Computer and Network Security
- Security Technology Part 1 –
VER 2021

"So much has been said and so much has been gained; thousands of lives have been lost, and empires have fallen because a secret was not kept"

(Joseph Migga Kizza, author Guide to Computer Security)

The art of keeping secrets resulted in victories in wars and in growth of mighty empires

Security Issues

- Confidentiality:
  - hanya pengirim dan penerima (yang dituju saja) yang dapat “memahami” isi pesan.
- End-Point Authentication:
  - pengirim ingin membuktikan identitas penerima begitu juga sebaliknya.
- Message Integrity:
  - pengirim dan penerima ingin memastikan bahwa pesan tidak mengalami interferensi (saat transmisi atau sesudahnya) tanpa terdektesi.

Cryptography

- The increased use of computer and communications systems by industry has increased the risk of theft of proprietary information. Although these threats may require a variety of countermeasures, encryption is a primary method of protecting valuable electronic information.

By Communications Privacy: Federal Policy and Actions, General Accounting Office Report GAO/OSI-94-2, November 1993

The Purpose of Cryptography

Word cryptography originally came from Greek "Krypto (secret) and graphein (write)

"hidden writing" , therefore:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

Efforts to keep secrets have been made by humans probably since the beginning of humanity itself.

How It Works?

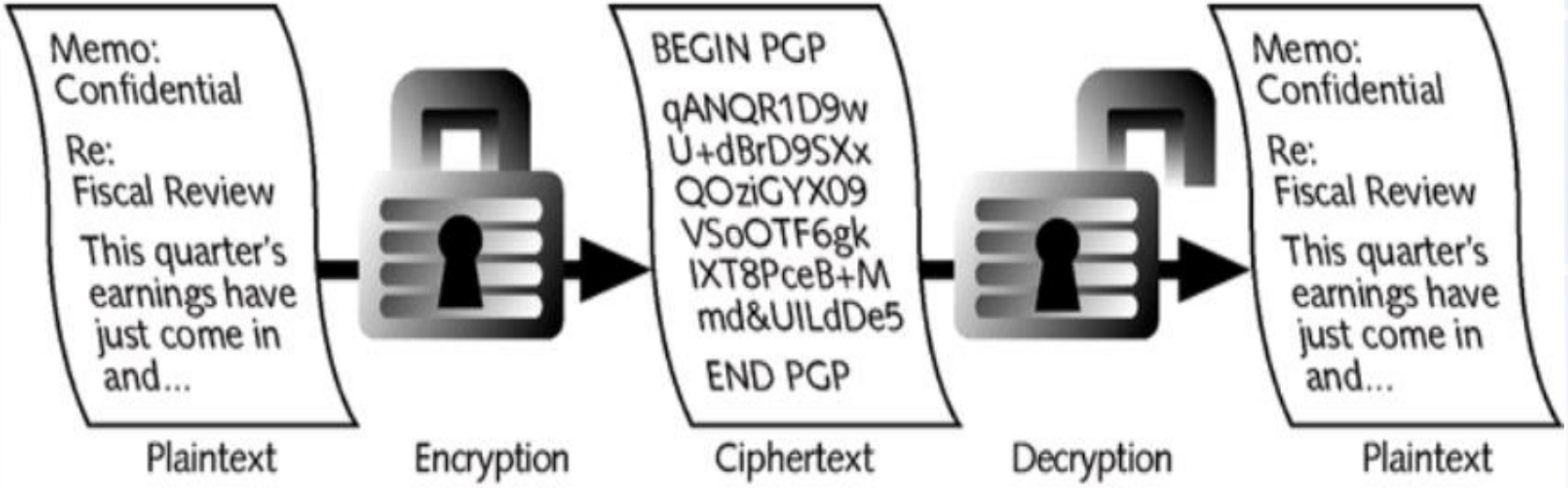


Figure 14-1 The encryption process

Terminology

- An original message is known as the **plaintext.**
- The process of converting from plaintext to ciphertext is known as **enciphering or encryption.**
- The coded message is called the **ciphertext.**
- restoring the plaintext from the ciphertext is **deciphering or decryption,**
- **Secret key** is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.

