INT 307
Multimedia Security System

Multimedia Encryption (I)

Sichen.Liu@xjtlu.edu.cn

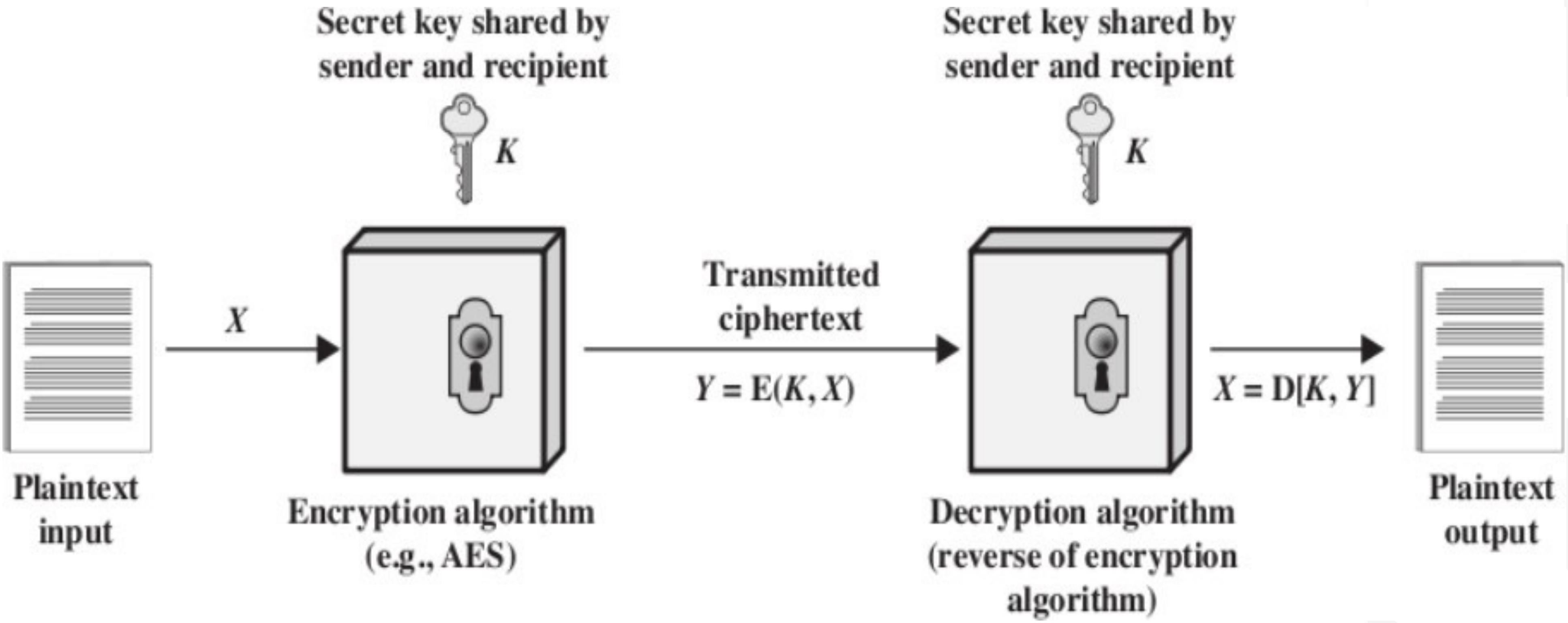
XJTLU | SCHOOL OF FILM AND TV ARTS

Xi'an Jiaotong-Liverpool University
西交利物浦大学

Terminology

- Plaintext: original message
- Ciphertext: encrypted or coded message
- Encryption: convert from plaintext to ciphertext (enciphering)
- Decryption: restore the plaintext from ciphertext (deciphering)
- Cipher: a particular algorithm (cryptographic system)
- Key: information used in encryption known only to sender/receiver
- Cryptography: study of algorithms used for encryption
- Cryptanalysis: study of techniques for decryption without knowledge of plaintext
- Cryptology: areas of cryptography and cryptanalysis

Simplified Model of Symmetric Encryption



Classical Encryption Techniques

- Two building blocks of all classical encryption techniques: **substitution** and **transposition** .
- **Substitution:** replacing an element of the plaintext with an element of ciphertext
- Overall substitution rule or varying ones for every element of the plaintext.
- **Transposition (permutation):** rearrange the order of appearance of the element of the plaintext.
- Multiple rounds of interlaced transpositions and substitutions.

