

# ECE 646 - Lecture 6

## Historical Ciphers

1

---

---

---

---

### Why (not) to study historical ciphers?

#### AGAINST

Not similar to modern ciphers

Long abandoned

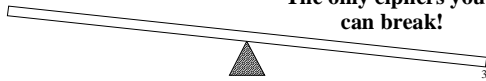
#### FOR

Basic components became a part of modern ciphers

Under special circumstances modern ciphers reduce to historical ciphers

Influence on world events

The only ciphers you can break!



---

---

---

---

### Secret Writing

**Steganography**  
(hidden messages)

**Cryptography**  
(encrypted messages)

**Substitution Transformations**

**Transposition Ciphers**  
(change the order of letters)

**Codes**  
(replace words)

**Substitution Ciphers**  
(replace letters)

4

---

---

---

---

### Selected world events affected by cryptology

- 1 - trial of Mary Queen of Scots - substitution cipher
- 1 - Zimmermann telegram, America enters World War I
- 1939-1945 Battle of England, Battle of Atlantic, D-day - ENIGMA machine cipher
- 1944 – world’s first computer, Colossus - German Lorentz machine cipher
- 1950s – operation Venona – breaking ciphers of soviet spies stealing secrets of the U.S. atomic bomb – one-time pad

---



---



---

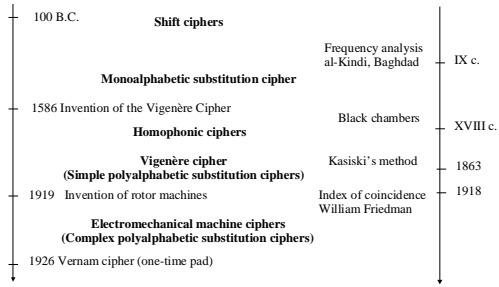


---

### Ciphers used predominantly in the given period(1)

#### Cryptography

#### Cryptanalysis




---



---



---

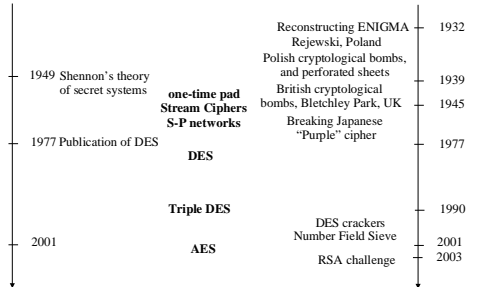


---

### Ciphers used predominantly in the given period(2)

#### Cryptography

#### Cryptanalysis




---



---



---



---

## Simple Monalphabetic substitution ciphers

### A. Caesar Cipher

$$c_i = f(m_i) = m_i + 3 \pmod{26}$$

$$m_i = f^{-1}(c_i) = c_i - 3 \pmod{26}$$

No key

### B. Shift Cipher

$$c_i = f(m_i) = m_i + k \pmod{26}$$

$$m_i = f^{-1}(c_i) = c_i - k \pmod{26}$$

Key = k

Number of keys = 26

8

---

---

---

---

## Coding characters into numbers

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

9

---

---

---

---

## Caesar Cipher: Example

**Plaintext:** I C A M E I S A W I C O N Q U E R E D

8 20 124 8 18 022 8 2 14 13 16 20 4 17 4 3

11 5 3 15 7 11 21 3 25 11 5 17 16 19 23 7 20 7 6

**Ciphertext:** L F D P H L V D Z L F R Q T X H U H G

10

---

---

---

---

## Simple Monalphabetic substitution ciphers (2)

### C. Affine Cipher

$$c_i = f(m_i) = k_1 \cdot m_i + k_2 \pmod{26}$$
$$\gcd(k_1, 26) = 1$$

$$m_i = f^{-1}(c_i) = k_1^{-1} \cdot (c_i - k_2) \pmod{26}$$

$$\text{Key} = (k_1, k_2)$$

$$\text{Number of keys} = 12 \cdot 26 = 312$$

11

---

---

---

---

## General Substitution Cipher

### 1. Monalphabetic (simple) substitution cipher

$$M = m_1 \ m_2 \ m_3 \ m_4 \ \dots \ m_N$$
$$C = f(m_1) \ f(m_2) \ f(m_3) \ f(m_4) \ \dots \ f(m_N)$$