The word *cipher has its* origin in an Arabic word *sifr, meaning empty or zero.*

Characterized of Cryptography (1)

- **The type of operations used for transforming plaintext to ciphertext.**
  - **All encryption algorithms are based on two general principles: substitution,** *in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element*,

    and transposition, *in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost.*

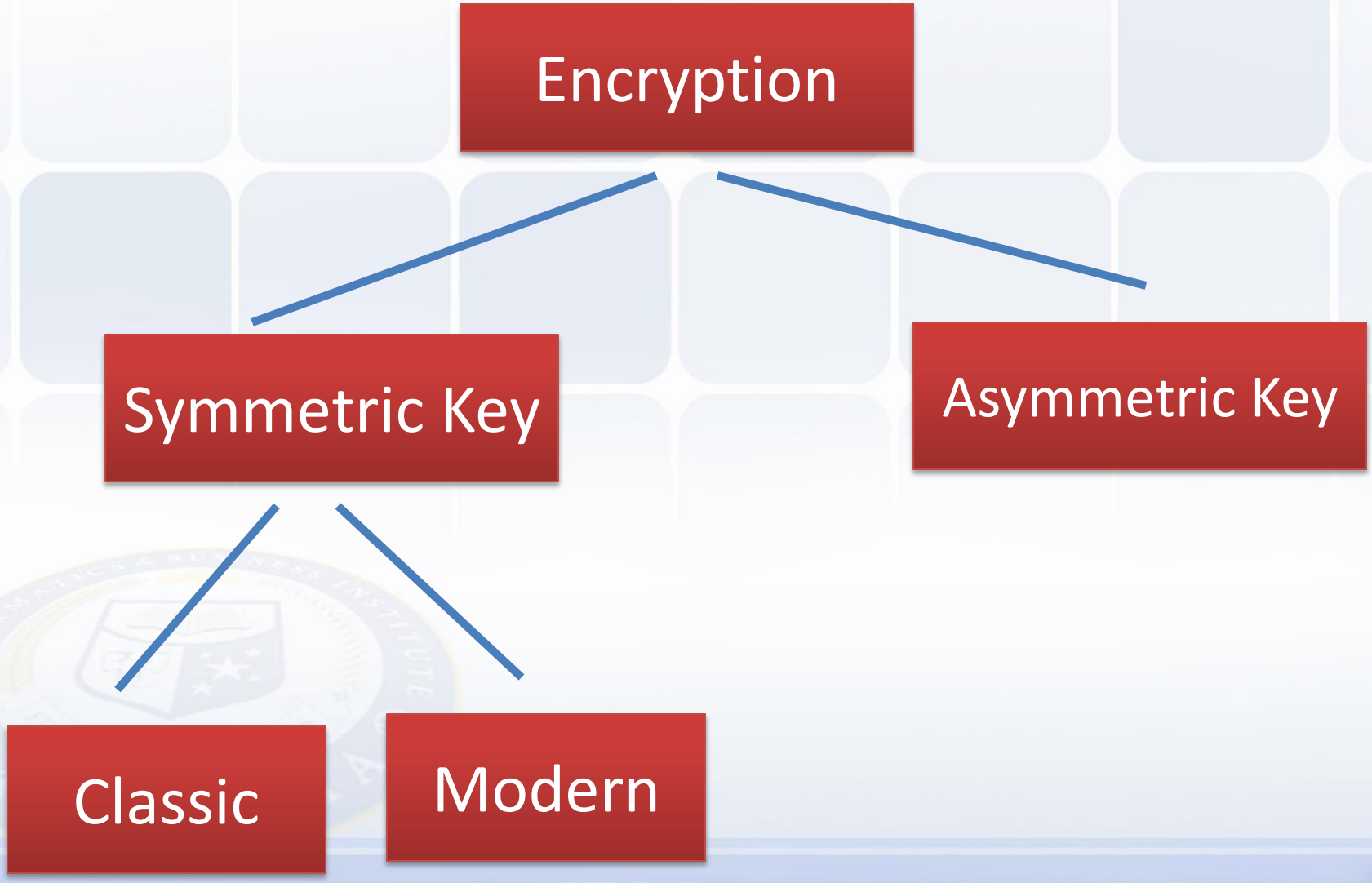
Characterized of Cryptography (2)

- **The number of keys used.**
  - **symmetric :**
    - *If both sender and receiver use the same key, the system is referred to as, single-key, secret-key, or conventional encryption.*
  - **asymmetric**
    - *If the sender and receiver use different keys, the system is referred to as, two-key, or public-key encryption*.

