Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

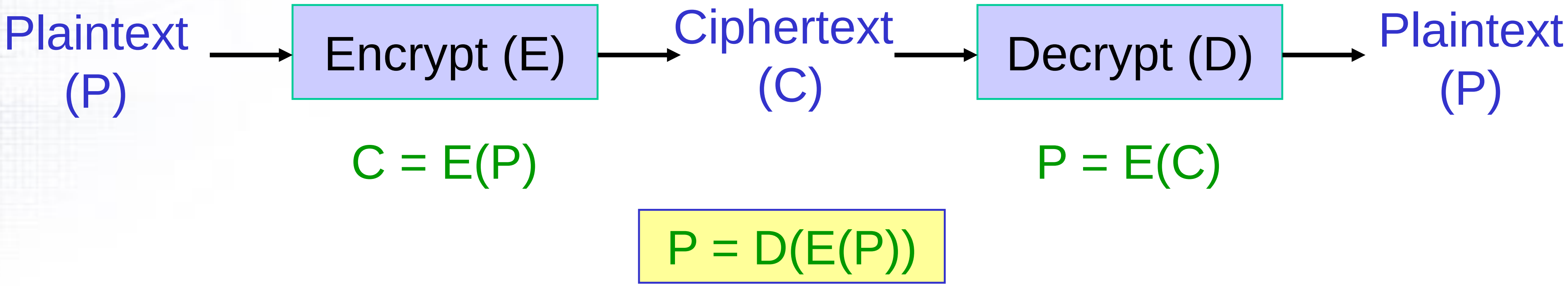
Lecture 1. Overview of Cryptography

§ 1.1 History of Cryptography

Slides for a Course Based on the Text
密碼學與網路安全
by 王旭正、柯宏叡

Introduction

- Cryptography：From the Greek for “hidden word” (Kryptós lógos)
  - A war over 3000 years: “Cryptography” (密碼學) vs. “Cryptanalysis” (破密學)



Plaintext (P) → Encrypt (E) → Ciphertext (C) → Decrypt (D) → Plaintext (P)

$C = E(P)$

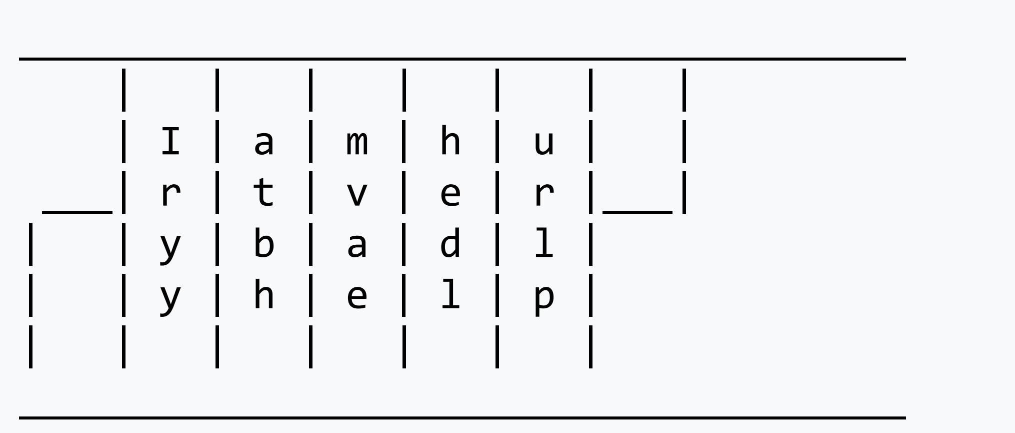
$P = E(C)$

$$\boxed{P = D(E(P))}$$

Transposition Cipher

Transposition Cipher (轉移密碼法)

- 5th C. B.C.：Scytale (斯巴達密碼棒)
  - Ex: The plaintext = “I am hurt very badly help”.