Generally  $f$  is a random permutation, e.g.,

$$f = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ s & l & t & a & v & m & c & e & r & u & b & q & p & d & f & k & h & w & y & g & x & z & j & n & i & o \end{pmatrix}$$

$$\text{Key} = f$$

$$\text{Number of keys} = 26! \approx 4 \cdot 10^{26} \approx 2^{89}$$

12

---

---

---

---

## General Substitution Cipher (2)

- #keys =  $2^{88}$
- Q: Is a brute-force attack possible?  
i.e., trying of all possible keys
- Q: Which other attack is possible?

13

---

---

---

---

### Most frequent single letters

Average frequency in a random string of letters:

$$\frac{1}{26} = 0.038 = 3.8\%$$

Average frequency in a long English text:

E	—	13%
T, N, R, I, O, A, S	—	6%-9%
D, H, L	—	3.5%-4.5%
C, F, P, U, M, Y, G, W, V	—	1.5%-3%
B, X, K, Q, J, Z	—	< 1%

---



---



---



---

### Most frequent digrams, and trigrams

**Digrams:**

TH, HE, IN, ER, RE, AN, ON, EN, AT

**Trigrams:**

THE, ING, AND, HER, ERE, ENT, THA, NTH,  
WAS, ETH, FOR, DTH

---



---

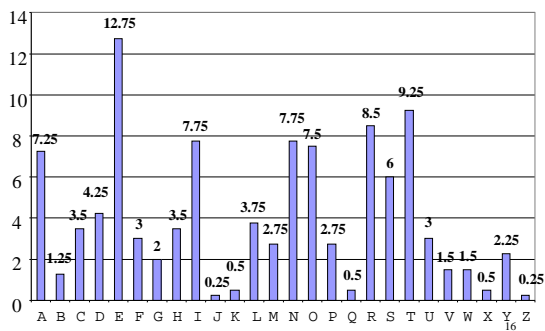


---



---

### Relative frequency of letters in a long English text by Stallings




---



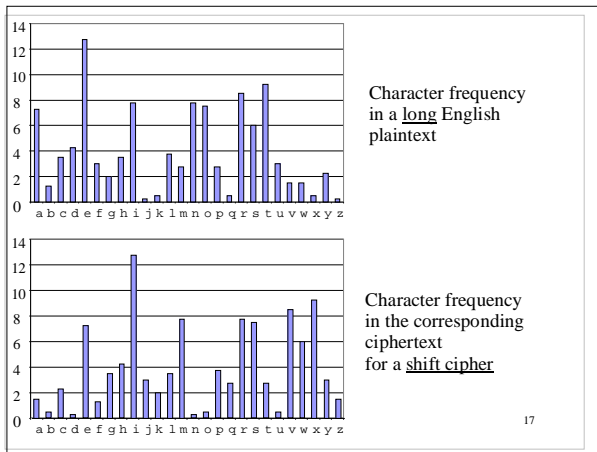
---



---



---




---



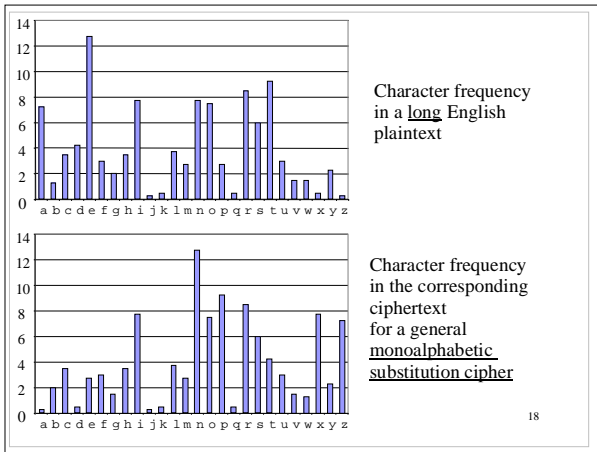
---



---



---




---



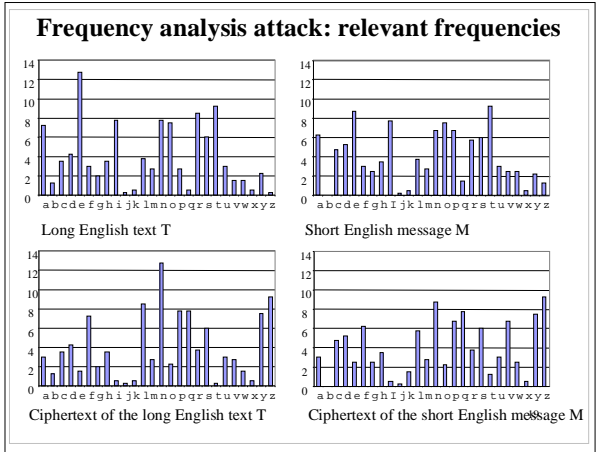
---



---



---




---



---



---



---