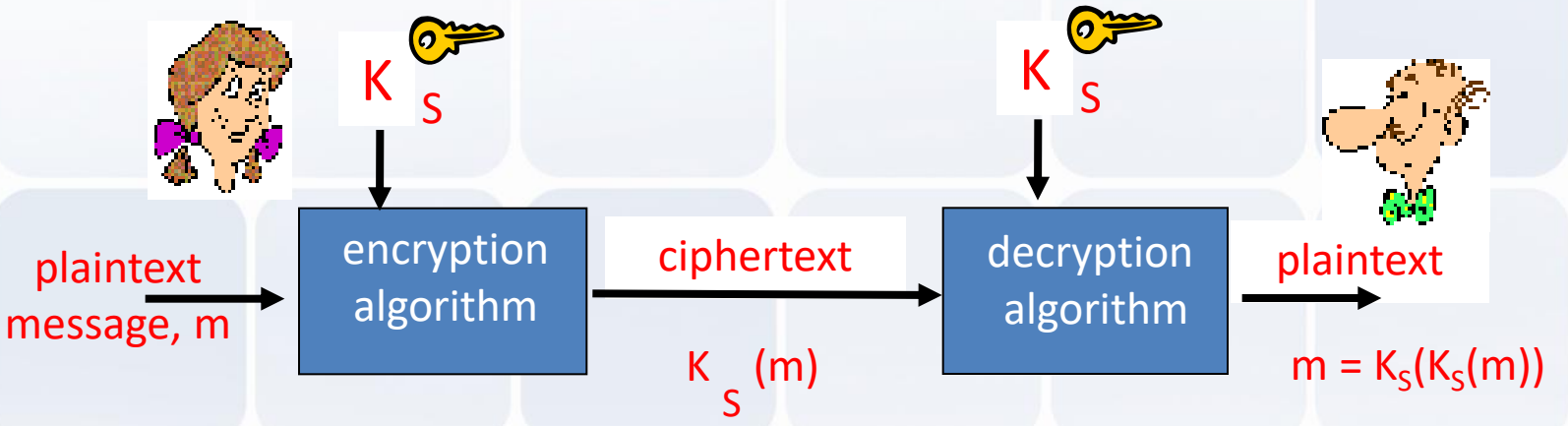
Characterized of Cryptography (3)

- **The way in which the plaintext is processed.**
  - **block cipher**
    - processes the input one block of elements at a time, producing an output block for each input block.
  - **stream cipher**
    - processes the input elements continuously, producing output one element at a time, as it goes along.

Cryptography



Symmetric Key



Example :

Twofish, Serpent, AES, Camellia, Blowfish, CAST5, RC4, DES, 3DES, Safer, IDEA, Salsa20, etc.

Classic/Traditional Cipher

- Basically : No computer needed, use pen and paper only.
- Algorithm :
  - Substitution Ciphers
  - Transposition Ciphers

Cipher Substitution - Caesar Cipher

- Replacing each letter of the alphabet with the letter standing three places further down the alphabet.

k: 3
p : MEET
c : PPHW

k : 3
p : THE PASSWORD IS SECRET
c: ?

k : 5
p : STAY SECRET
c: ?

