All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

All rights are reserved by Li Jingtao @ Fudan University

信息安全（01）

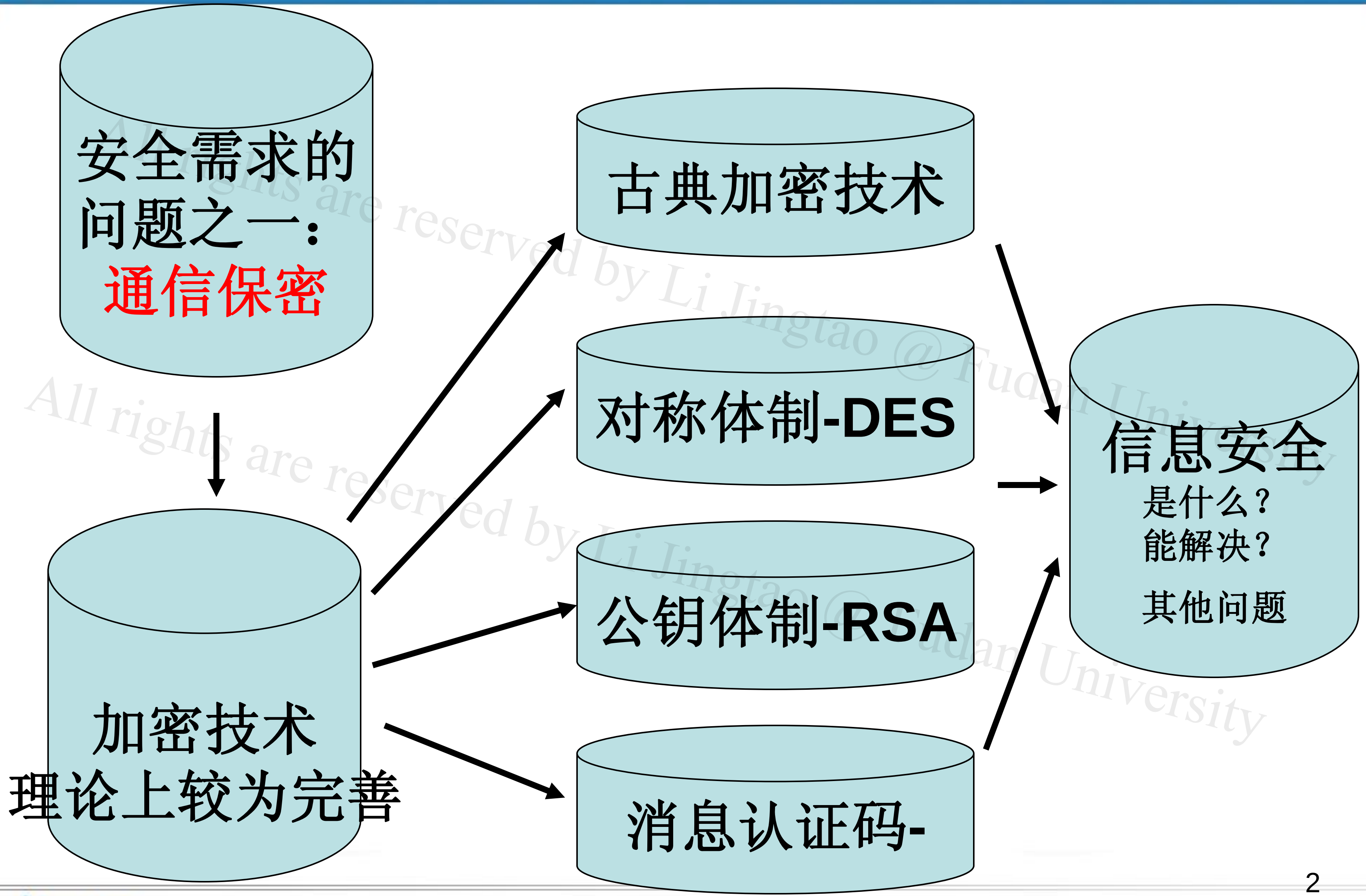
Introduction to Cryptography

-Classical Encryption Techniques

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

故事是这样开始的……



安全需求的问题之一：通信保密

加密技术理论上较为完善

古典加密技术

对称体制-DES

公钥体制-RSA

消息认证码-

信息安全

是什么？

能解决？

其他问题

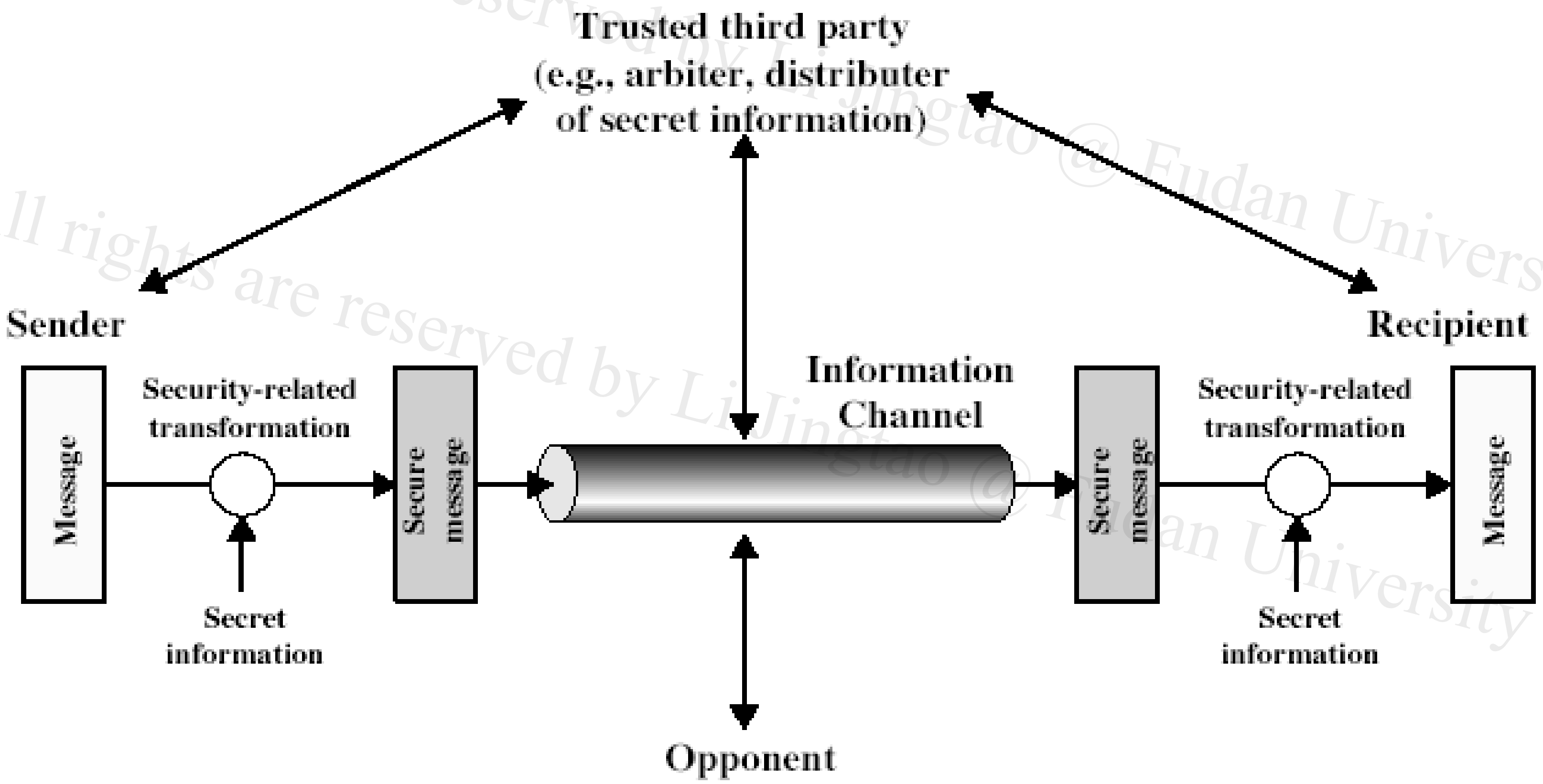
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

问题：通信保密

- **Confidentiality，机密性，保密性**



问题讨论的环境

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

古人的智慧

- 羊皮传书
- 藏头诗
- Caesar

All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

羊皮传书

- 古希腊的斯巴达人将一条1厘米宽、20厘米左右长的羊皮带，以螺旋状绕在一根特定粗细的木棍上

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

藏头诗