### Frequency analysis attack (1)

**Step 1:** Establishing the relative frequency of letters in the ciphertext

**Ciphertext:**

FMXVE DKAPH FERBN DKRXR SREFM ORUDS  
DKDVS HVUFE DKAPR KDLYE VLRHH RH

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  
= - ≡ ≡ ≡ ≡ ≡ ≡ - - - - = ≡ ≡ ≡ ≡ ≡ ≡ = ≡ = -

R - 8  
D - 7  
E, H, K - 5

20

---

---

---

---

---

---

### Frequency analysis attack (2)

**Step 2:** Assuming the relative frequency of letters in the corresponding message, and deriving the corresponding equations

**Assumption:** Most frequent letters in the message: E and T

**Corresponding equations:**

E → R      f(E) = R  
T → D      f(T) = D  
  
4 → 17      f(4) = 17  
19 → 3      f(19) = 3

21

---

---

---

---

---

---

### Frequency analysis attack (3)

**Step 3:** Verifying the assumption for the case of affine cipher

$$f(4) = 17$$

$$f(19) = 3$$



$$4 \cdot k_1 + k_2 \equiv 17 \pmod{26}$$

$$19 \cdot k_1 + k_2 \equiv 3 \pmod{26}$$



$$15 \cdot k_1 \equiv -14 \pmod{26}$$



$$15 \cdot k_1 \equiv 12 \pmod{26}$$

22

---

---

---

---

---

---

## Substitution Ciphers (2)

### 2. Polyalphabetic substitution cipher

$$M = \begin{matrix} m_1 & m_2 & \dots & m_d \\ m_{d+1} & m_{d+2} & \dots & m_{2d} \\ m_{2d+1} & m_{2d+2} & \dots & m_{3d} \\ \dots & \dots & \dots & \dots \end{matrix}$$

$$C = \begin{matrix} f_1(m_1) & f_2(m_2) & \dots & f_d(m_d) \\ f_1(m_{d+1}) & f_2(m_{d+2}) & \dots & f_d(m_{2d}) \\ f_1(m_{2d+1}) & f_2(m_{2d+2}) & \dots & f_d(m_{3d}) \\ \dots & \dots & \dots & \dots \end{matrix}$$

