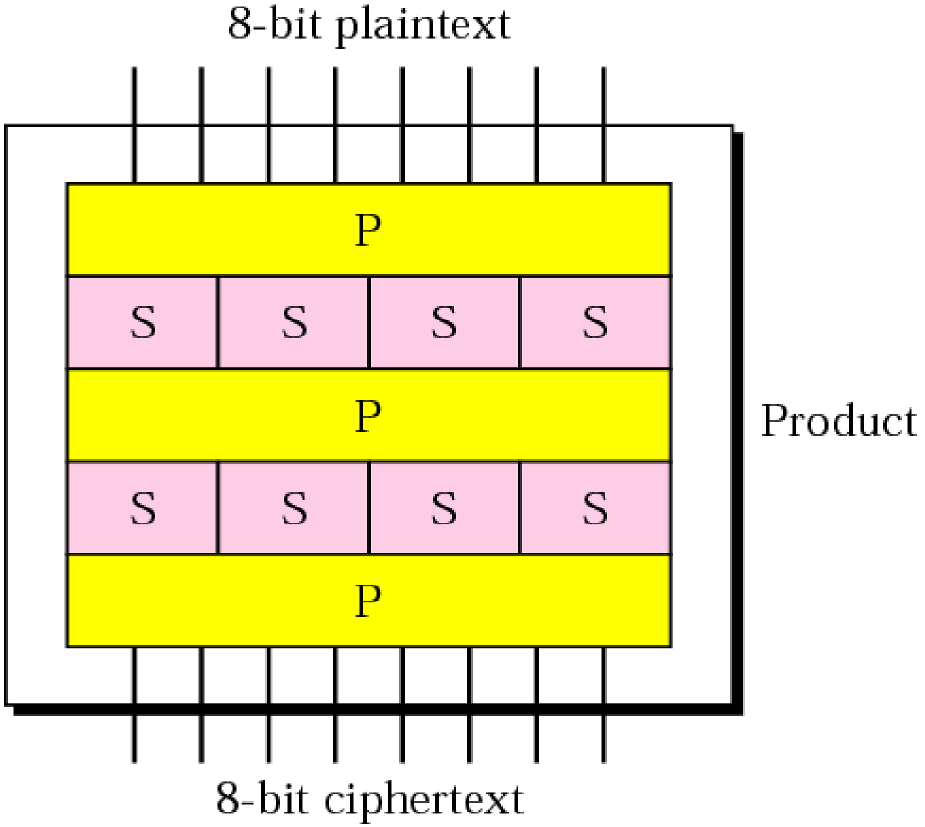


S box

- Substitution box
- Performs substitution at bit level
- Transposes the permuted bits
- substitutes one decimal digit with another
- 3 components
  - Encoder
  - Decoder
  - P box