Parameters and Design Features of A Symmetric Block Cipher

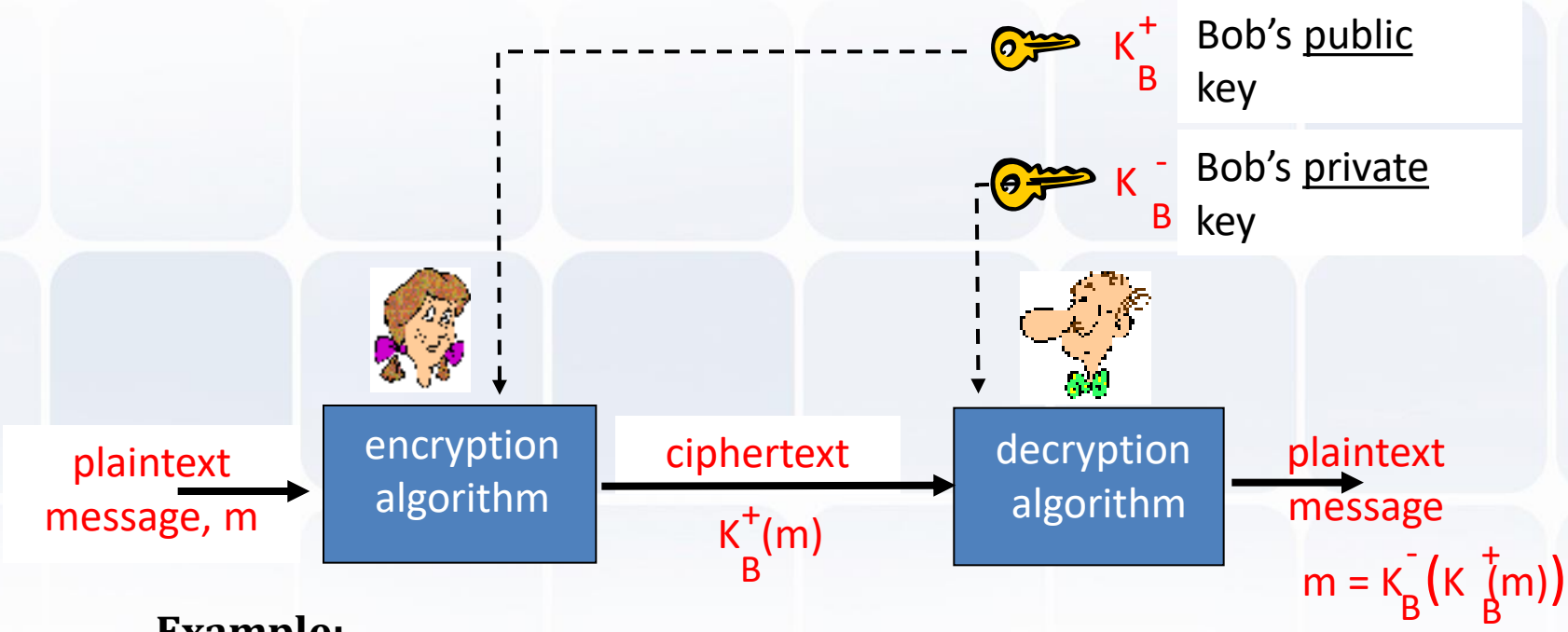
- **Block size:** Larger block sizes mean greater security (all other things being equal) but reduced encryption/decryption speed. A block size of 128 bits is a reasonable tradeoff and is nearly universal among recent block cipher designs.
- **Key size:** Larger key size means greater security but may decrease encryption/decryption speed. The most common key length in modern algorithms is 128 bits.
- **Number of rounds:** The essence of a symmetric block cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. A typical size is 16 rounds.
- **Subkey generation algorithm:** Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis.
- **Round function:** Again, greater complexity generally means greater resistance to cryptanalysis.

Symmetric Key

- Major Problem: How to distribute key securely or key exchange

- Brute-force attacks will methodically attempt to check each key until the key that decrypts the message is found. However, brute-force attacks are often impractical because the amount of time necessary to search the keys is greater than the useful life expectancy of the hidden information.

Asymmetric Key



Example:

- Diffie-Hellman
- RSA (Rivest-Shamir-Adleman of MIT)
- PGP (Phil Zimmerman of MIT)
- ECC (Elliptic Curve Cryptography)

- The private key should keep remain secret and only known by its owner.
- Public key is published widely.

Asymmetric Key

- The main problem: **speed.**
  - Public key calculations is longer than symmetric key calculations.
- It may leads to man in-the middle attack

Classic Chipertext

Shift Cipher

Assign a numerical equivalent to each letter.

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9

K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

Plaintext : we will meet at midnight

Become (A_1) : 22 4 22 8 11 11 12 4 4 10 0 19
12 8 3 13 8 6 7 19

Shift Cipher (1)

- If known Key (k) = 11
- Ci = k + A_1

  = 7 15 7 …….

  if K + A_1 > 25, then uses modulo concept

- Then the Ci =

  H P H ……

Shift Cipher (2)

- If k = 16
- p : LAW AND ORDER
- Ci = ?

Monoalphabetic Ciphers (1)

- The "cipher" line can be *any permutation* of the 26 alphabetic characters.
- A single cipher alphabet (mapping from plain alphabet to cipher alphabet)

Monoalphabetic Ciphers (2)

- Pt : abcdefghijklmnopqrstuvwxyz
- Kt : DKVQFIBJWPESCXHTMYAUOLRGZN

Then :

- Pt : The Password is Secret
- Kt : ?