$d$  is a **period** of the cipher

$$\text{Key} = d, f_1, f_2, \dots, f_d$$

Number of keys for a given period  $d = (26!)^d \approx (4 \cdot 10^{26})^d$

---



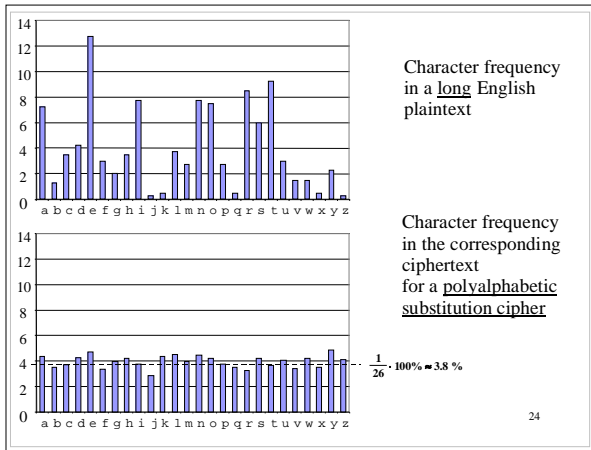
---



---



---




---



---



---



---

## Polyalphabetic substitution ciphers Simplifications (1)

### A. Vigenère cipher: polyalphabetic shift cipher

Invented in 1568

$$c_i = f_{i \bmod d}(m_i) = m_i + k_{i \bmod d} \bmod 26$$

$$m_i = f_{i \bmod d}^{-1}(c_i) = m_i - k_{i \bmod d} \bmod 26$$

$$\text{Key} = k_0, k_1, \dots, k_{d-1}$$

Number of keys for a given period  $d = (26)^d$

25

---



---



---



---

**Vigenère Square**

plaintext:     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

Key = "nsa"

3	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 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 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 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 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 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 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 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 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 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 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 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 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 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
1	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 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 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 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 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 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
2	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 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 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 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 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 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

26

---

---

---

---

---

---

---

---

**Vigenère Cipher - Example**

**Plaintext:** TO BE OR NOT TO BE

**Key:** NSA

**Encryption:**

T	O	B
E	O	R
N	O	T
T	O	B
E		
<hr style="width: 50%; margin: 0 auto;"/>		
G	G	B
R	G	R
A	G	T
G	G	B
R		

**Ciphertext:** GGBRGRAGTGGBR

27

---

---

---

---

---

---

---

---

**Determining the period of the polyalphabetic cipher  
Kasiski's method**

**Ciphertext:**     G G B R G R A G T G G B R

→  
Distance = 9

*Period d is a divisor of the distance between  
identical blocks of the ciphertext*

In our example: d = 3 or 9

28

---

---

---

---

---

---

---

---

### Index of coincidence method (1)

$n_i$  - number of occurrences of the letter  $i$  in the ciphertext

$i = a \dots z$

$N$  - length of the ciphertext

$p_i$  = frequency of the letter  $i$  for a long ciphertext

$$p_i = \lim_{N \rightarrow \infty} \frac{n_i}{N}$$

$$\sum_{i=a}^z p_i = 1$$

29

---

---

---

---

### Index of coincidence method (2)

Measure of roughness:

$$M.R. = \sum_{i=a}^z \left( p_i - \frac{1}{26} \right)^2 = \sum_{i=a}^z p_i^2 - \frac{1}{26}$$

**M.R.**    **0.028**   **0.014**   **0.006**   **0.003**

**period**   **1**       **2**       **5**       **10**

30

---

---

---

---

### Index of coincidence method (3)

Index of coincidence

The approximation of  $\sum_{i=a}^z p_i^2$

**Definition:**

Probability that two random elements of the ciphertext are identical

**Formula:**

$$I.C. = \sum_{i=a}^z \frac{\binom{n_i}{2}}{\binom{N}{2}} = \frac{\sum_{i=a}^z (n_i - 1) \cdot n_i}{(N - 1) \cdot N}$$

31

---

---

---

---

### Index of coincidence method (4)

Measure of roughness

$$M.R. = I.C. - \frac{1}{26} = \frac{\sum_{i=a}^z (n_i - 1) \cdot n_i}{(N-1) \cdot N} - \frac{1}{26}$$

<b>M.R.</b>	<b>0.028</b>	<b>0.014</b>	<b>0.006</b>	<b>0.003</b>
<b>period</b>	<b>1</b>	<b>2</b>	<b>5</b>	<b>10</b>

32

---



---



---



---

### Polyalphabetic substitution ciphers Simplifications (2)

**B. Rotor machines used before and during the WWII**

Country	Machine	Period
Germany:	Enigma	d=26·25·26 = 16,900
U.S.A.:	M-325, Hagelin M-209	
Japan:	“Purple”	
UK:	Typex	d=26·(26-k)·26, k=5, 7, 9
Poland:	Lacida	d=24·31·35 = 26,040