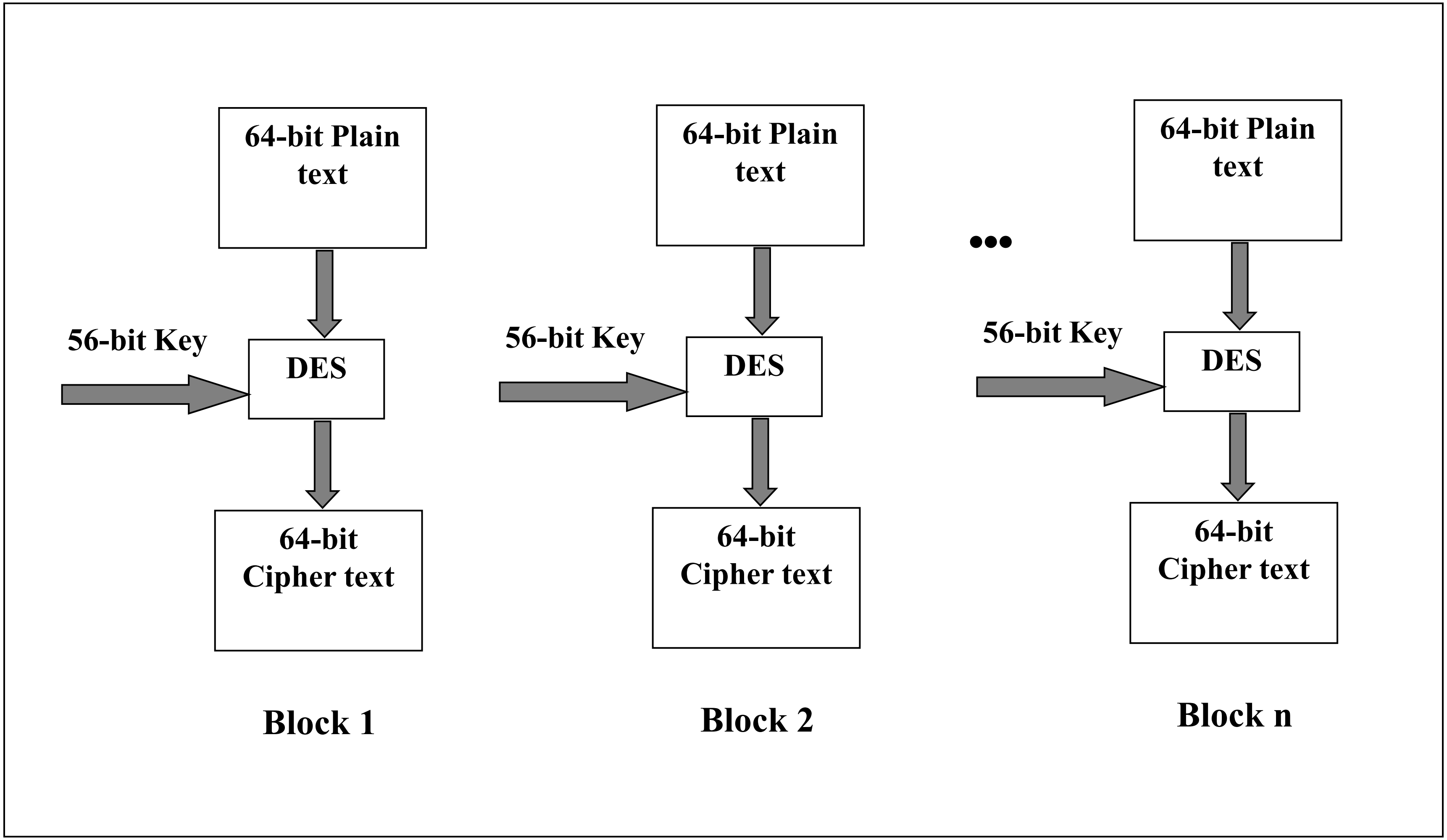
Product block



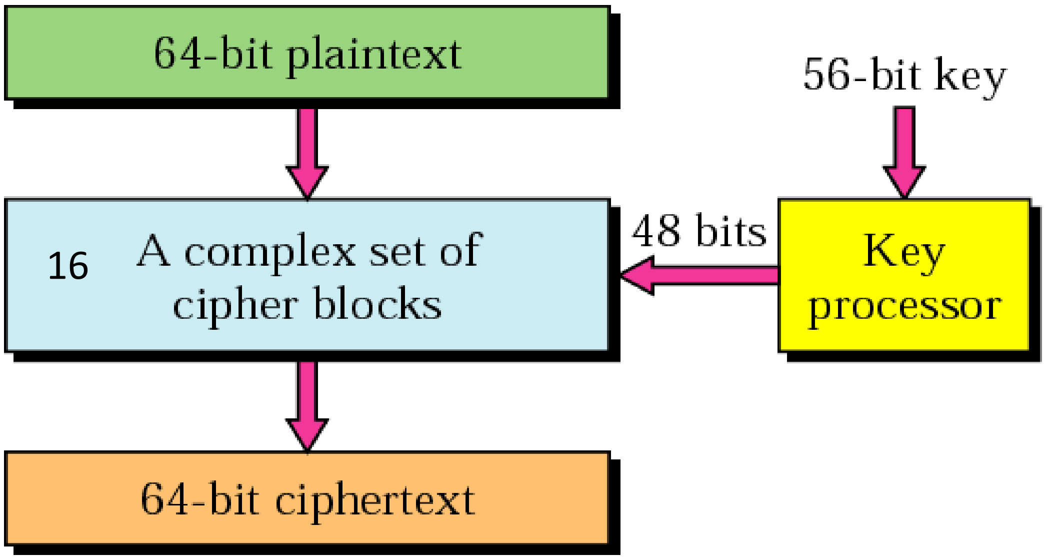
Data Encryption Standard (DES)