Properties of Cryptographic Systems

- Operations used for encryption
  - Substitution: replace one element in plaintext with another
  - Transposition: re-arrange elements
  - Product systems: multiple stages of substitutions and transpositions
- Number of keys used
  - Symmetric: sender/receiver use same key (shared-key)
  - Public-key: sender/receiver use different keys (asymmetric)
- Processing of plaintext
  - Block cipher process one block of elements at a time
  - Stream cipher process input elements continuously

Cryptanalysis and Brute-Force Attacks

- Objective of attacker: recover key (not just message)
- Approaches of attacker
  - Cryptanalysis: Exploit characteristics of algorithm to deduce plaintext or key
  - Brute-force attack Try every possible key on ciphertext until intelligible translation into plaintext obtained
- If either attack finds key, all future/past messages are compromised

Measures of Security

- Unconditionally Secure
  - Ciphertext does not contained enough information to derive plaintext or key
  - One-time pad is only unconditionally secure cipher (but not very practical)
- Computationally Secure
  - Cost of breaking cipher exceeds value of encrypted information
  - Time required to break cipher exceeds useful lifetime of encrypted information
  - Hard to estimate value/lifetime of some information
  - Hard to estimate how much effort needed to break cipher

Brute-Force Attacks

- On average, number of guesses is half the key space

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

Caesar Cipher

- Earliest known cipher, used by Julius Caesar (Roman general 2000 years ago)
- Replace each letter by the later three positions along in alphabet

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
Cipher:	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

- Character c of the ciphertext is computed as

$$C = E(3, p) = (p + 3)\text{mod}26$$

where each letter of the alphabet is represented by an integer.
- Assuming case-insensitive encoding with the Caesar cipher.
- Generalised Caesar Cipher
  - Allow shift by k positions
  - Assume each letter assigned number $(a = 0, b = 1, \cdots)$

$$\begin{aligned} C &= E(k, p) = (p + k) mod 26 \\ p &= D(k, C) = (C - k) mod 26 \end{aligned}$$

Breaking the Caesar Cipher

- Brute force attack
  - Try all 25 keys, e.g. k = 1, k = 2, . . .
  - Plaintext should be recognized
- Recognizing plaintext in brute force attacks
  - Need to know the" structure" of plaintext
  - Language? Compression?
- How to improve against brute force?
  - Hide the encryption/decryption algorithm: **Not practical**
  - Compress, use different language: **Limited options**
  - Increase the number of keys