33

---



---



---



---

### Substitution Ciphers (3)

3. Running-key cipher

$$M = m_1 \quad m_2 \quad m_3 \quad m_4 \quad \dots \quad m_N$$

$$K = k_1 \quad k_2 \quad k_3 \quad k_4 \quad \dots \quad k_N$$

**K is a fragment of a book**

$$C = c_1 \quad c_2 \quad c_3 \quad c_4 \quad \dots \quad c_N$$

$$c_i = m_i + k_i \text{ mod } 26$$

$$m_i = c_i - k_i \text{ mod } 26$$

**Key:** book (title, edition), position in the book (page, row)

---



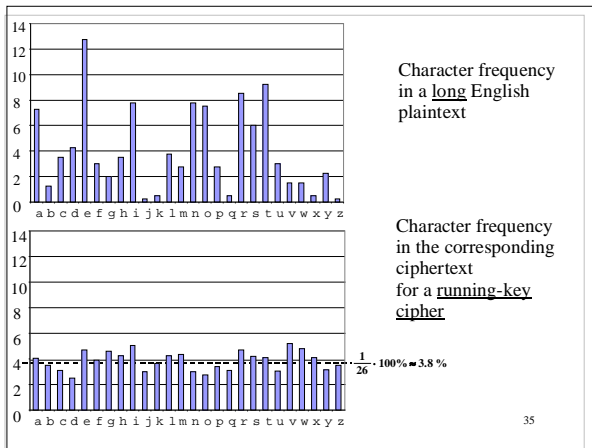
---



---



---




---



---



---



---

### Substitution Ciphers (4)

#### 4. Polygram substitution cipher

$$M = \begin{matrix} m_1 & m_2 & \dots & m_d & - & M_1 \\ m_{d+1} & m_{d+2} & \dots & m_{2d} & - & M_2 \\ m_{2d+1} & m_{2d+2} & \dots & m_{3d} & - & M_3 \\ \dots & \dots & \dots & \dots & & \dots \\ m_{(d-1)d+1} & m_{(d-1)d+2} & \dots & m_{(d-1)d} & - & M_{d-1} \\ m_{(d-1)d+1} & m_{(d-1)d+2} & \dots & m_{(d-1)d} & - & M_d \end{matrix}$$

$$C = \begin{matrix} c_1 & c_2 & \dots & c_d & - & C_1 \\ c_{d+1} & c_{d+2} & \dots & c_{2d} & - & C_2 \\ c_{2d+1} & c_{2d+2} & \dots & c_{3d} & - & C_3 \\ \dots & \dots & \dots & \dots & & \dots \\ c_{(d-1)d+1} & c_{(d-1)d+2} & \dots & c_{(d-1)d} & - & C_{d-1} \\ c_{(d-1)d+1} & c_{(d-1)d+2} & \dots & c_{(d-1)d} & - & C_d \end{matrix}$$

d is the length of a message block

$$C_i = f(M_i) \quad M_i = f^{-1}(C_i)$$

Key = d, f

Number of keys for a given block length d =  $(26^d)^{d!}$

---



---



---



---

### Playfair Cipher 1854

**Key:** PLAYFAIR IS A DIGRAM CIPHER

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

*Convention 1*

message	P	O	L	A	N	D
ciphertext	A	K	A	Y	Q	R

*Convention 2*

message	P	O	L	A	N	D
ciphertext	K	A	R	S	R	Q

37

---



---



---



---

## Hill Cipher

1929

### Ciphering:

$$C_{[1 \times d]} = M_{[1 \times d]} \cdot K_{[d \times d]}$$

$$(c_1, c_2, \dots, c_d) = (m_1, m_2, \dots, m_d) \begin{pmatrix} k_{11} & k_{12} & \dots & k_{1d} \\ \dots & \dots & \dots & \dots \\ k_{d1} & k_{d2} & \dots & k_{dd} \end{pmatrix}$$

*ciphertext block* = *message block* · *key matrix*

38

---

---

---

---

## Hill Cipher

### Deciphering:

$$M_{[1 \times d]} = C_{[1 \times d]} \cdot K^{-1}_{[d \times d]}$$

*message block* = *ciphertext block* · *inverse key matrix*

where

$$K_{[d \times d]} \cdot K^{-1}_{[d \times d]} = \begin{pmatrix} 1, 0, \dots, 0, 0 \\ 0, 1, \dots, 0, 0 \\ \dots & \dots & \dots & \dots \\ 0, 0, \dots, 1, 0 \\ 0, 0, \dots, 0, 1 \end{pmatrix}$$