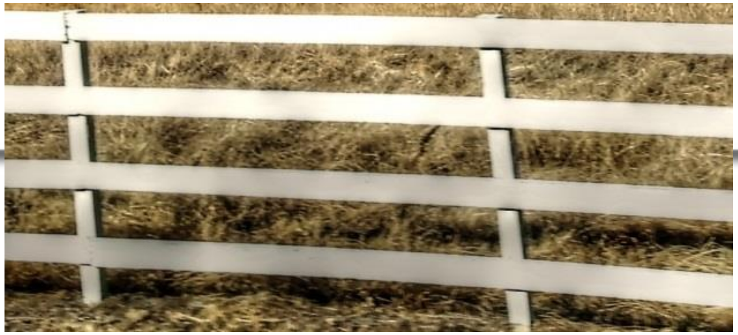
```
______________________________________
    |   |   |   |   |   |   |
    | I | a | m | h | u |   |
 ___| r | t | v | e | r |___|
|   | y | b | a | d | l |
|   | y | h | e | l | p |
|   |   |   |   |   |   |

______________________________________
```

The ciphertext = “Iryyatbhmvaehedlurlp”.

From: https://en.wikipedia.org/wiki/Scytale#/media/File:Skytale.png

Transposition Cipher



- Rail-fence Cipher (籬笆密碼法)
  - Ex: The plaintext = “WE ARE DISCOVERED. RUN AT ONCE.” with 6 "rails":

```
W.........V.........O
.E.......O.E.......T.N
..A.....C...R.....A...C
...R...S.....E...N.....E
....E.I.......D.U.......X
.....D.........R.........X
```

$24 + x = 6 + 5(y - 1),\ 0 \leq x < 6 \Rightarrow 23 = 5y - x$
$\Rightarrow y = 5,\ x = 2.$

$26 = 6 + 5(y - 1) \Rightarrow y = 5 \Rightarrow$ first, last = 3, others = 5

The ciphertext = “WVO EOETN ACRAC RSENE EIDU DR”,

or: “WVOEOETNACRACRSENEEIDUXDRX”.

Substitution Cipher

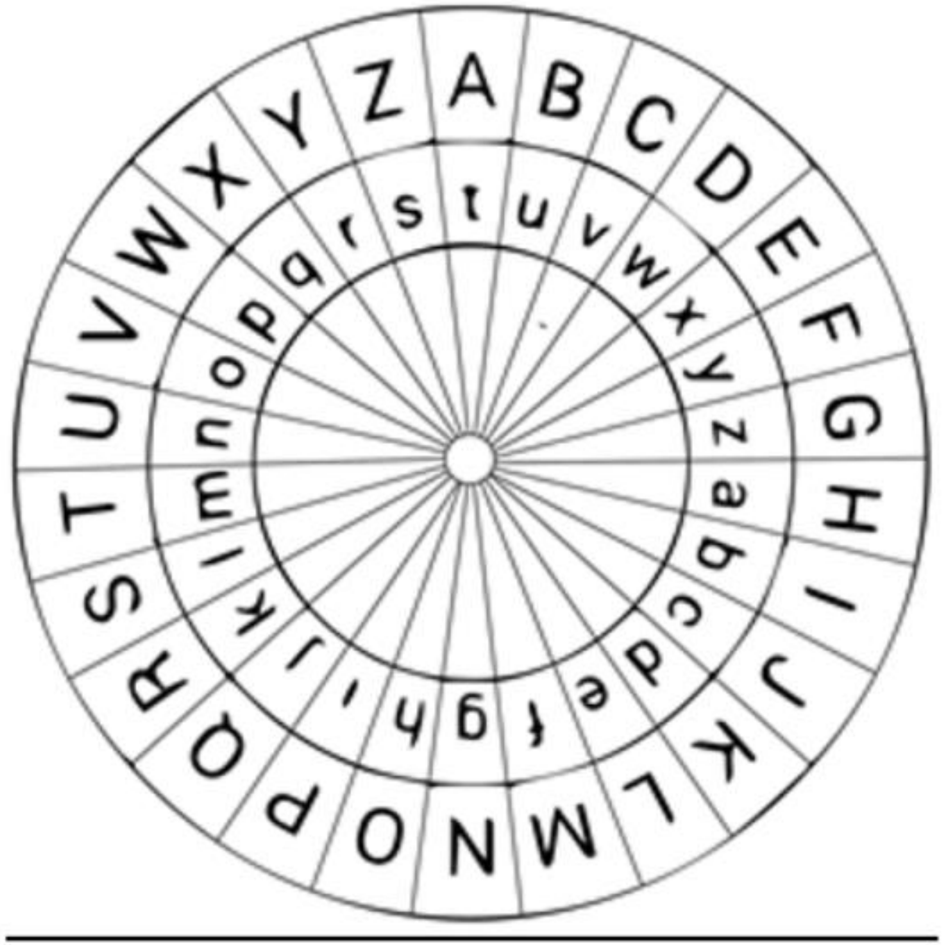
Substitution Cipher (

- 4th C. B.C. ： Ancient et letters. Each letter is replaced with another le
- 1th C. B.C. ： Caesar 碼法)
  - Ex: Key = D:

A	B		T	U	V	W	X	Y	Z
D	E		W	X	Y	Z	A	B	C

The plaintext = “

The ciphertext = KHU”.



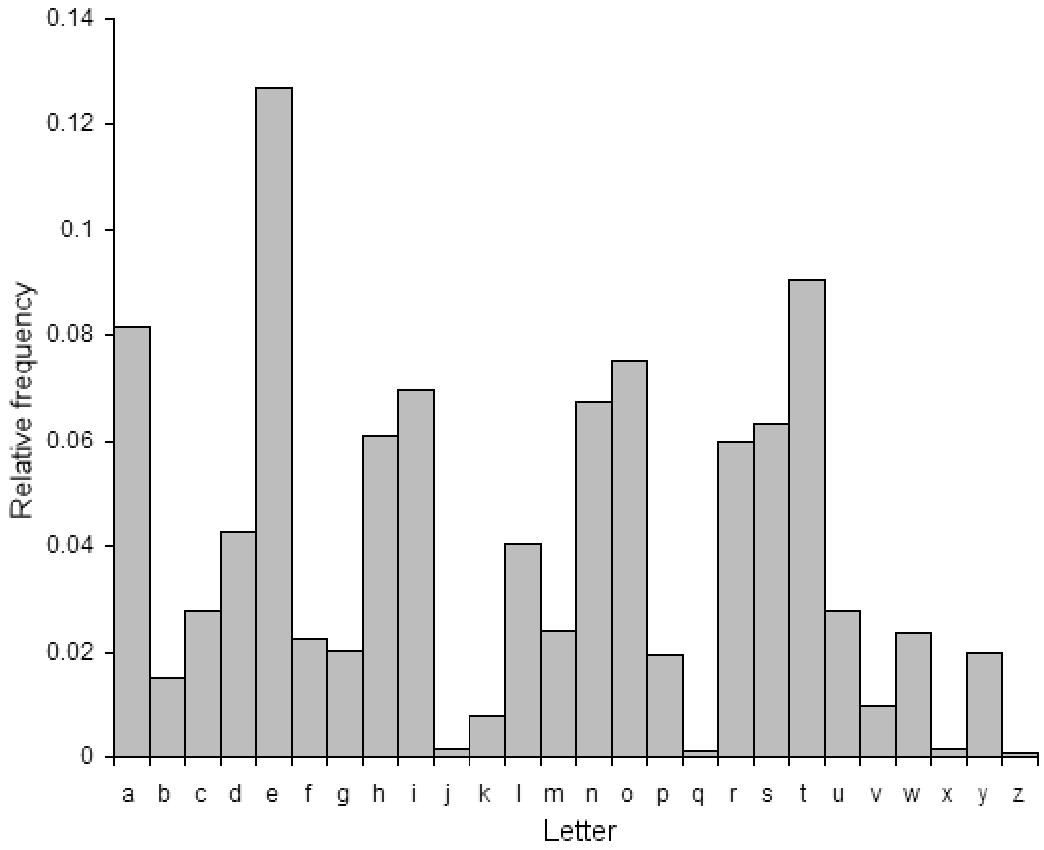
A Caesar Wheel

- Mixed alphabet or de
  - Ex: keyword “math".

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

Substitution Cipher

- A mono-alphabetic cipher (單一字元替代密碼法) uses fixed substitution over the entire message, whereas a poly-alphabetic cipher (多元式字元替代密碼法) uses a number of substitutions at different positions in the message, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext and vice versa.
- 9th Century: Arab Al-Kindi (c. 801–873, also known as “Alkindus” in Europe) ： Frequency Analysis (頻率分析法).