- most widely used block cipher in world
- encrypts 64-bit data using 56-bit key
- has widespread use
- has been considerable controversy over its security

Conceptual View of DES



Data Encryption Standard



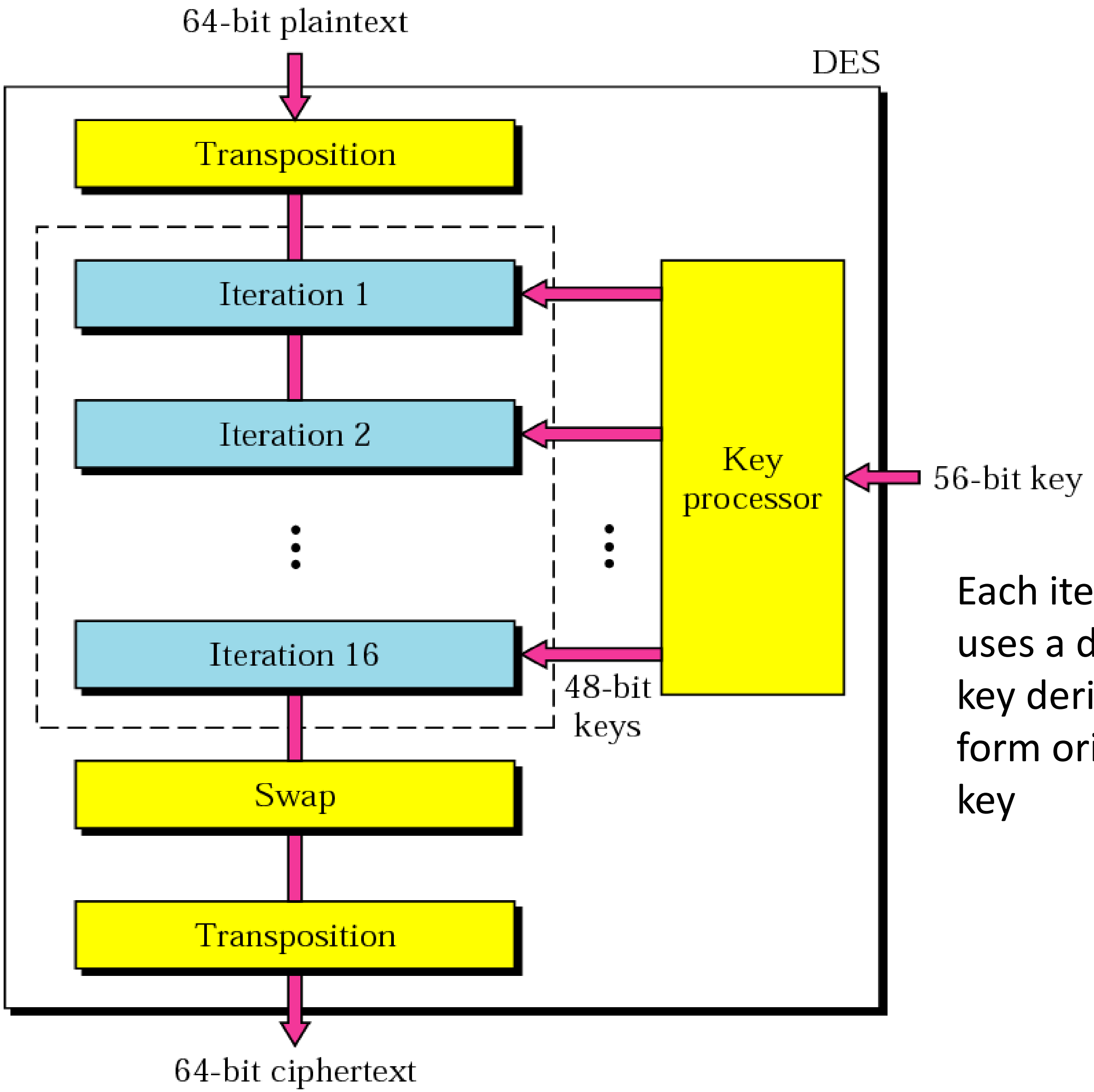
DES has

2 transposition blocks

one swapping block

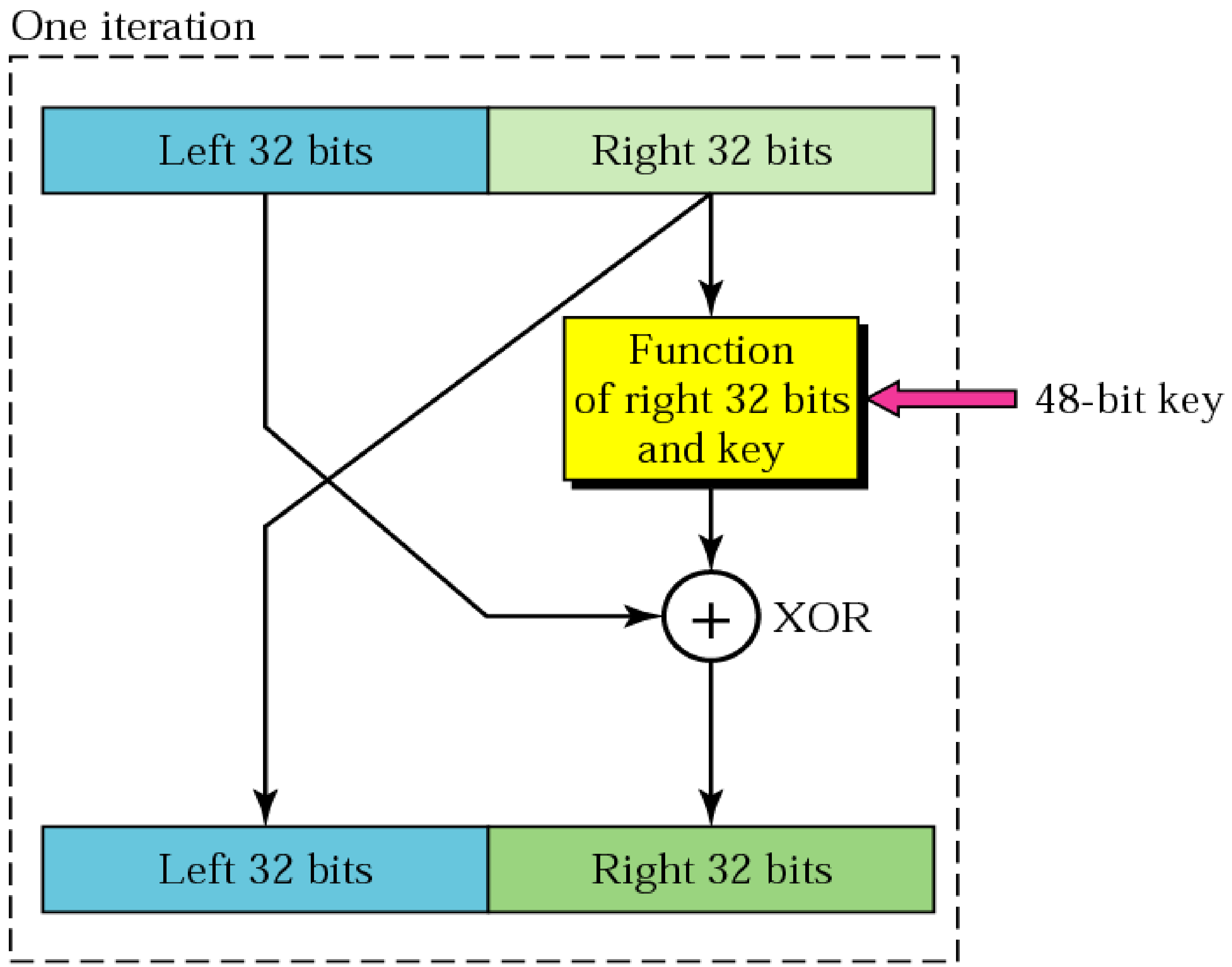
16 complex blocks called the iteration blocks