Monoalphabetic (Substitution) Ciphers

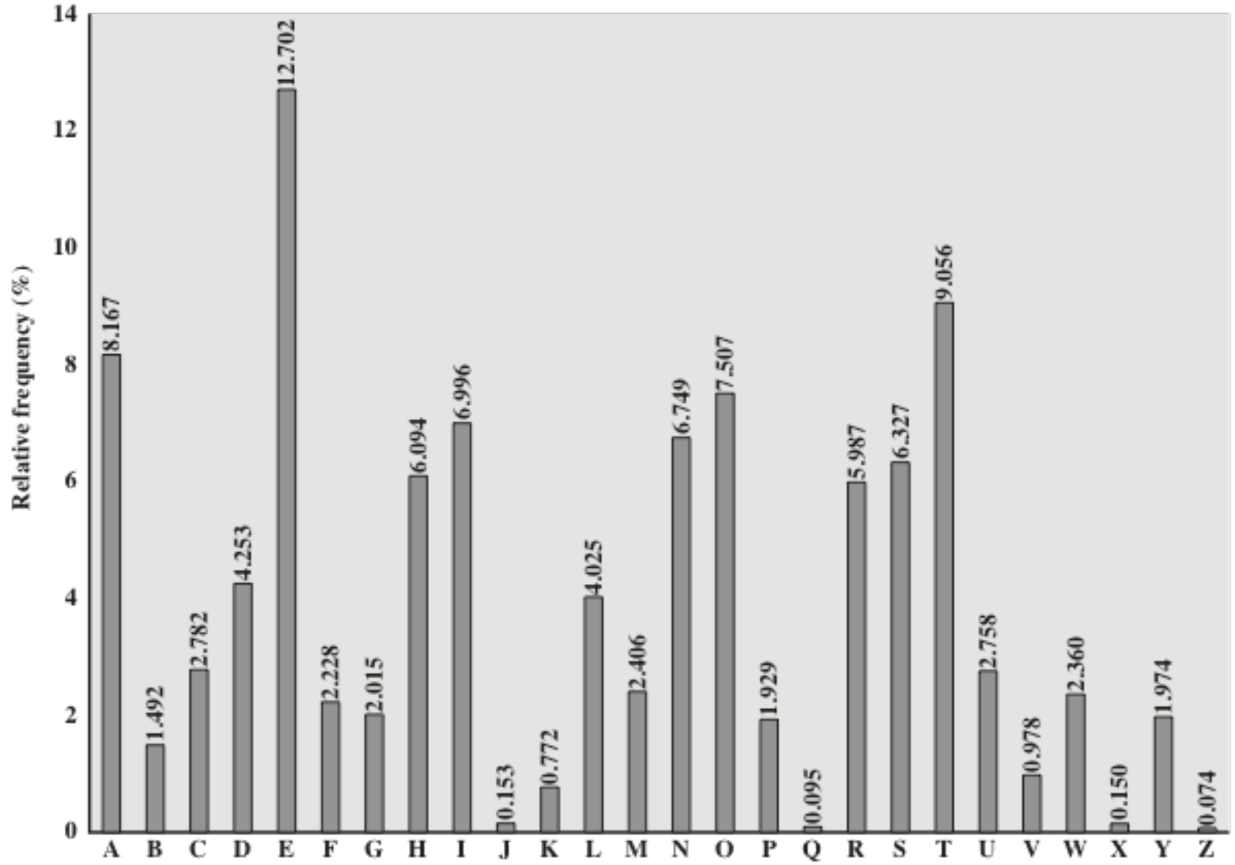
- Monoalphabetic: use a single alphabet for both plaintext and ciphertext
- Arbitrary substitution: one element maps to any other element
- n element alphabet allows $n!$ permutations or keys
- Example:

```
Plain :a b c d e ... w x y z
Cipher:D Z G L S ... B T F Q
```

- Try brute force . . .
- Caesar cipher: 26 keys
- Monoalphabetic (English alphabet): $26!$ keys ($> 4 \times 10^{26}$)

Attacks on Monoalphabetic Ciphers

- Fundamental problem with monoalphabetic ciphers
  - Ciphertext reflects the frequency data of original plaintext
  - Solution 1: encrypt multiple letters of plaintext
  - Solution 2: use multiple cipher alphabets



Playfair Cipher

letter ⇒ letxterx

go rt sr dt

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

- Initialisation: keyword (**smythework**)
  1. Create 5x5 matrix and write keyword (row by row)
  2. Fill out remainder with alphabet, not repeating any letters
  3. Special: Treat I and J as same letter
- Encryption
  1. Operate on pair of letters (digram) at a time
  2. Plaintext in same row: replace with letters to right
  3. Plaintext in same column: replace with letters below
  4. Else, replace by letter in same row as it and same column as other plaintext letter
  5. Special: if digram with same letters, separate by special letter, x.
- Rightness property is to be interpreted circularly in each row
- Belowness property is to be interpreted circularly in each column.