Vigenère Cipher (1)

- In addition to the plaintext, the Vigenère cipher also requires a keyword, which is repeated so that the total length is equal to that of the plaintext.
- For example, suppose the plaintext is IBI DARMAJAYA, and the keyword is HEBAT.

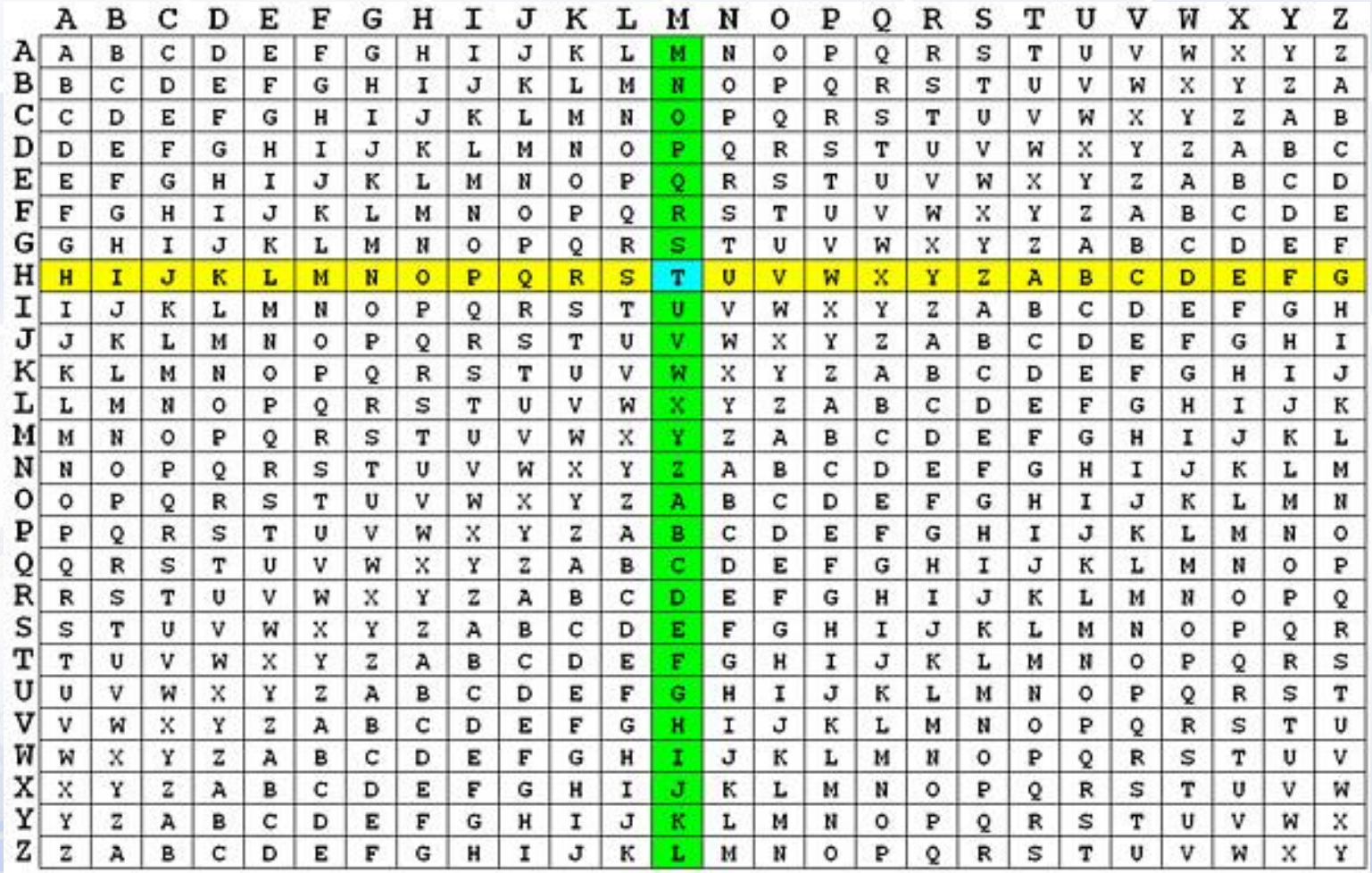
Vigenère Cipher (2)

- To encrypt, pick a letter in the plaintext and its corresponding letter in the keyword, use the keyword letter and the plaintext letter as the row index and column index, respectively, and the entry at the row-column intersection is the letter in the ciphertext.
- For example, the first letter in the plaintext is **I** and its corresponding keyword letter is **H**.