*key matrix* · *inverse key matrix* = *identity matrix*

39

---

---

---

---

## Hill Cipher - Known Plaintext Attack (1)

### Known:

$$C_1 = (c_{11}, c_{12}, \dots, c_{1d}) \quad M_1 = (m_{11}, m_{12}, \dots, m_{1d})$$

$$C_2 = (c_{21}, c_{22}, \dots, c_{2d}) \quad M_2 = (m_{21}, m_{22}, \dots, m_{2d})$$

.....

$$C_d = (c_{d1}, c_{d2}, \dots, c_{dd}) \quad M_d = (m_{d1}, m_{d2}, \dots, m_{dd})$$

### We know that:

$$(c_{11}, c_{12}, \dots, c_{1d}) = (m_{11}, m_{12}, \dots, m_{1d}) \cdot K_{[d \times d]}$$

$$(c_{21}, c_{22}, \dots, c_{2d}) = (m_{21}, m_{22}, \dots, m_{2d}) \cdot K_{[d \times d]}$$

.....

$$(c_{d1}, c_{d2}, \dots, c_{dd}) = (m_{d1}, m_{d2}, \dots, m_{dd}) \cdot K_{[d \times d]}$$

40

---

---

---

---

### Hill Cipher - Known Plaintext Attack (2)

$$\begin{pmatrix} c_{11}, c_{12}, \dots, c_{1d} \\ c_{21}, c_{22}, \dots, c_{2d} \\ \dots \\ c_{d1}, c_{d2}, \dots, c_{dd} \end{pmatrix} = \begin{pmatrix} m_{11}, m_{12}, \dots, m_{1d} \\ m_{21}, m_{22}, \dots, m_{2d} \\ \dots \\ m_{d1}, m_{d2}, \dots, m_{dd} \end{pmatrix} \begin{pmatrix} k_{11}, k_{12}, \dots, k_{1d} \\ k_{21}, k_{22}, \dots, k_{2d} \\ \dots \\ k_{d1}, k_{d2}, \dots, k_{dd} \end{pmatrix}$$

$$C_{[d \times d]} = M_{[d \times d]} \cdot K_{[d \times d]}$$

$$K_{[d \times d]} = M^{-1}_{[d \times d]} \cdot C_{[d \times d]}$$

41

---



---



---



---

### Substitution Ciphers (5)

#### 4. Homophonic substitution cipher

$$M = \{ A, B, C, \dots, Z \}$$

$$C = \{ 0, 1, 2, 3, \dots, 99 \}$$

$$c_i = f(m_i, \text{random number})$$

$$m_i = f^{-1}(c_i)$$

$$f: E \rightarrow 17, 19, 27, 48, 64$$

$$A \rightarrow 8, 20, 25, 49$$

$$U \rightarrow 45, 68, 91$$

.....

$$X \rightarrow 33$$

42

---



---



---



---

### Transposition ciphers

$$M = m_1 \quad m_2 \quad m_3 \quad m_4 \quad \dots \quad m_N$$

$$C = m_{f(1)} \quad m_{f(2)} \quad m_{f(3)} \quad m_{f(4)} \quad \dots \quad m_{f(N)}$$