General scheme of DES

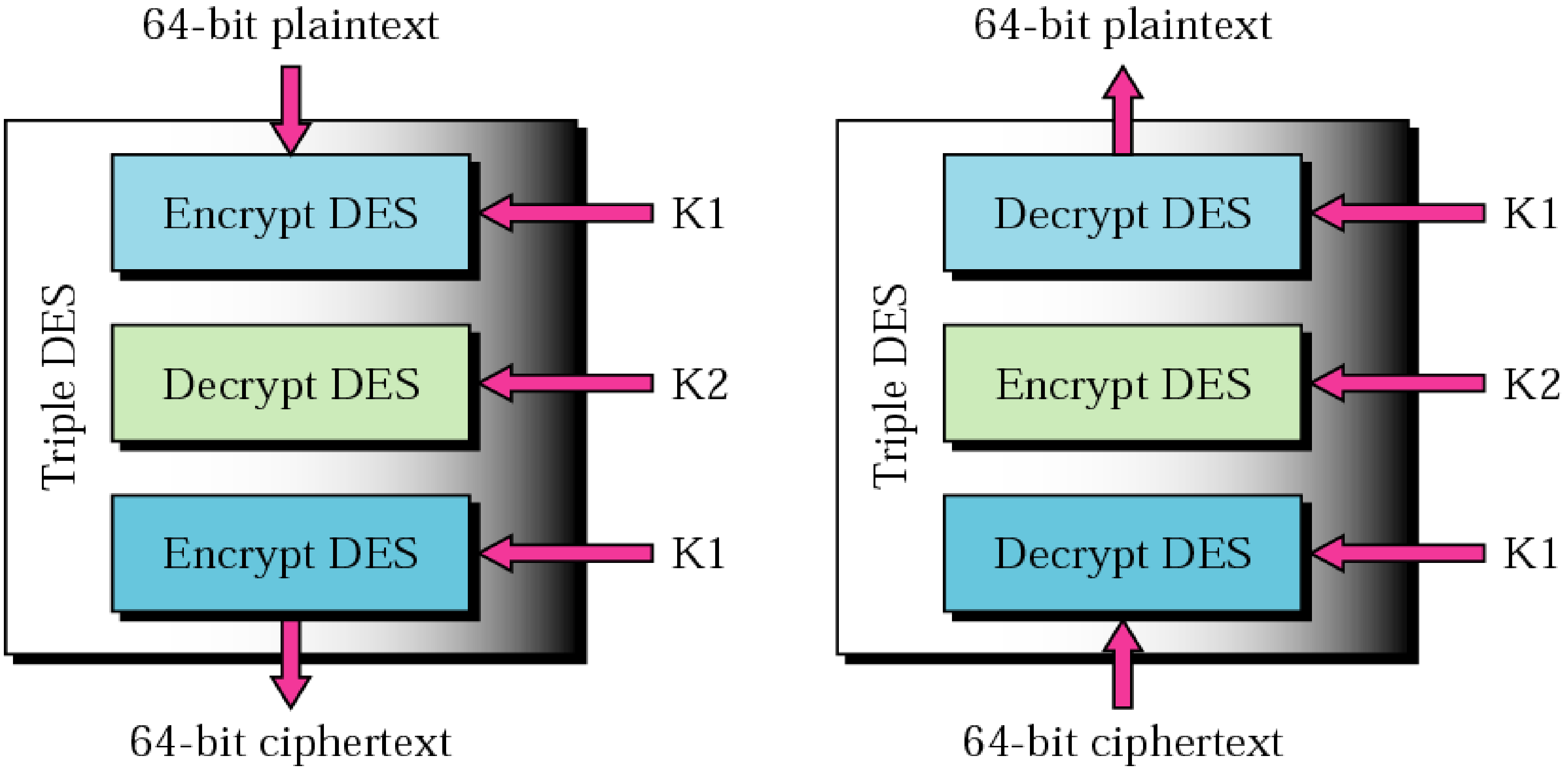


Each iteration uses a different key derived form original key

Iteration block



Triple DES



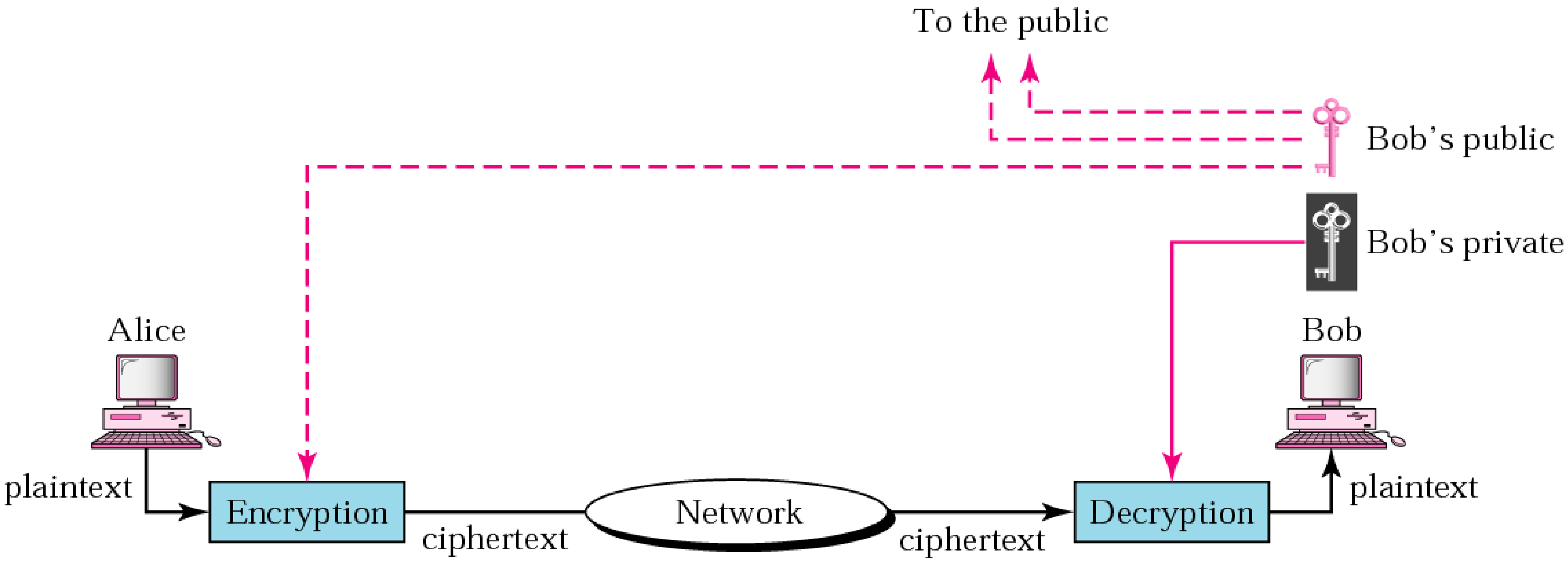
a. Encryption triple DES

b. Decryption triple DES

The DES cipher uses the same concept as the Caesar cipher, but the encryption/decryption algorithm is much more complex due to the sixteen 48-bit keys derived from a 56-bit key.

Public Key Cryptography

- Two keys
- Public and private key
- Public key is announced to the public



Advantages

- Removes the restriction of a shared symmetric key between two entities
- Number of keys needed is reduced
- For 10 users require 20 keys

Public-key algorithms are more efficient for short messages.

Disadvantages

- Complex algorithms
- Association between the entity and the public key must be verified