Vigenère tableau

keywords

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
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

Vigenère Cipher (3)

- p(t) = we will
- k = secret
- c(t) = OI YZPE

Vigenère Cipher

- plaintext: we are discovered save yourself
- Key : *deceptive*
- Cipher : ?

Answer :

- plaintext: ?
- key: *?*
- ciphertext: ?

Vigenère Cipher (4)

p(t) = I B I D A R M A J A Y A

k = H E B A T

c(t) = ?

Playfair Cipher (1)

- Invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair.
- Based on the use of a 5 x 5 matrix of letters constructed using a 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

Playfair (2)

plaintext is encrypted two letters at a time

- if a pair is a repeated letter, insert filler like **'X'** so that **balloon** would be treated as **ba lx lo on**.
- if both letters fall in the same row, replace each with letter to right (wrapping back to start from end). For example, **ar** is encrypted as RM.
- if both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom). For example, **mu** is encrypted as **CM**.
- otherwise each letter is replaced by the letter in **the same row** and **in the column of the other** letter of the pair. Thus, **hs** becomes **BP** and **ea** becomes **IM** (or **JM**, as the encipherer wishes).

Playfair (3)

- If p(t) = sometime
- k = monarchy
- C(t) = ?
- Answer =
- SO = PA
- ME = CL
- TI = SK
- ME= CL

Playfair (4)

- If p(t) = password and secret
- k = trust
- C(t) = ?

Hill Cipher

$$\begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{14} & K_{33} \end{pmatrix} x \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \mod 26 \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix}$$

- p(t) : Semoga
- c(t) : ?
- Key : $\begin{pmatrix} 3 & 1 & 2 \\ 5 & 1 & 3 \\ 2 & 4 & 7 \end{pmatrix}$

Hill Cipher

ARRANGE => SEMOGA = SEM
OGA

SEM = 18 4 12

Then :

$$\begin{pmatrix} 3 & 1 & 2 \\ 5 & 1 & 3 \\ 2 & 4 & 7 \end{pmatrix} x \begin{pmatrix} 18 \\ 4 \\ 12 \end{pmatrix} = \begin{pmatrix} 54 & 4 & 24 \\ 90 & 4 & 36 \\ 36 & 16 & 84 \end{pmatrix} = \begin{pmatrix} 82 \\ 130 \\ 136 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 \\ 0 \\ 6 \end{pmatrix} = \begin{pmatrix} E \\ A \\ G \end{pmatrix}$$

Hill Cipher

OGA = 14 6 0

Then :

$$\begin{pmatrix} 3 & 1 & 2 \\ 5 & 1 & 3 \\ 2 & 4 & 7 \end{pmatrix} x \begin{pmatrix} 14 \\ 6 \\ 0 \end{pmatrix} = \begin{pmatrix} 42 & 6 & 0 \\ 70 & 6 & 0 \\ 28 & 24 & 0 \end{pmatrix} = \begin{pmatrix} 48 \\ 76 \\ 52 \end{pmatrix} \bmod 26 = \begin{pmatrix} 22 \\ 24 \\ 0 \end{pmatrix} = \begin{pmatrix} W \\ Y \\ A \end{pmatrix}$$

So, c(t) : EAG WYA

Hill Cipher

- P(t) : PASSWORD AND SECRET
- Key : $\begin{pmatrix} 5 & 1 & 2 \\ 2 & 1 & 3 \\ 1 & 3 & 6 \end{pmatrix}$
- C(t) : ????

Transposition Cipher

- Permutation Technique

1	2	3	4	5	6
3	5	1	6	4	2

- Plaintext : SAYA SEDANG BELAJAR KEAMANAN KOMPUTER

  : SAYASE DANGBE LAJARK EAMANA NKOMPU TERXXX

  Ciphertext : YSSEAA NBDEGA JRLKAA MNEAAA OPNUMK RXTXXE

Find the Plaintext

- UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
- VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
- EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

How?

1. Determines the relative frequency of the letters.

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				

Note :
- If the message were long enough, this technique alone might be sufficient,
- we cannot expect an exact match

How ?

2. compared to a standard frequency distribution for English.