Letters of the plaintext are rearranged without changing them

43

---



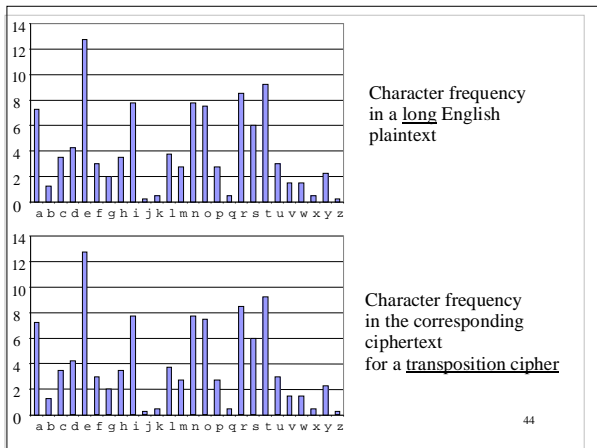
---



---



---




---



---



---

### Transposition cipher Example

**Plaintext:** CRYPTANALYST

**Key:** KRIS

**Encryption:**

	2 3 1 4
	K R I S
	C R Y P
	T A N A
	L Y S T

**Ciphertext:** YNSCTLRAYPAT

45

---



---



---



---

### One-time Pad Vernam Cipher

*Gilbert Vernam, AT&T* 1926  
*Major Joseph Mauborgne*

$$c_i = m_i \oplus k_i$$

$m_i$	01110110101001010110101
$k_i$	11011101110110101110110
$c_i$	10101011011111111000011

**All bits of the key must be chosen at random  
and never reused**

46

---



---



---



---

### One-time Pad Equivalent version

$$c_i = m_i + k_i \text{ mod } 26$$

$m_i$	TO	BE	OR	NOT	TO	BE
$k_i$	AX	TC	VI	URD	WM	OF
$c_i$	TL	UG	JZ	HFW	PK	PJ

All letters of the key must be chosen at random  
and never reused

47

---

---

---

---

---

### Perfect Cipher

Claude Shannon

*Communication Theory of Secrecy Systems, 1948*

$$\forall \begin{matrix} m \in M \\ c \in C \end{matrix} P(M=m | C=c) = P(M=m)$$

*The cryptanalyst can guess a message with  
the same probability without knowing a ciphertext  
as with the knowledge of the ciphertext*

48

---

---

---

---

---

### Is substitution cipher a perfect cipher?

$$C = XRZ$$

$$P(M=ADD | C=XRZ) = 0$$

$$P(M=ADD) \neq 0$$

49

---

---

---

---

---

### Is one-time pad a perfect cipher?

$$C = XRZ$$

$$P(M=ADD | C=XRZ) \neq 0$$

$$P(M=ADD) \neq 0$$

M might be equal to

*CAT, PET, SET, ADD, BBC, AAA, HOT,  
HIS, HER, BET, WAS, NOW, etc.*

50

---

---

---

---

### Key Sizes

- How many key bits are needed assuming that brute-force attacks are the only possible attacks.

key length	security estimation
56 – 64 bits	short term (a few hours or days)
112 – 128 bits	long term (several decades w/o quantum computers)
256 bits	long term (several decades even w/ quantum computers)