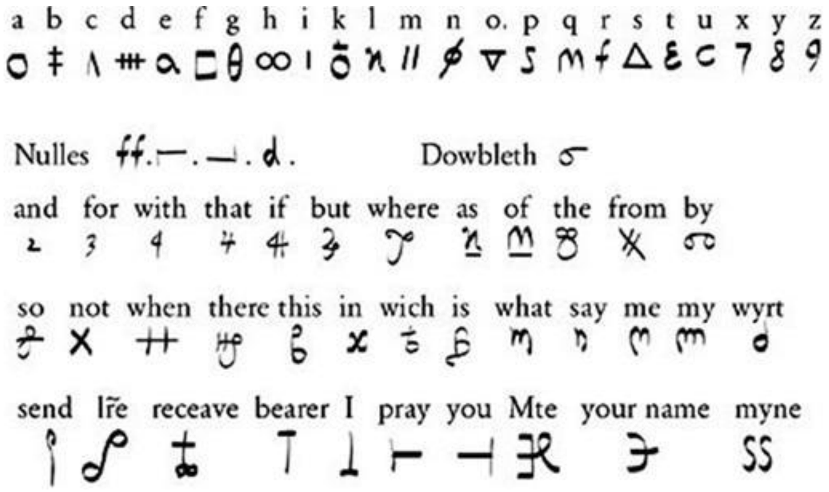


Substitution Cipher

- Add Null：can be used in real world!
- Deliberately misspell some words
- Codeword Substitution Cipher (字碼替代密碼法)： too complicated.
- Nomenclator Cipher (命名密碼法)
  - Ex: How Cryptology Killed Mary Queen of Scots.

    http://5010.mathed.usu.edu/Fall2014/KKing/sigmary.html

    (In 1587, the cryptanalyst won.)


a b c d e f g h i k l m n o p q r s t u x y z
Nulles
Dowbleth
and for with that if but where as of the from by
so not when there this in wich is what say me my wyrt
send lre receave bearer I pray you Mte your name myne

Substitution Cipher

- Vigènere Cipher (維吉尼爾密碼法)：Poly-alphabetic substitution cipher
  - Ex: The plaintext = “You should sleep early”.

Key = NOW:

	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
⋮													⋮													
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
⋮													⋮													
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
⋮													⋮													
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

The ciphertext = “LCQ FVKHZZ FZARD ANFHL”.