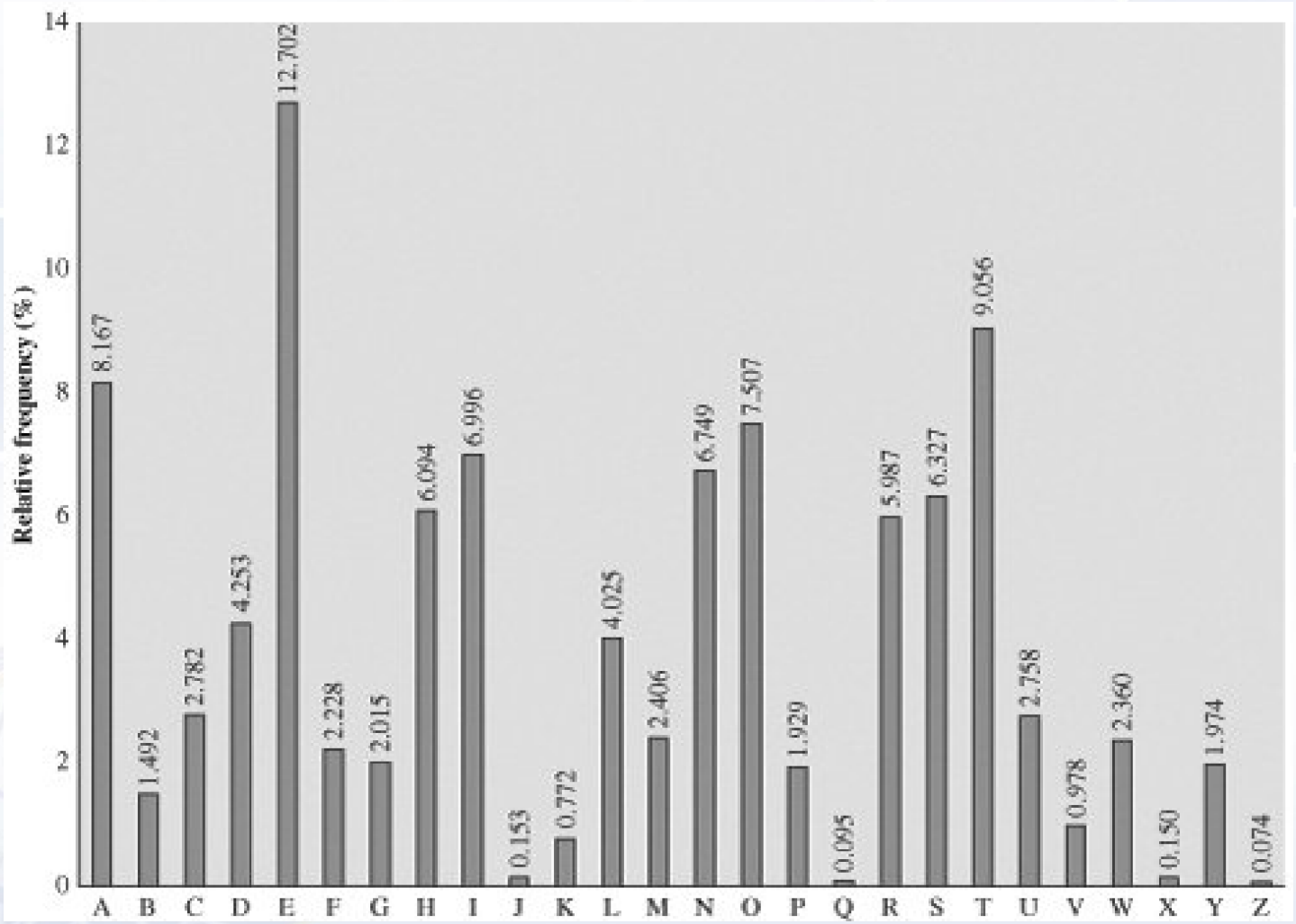


Figure Relative Frequency of Letters in English Text

How ?

Compare Result :

- cipher letters P and Z are likely equivalents with plain letters e and t (but it is not certain which is which).
- 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}.
- The letters with the lowest frequencies (namely, A, B, G, Y, I, J) are likely included in the set {b, j, k, q, v, x, z}.

How ?

So far we got :

- UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
- t a e e te a that e e a a
- VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
- e t ta t ha e ee a e th t a
- EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
- e e e tat e the t

How ?

Finally :

- it was disclosed yesterday that several informal but
- direct contacts have been made with political
- representatives of the viet cong in moscow

END