51

---

---

---

---

### Elements of Block Ciphers

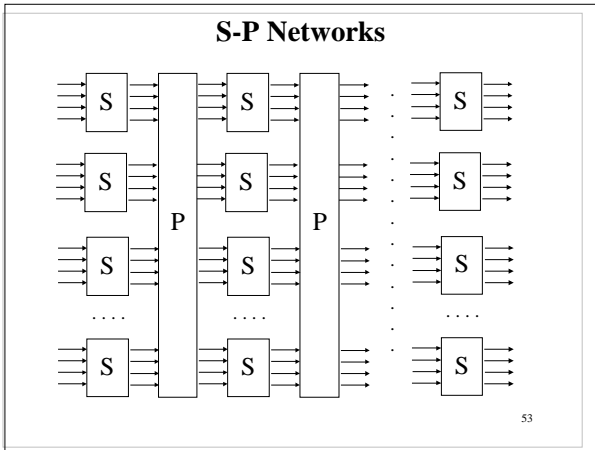
52

---

---

---

---




---



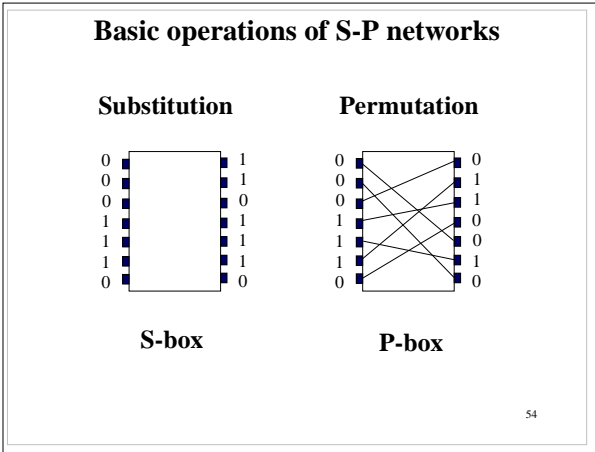
---



---



---




---



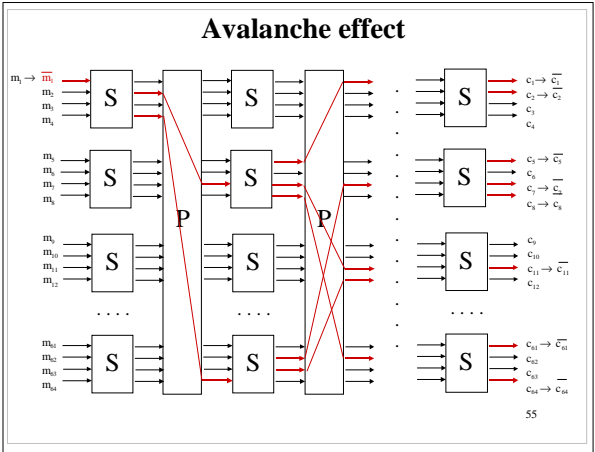
---



---



---




---



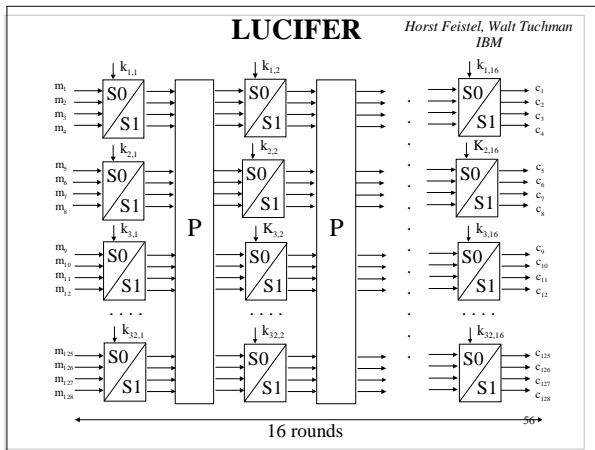
---



---



---




---

---

---

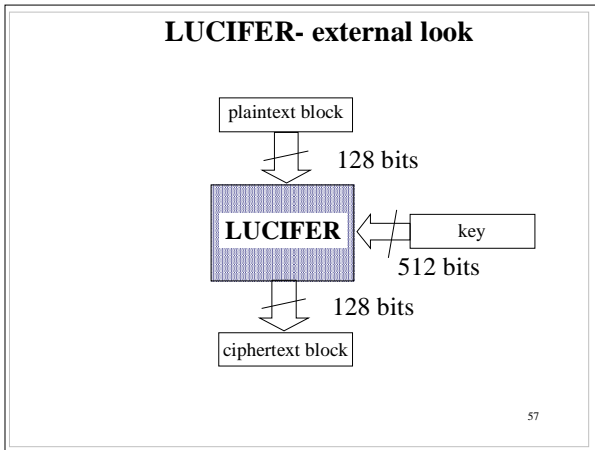
---

---

---

---

---




---

---

---

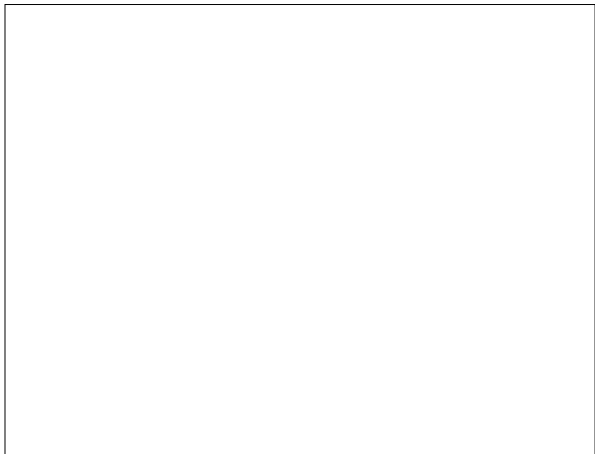
---

---

---

---

---




---

---

---

---

---

---

---

---