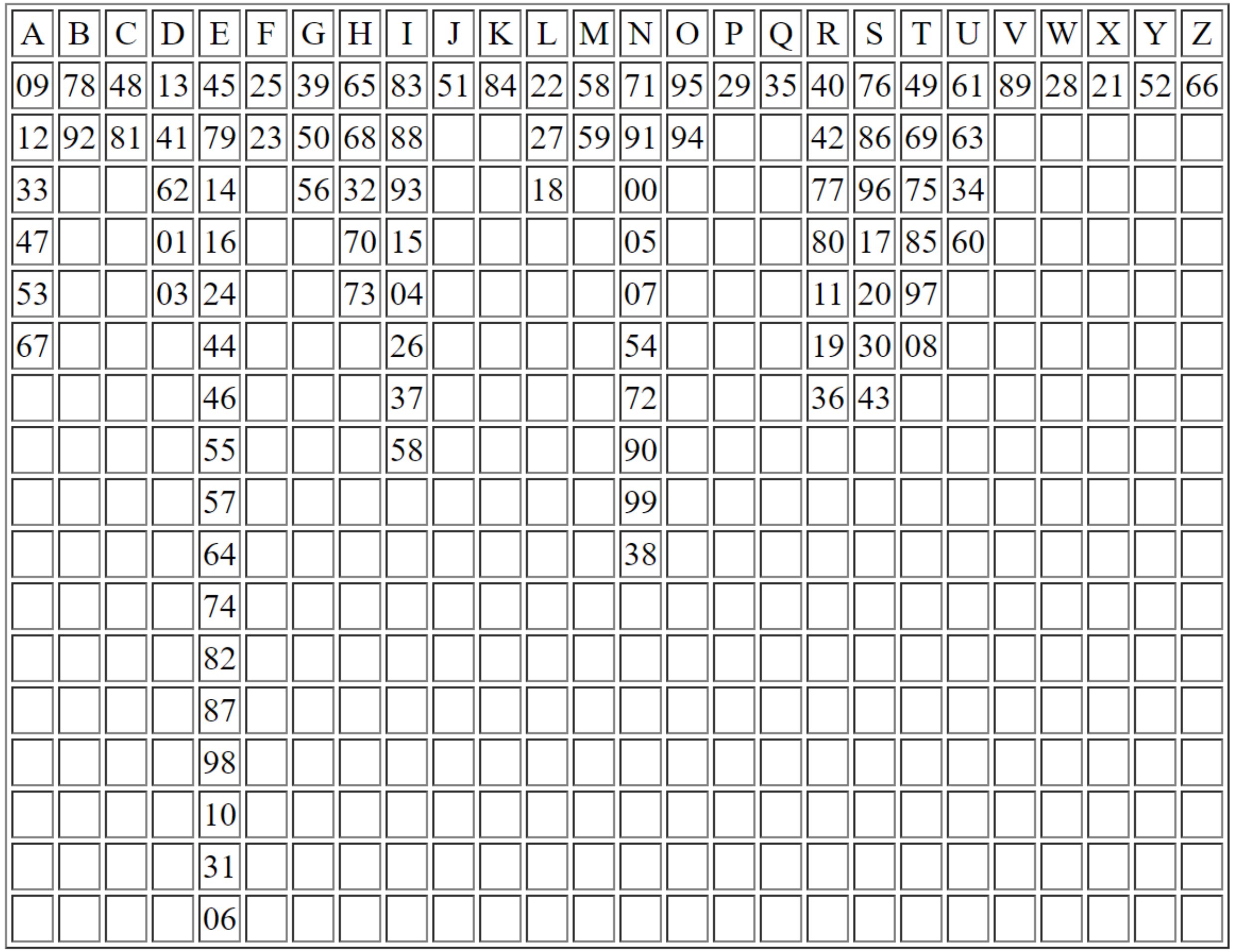
Substitution Cipher

- 19th Century：Kasiski Test (卡斯楚測試)
  - Ex:
    1. After analyzing the ciphertext, it is found that "AB", "PQR", and "UVWX" are repeated several times, and the distances between them are 21, 7, and 28, respectively.
    2. Then it can be judged that the length of the key is about 7 (GCD of them).
    3. Collect the ciphertext every seven letters, and partition the ciphertext into seven segments.
    4. Use Frequency Analysis for each segment.

Substitution Cipher

- Homophonic Substitution Cipher (等價替代字碼法) – Mono-alphabetic substitution cipher.
  - Ex: The plaintext = “CRYPTOGRAPHY IS VERY INTERESTING”.

    The ciphertext = “48 40 52 29 49 95 39 42 09 29 65 52 83 76 89 45 77 52 88 71 69 79 80 14 86 75 93 91 50”.



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
09	78	48	13	45	25	39	65	83	51	84	22	58	71	95	29	35	40	76	49	61	89	28	21	52	66
12	92	81	41	79	23	50	68	88			27	59	91	94			42	86	69	63					
33			62	14		56	32	93			18		00				77	96	75	34					
47			01	16			70	15					05				80	17	85	60					
53			03	24			73	04					07				11	20	97						
67				44				26					54				19	30	08						
				46				37					72				36	43							
				55				58					90												
				57									99												
				64									38												
				74																					
				82																					
				87																					
				98																					
				10																					
				31																					
				06																					

Substitution Cipher

- In WW2：One-time Pad Cipher (單次金鑰使用密碼法)：|Key| = |plaintext|
  - Perfect Security / Theoretical Security
  - Ex: The plaintext = “MEET ME OUTSIDE”.

Plaintext (P)	M	E	E	T	M	E	O	U	T	S	I	D	E
Numerical P	12	4	4	19	12	4	14	20	19	18	8	3	4
OTP	B	D	U	F	G	H	W	E	I	U	F	G	W
Numerical OTP	1	3	20	5	6	7	22	4	8	20	5	6	22
Numerical C	13	7	24	24	18	11	10	24	1	12	13	9	0
Ciphertext (C)	N	H	Y	Y	S	L	K	Y	B	M	N	J	A

BDUFGHWEIUFGWDL
KNFLNDKLFNLKIREU
POWQIRINMAHJWOC
IEMBRIWODSNGKDA
KEWPCWIDCNFLPQX

Page 1

The ciphertext = “NHYYSLKYBMNJA”.