Playfair Cipher Example

- Plaintext: hello
- Keyword: thailand
- Ciphertext: LDAZEU

hello

Plain ⇒ he lx lo

Cipher: ld az eu

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

Playfair Cipher - Is it Breakable?

- Cipher does alter the relative frequencies associated with the individual letters and with digrams and with trigrams, but not sufficiently
- Better than monoalphabetic: relative frequency of digrams much less than of individual letters
- But relatively easy (digrams, trigrams, expected words)

Hill Cipher: Multi-letter Cipher

- Assign the integer 0 and 25 to the letter 'a' through 'z' of the plaintext.
- Encryption key K: 3×3 matrix of integer

$$K = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{12} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix}$$

- Transform three letters at a time from the plaintext p_1,p_2 and p_3 into c_1, c_2 and c_3

$$\begin{aligned} c_1 &= (k_{11}p_1 + k_{12}p_2 + k_{13}p_2)\text{mod}26 \\ c_2 &= (k_{21}p_1 + k_{22}p_2 + k_{23}p_2)\text{mod}26 \\ c_3 &= (k_{31}p_1 + k_{32}p_2 + k_{33}p_2)\text{mod}26 \end{aligned}$$

- It can be written as vector-matrix form

$$C = KP\text{mod}26$$

- The decryption would require the inverse of K matrix

$$P = K^{-1}C\text{mod}26$$

How Secure is Hill Cipher?

- Strength is that it completely hides single-letter frequencies
  - The use of a larger matrix hides more frequency information
  - A 3 x 3 Hill cipher hides not only single-letter but also two-letter frequency information
- Strong against a ciphertext-only attack but easily broken with a known plaintext attack

Polyalphabetic Ciphers

- Use different monoalphabetic substitutions as proceed through plaintext
- Set of monoalphabetic ciphers
- Key determines which monoalphabetic cipher to use for each plaintext letter
- Examples
    - Vigenere cipher
    - Vernam cipher
    - One time pad

Vigenere Cipher

- Set of 26 general Caesar ciphers
- Letter in key determines the Caesar cipher to use
- Key must be as long as plaintext: repeat a keyword
- For example, if the keyword is **deceptive**, the message "we are discovered save yourself" is encrypted as:

key: deceptivedeceptivedeceptive
plaintext: wearediscoveredsaveyourself
ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

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

Vigenere Cipher - Is it Breakable?

- Yes
- For keyword length m, Vigen`ere is m monoalphabetic substitutions
- Break the monoalphabetic ciphers separately
- Weakness is repeating, structured keyword

One Time Pad

- Similar to Vigenere, but use random key as long as plaintext
- Only known scheme that is unbreakable (unconditional security)
  - Ciphertext has no statistical relationship with plaintext
  - Given two potential plaintext messages, attacker cannot identify the correct message
- Two practical limitations
  - Difficult to provide large number of random keys
  - Distributing unique long random keys is difficult
- Limited practical use

One Time Pad Example

- Attacker knows the ciphertext

```
ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERFPLUYTS
```

- Attacker tries all possible keys. Two examples

```
key1:       pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih
plaintext1: mr mustard with the candlestick in the hall

key2:       mfugpmiydgaxgoufhklllmhsqdqogtewbqfgyovuhwt
plaintext2: miss scarlet with the knife in the library
```

- There are many other legible plaintexts obtained with other keys. No way for attacker to know the correct plaintext

Rail Fence Transposition

- Plaintext letters written in diagonals over N rows (depth)
- Ciphertext obtained by reading row-by-row
- Easy to break: letter frequency analysis to determine depth
- Example:

```
plaintext: internettechnologiesandapplications
depth: 3
```

Rail Fence Transposition

- Example: 'WE ARE DISCOVERED. FLEE AT ONCE' and *d* = 3

```
W . . . E . . . C . . . R . . . L . . . T . . . E
. E . R . D . S . O . E . E . F . E . A . O . C .
. . A . . . I . . . V . . . D . . . E . . . N . .
```