Contemporary Cryptography

Contemporary Cryptography (近代密碼學)

- 1977：Data Encryption Standard, DES (資料加密標準)：Horst Feistel, NBS (NIST).
- 1976：Public-key Cryptography：Diffie and Hellman
- 1978：RSA：Rivist, Shamir and Adleman
- 2000：Advance Encryption Standard, AES (新加密標準)：Rijndael
- 1984：Quantum Cryptography (量子密碼)：Stephen Weisner

Steganography

- Physical
  - Secret inks
  - Hide (in the area of stamp, on the slave‘s head, …)
  - Morse code
  - Null cipher (空密碼)
    - Ex: “*News Eight Weather: Tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The[highway is not]knowingly slippery. Highway evacuation is suspected. Police report emergency situations in downtown ending near Tuesday.*”

      Message: “Newt is upset because he thinks he is President”.

Steganography

- Physical
  - Null cipher (空密碼)
    - Ex: A Puzzle for Inspector M
      (Source: "The Silent World
      Nicholas Quinn", by *Colin*

Dear George, 3rd March

r your
ckage.
ready
ay
st.
room
or three
ıse
troy

ly,

Dear George, 3rd March

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final dispatch to the Syndicate by Friday 20th or at the very least, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours,

Steganography

- Digital
  - Text, Sound, Picture, Media, or Printed (hide the ciphertext).

Information Hiding：Covert Channels (隱藏式通道), Steganography (隱寫術), Anonymity (匿名法), Copyright Marking (版權標記).

- Watermarking (數位浮水印) vs. Steganography

- Visual Cryptography (視覺密碼) vs. Steganography

Steganography

- HW1: In one of Dorothy Sayers’ mysteries, Lord Peter is confronted with the following message:

I thought to see the fairies in the fields, but I saw only the evil elephants with their black backs. Woe! how that sight awed me! The elves danced all around and about while I heard voices calling clearly. Ah! how I tried to see--throw off the ugly cloud--but no blind eye of a mortal was permitted to spy them. So then came minstrels, having gold trumpets, harps and drums. These played very loudly beside me, breaking that spell. So the dream vanished, whereat I thanked Heaven. I shed many tears before the thin moon rose up, frail and faint as a sickle of straw. Now though the Enchanter gnash his teeth vainly, yet shall he return as the spring returns. Oh, wretched man! Hell gapes, Erebus now lies open. The mouths of Death wait on thy end.

He also discovers the key to the message, which is a sequence of integers:

787656543432112343456567878878765654
3432112343456567878878765654433211234

Steganography

- HW1:
  (a) Decrypt the message. [Hint: What is the largest integer value?]
  (b) If the algorithm is known but not the key, how secure is the scheme?
  (c) If the key is known but not the algorithm, how secure is the scheme?

Computer Science and Information Engineering
National Chi Nan University

The Principle and Application of Secret Sharing

Dr. Justie Su-Tzu Juan

Lecture 1. Overview of Cryptography

§ 1.2 Contemporary Cryptography (1)

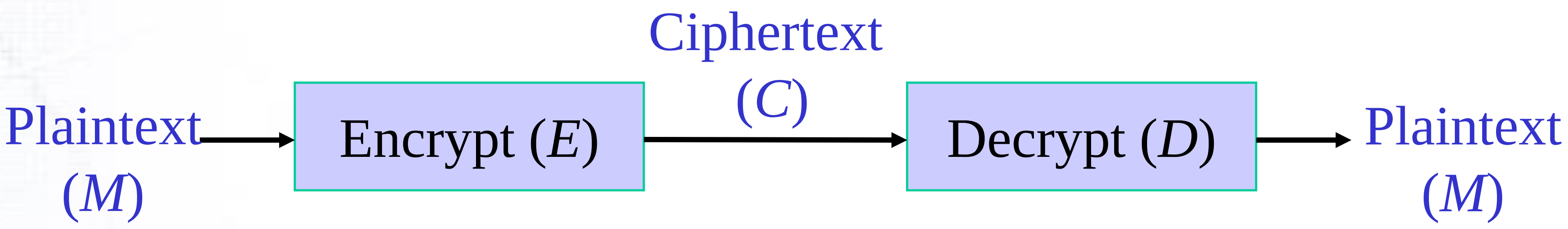
Slides for a Course Based on the Text
近代密碼學及其應用
by 賴溪松、韓亮、張真誠