- Crypted-message: WECRLTEERDSOEEFEAOCAIVDEN

Rows/Columns Transposition

- Plaintext letters written in rows
- Ciphertext obtained by reading column-by-column, but re-arranged
- Key determines order of columns to read
- Easy to break using letter frequency (try different column orders)
- Example

```
plaintext: securityandcryptography
key: 315624
```

Rows/Columns Transposition

- Transposition ciphers can be made stronger by using multiple stages of transposition

```
plaintext:  attackpostponeduntiltwoamxyz
key: 3421567
ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

- Transpose again using same key

```
output:     NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

Original plaintext letters, by position:

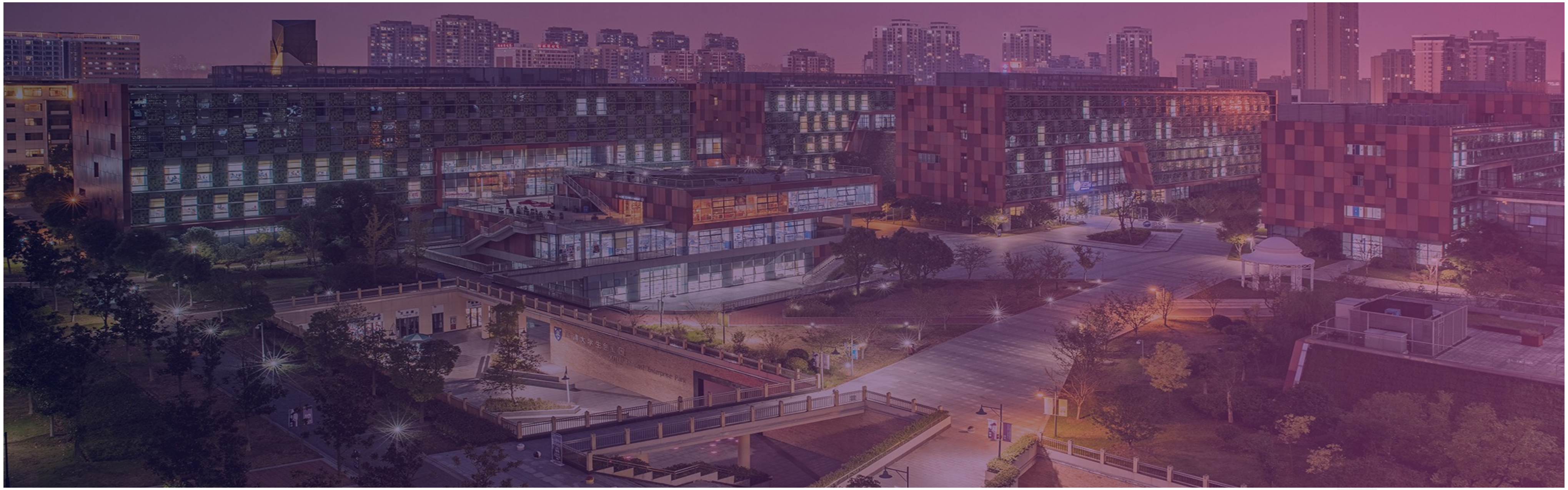
```
01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28
```

After first transposition:

```
03 10 17 24 04 11 18 25 02 09 16 23 01 08
15 22 05 12 19 26 06 13 20 27 07 14 21 28
```

After second transposition:

```
17 09 05 27 24 16 12 07 10 02 22 20 03 25
15 13 04 23 19 14 11 01 26 21 18 08 06 28
```



THANK YOU

VISIT US

WWW.XJTLU.EDU.CN

FOLLOW US

@XJTLU

Xi'an Jiaotong-Liverpool University
西交利物浦大学

XJTLU | SCHOOL OF FILM AND TV ARTS