Goals of Cryptography

- CONFIDENTIALITY (秘密性) (or SECRECY, or PRIVACY)
  - Keep information secret
- AUTHENTICATION (鑑定性)
  - Receiver can verify who sender was
- INTEGRITY (完整性)
  - Detect modified messages
- NON-REPUDIATION (不可否認性)
  - Sender cannot later falsely deny sending a message. (Receiver cannot falsely deny receiving it.)

Cryptography Systems

Cryptography Systems (密碼系統)



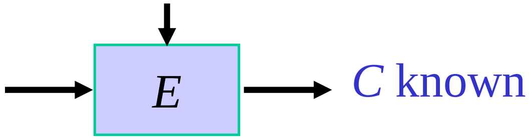
$C = E_{k1}(M)$ $M = E_{k2}(C)$

$$\boxed{M = D_{k2}(E_{k1}(M))}$$

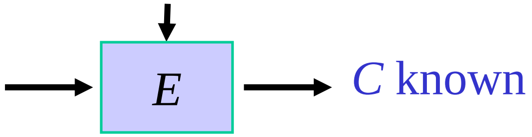
- When $k_1 = k_2$：Symmetric Key Cryptosystem (對稱金鑰密碼系統)、One-key Cryptosystem (單一金鑰密碼系統)、Private Key Cryptosystem (秘密金鑰密碼系統)、Conventional cryptosystem (傳統密碼系統)
- When $k_1 \neq k_2$：Asymmetric Cryptosystem (非對稱密碼系統)、Two Key Cryptosystem (雙金鑰密碼系統)、Public Key Distribution System (公開金鑰分配系統)

Types of Attacks

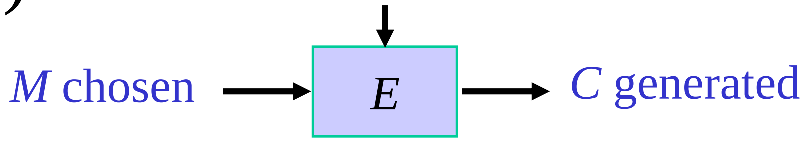
- Ciphertext-Only Attack (密文攻擊法)

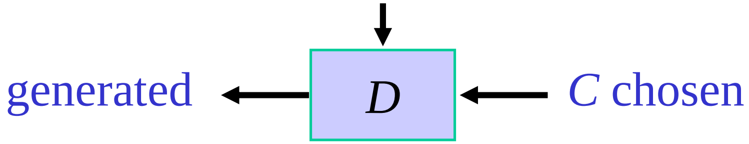


- Known-Plaintext Attack (已知明文攻擊法)



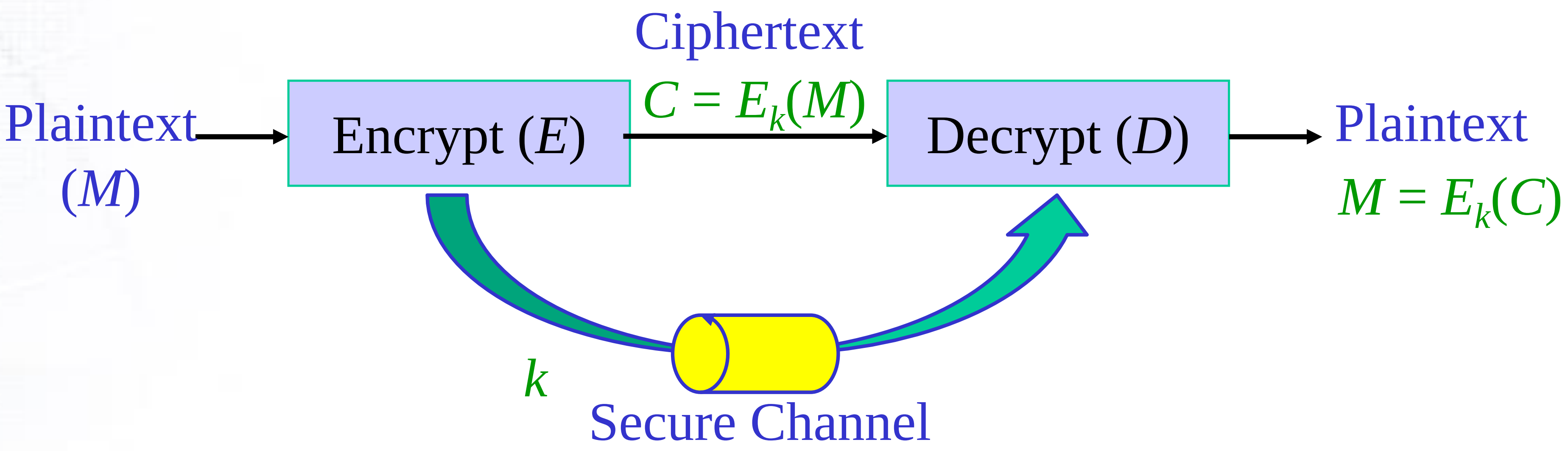
- Chosen-Text Attack (選擇文攻擊法)
  - Chosen-Plaintext Attack
  - Chosen-Ciphertext Attack





Symmetric Key Cryptosystem

Symmetric Key Cryptosystem:



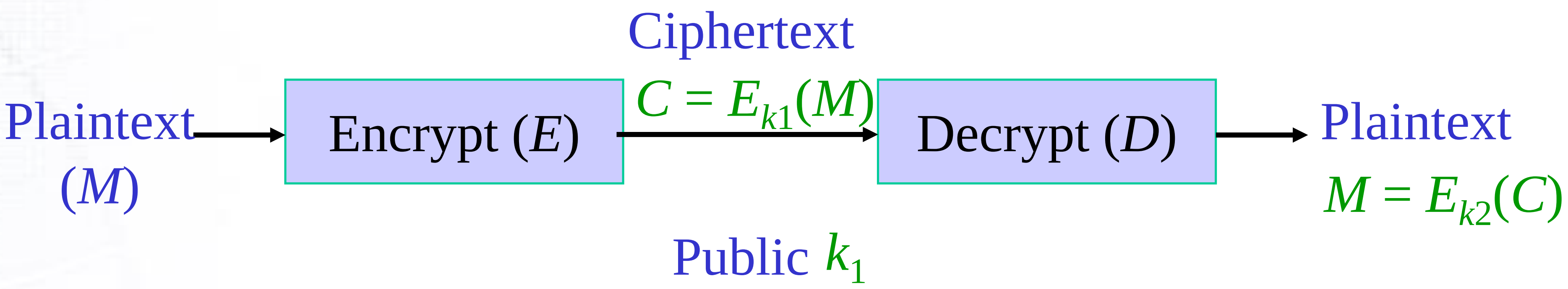
- Advantage: Secrecy, Authentication, Integrity
- Disadvantage: 1. Need secure channel

  2. Too many keys required ($n(n – 1)/2$, for n participants.)

  3. No “Non-repudiation"

Symmetric Key Cryptosystem

Asymmetric Cryptosystem (1976, Diffie and Hellman)**:**



Ciphertext

$C = E_{k1}(M)$

Plaintext (M)

Encrypt (E)

Decrypt (D)

Plaintext

$M = E_{k2}(C)$

Public k_1

- Advantage: Secrecy, Integrity, Non-repudiation, Only one key for each participant.
  - If Commutative ($D_{k2}(E_{k1}(M)) = M = E_{k1}(D_{k2}(M))$): Non-repudiation (Digital Signature, 數位簽章)
- Disadvantage: Calculations are complex and time-consuming

(RSA takes 1000 times longer than DES)

Security Types

By Shannon, 1949.

- Theoretical Security or Perfect Security (理論安全):
  - – One-Time Pad
  - – Stream Cryptography (not really)

- Practical Security or Computational Security (實際安全):
  - Work Characteristic $W(n) > 10^{30}$
  - Historical Work Characteristic $W_h(n) > 10^{30}$