明才子唐伯虎：

- 我爱兰江水悠悠，爱晚亭上枫叶稠。
- 秋月溶溶照佛寺，香烟袅袅绕经楼。

All rights are reserved by Li Jingtao @ Fudan University

明朝解缙祝某宰相寿辰进诗：

- 真真宰相,老老元臣,乌纱戴顶,龟鹤遐林.
  - 粗看"密文”,浑然诗句,颂扬兼祝愿,福禄寿全有;细究则密语藏头,挖苦带讽刺,诅咒"真老乌龟”

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Caesar Cipher

- earliest known substitution cipher by Julius Caesar
- first attested use in military affairs

- example:

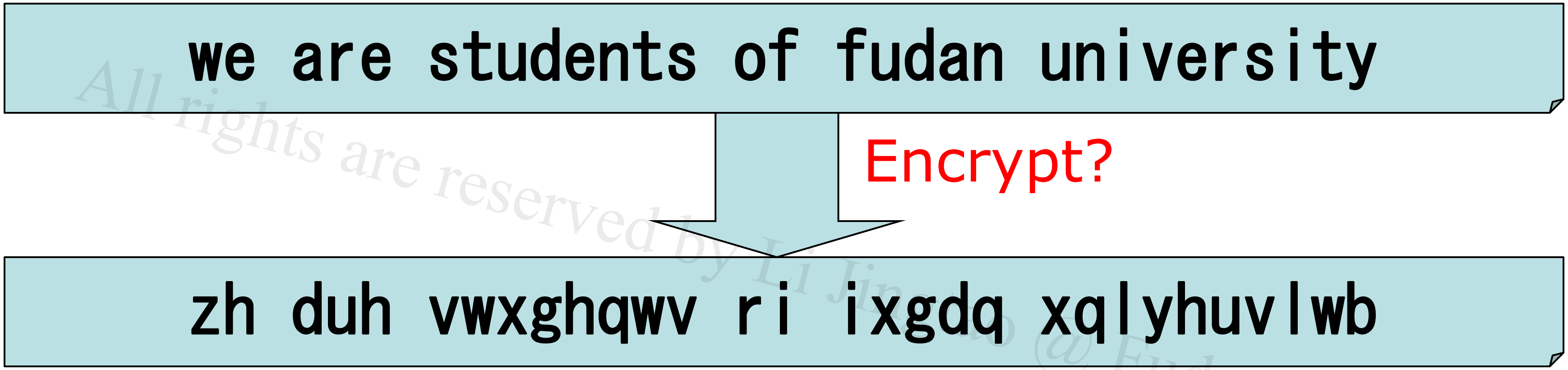
```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Caesar Cipher Exercise



we are students of fudan university

Encrypt?

zh duh vwxghqwv ri ixgdq xqlyhuvlwb

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Terminologies

- **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 plaintext from ciphertext

All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

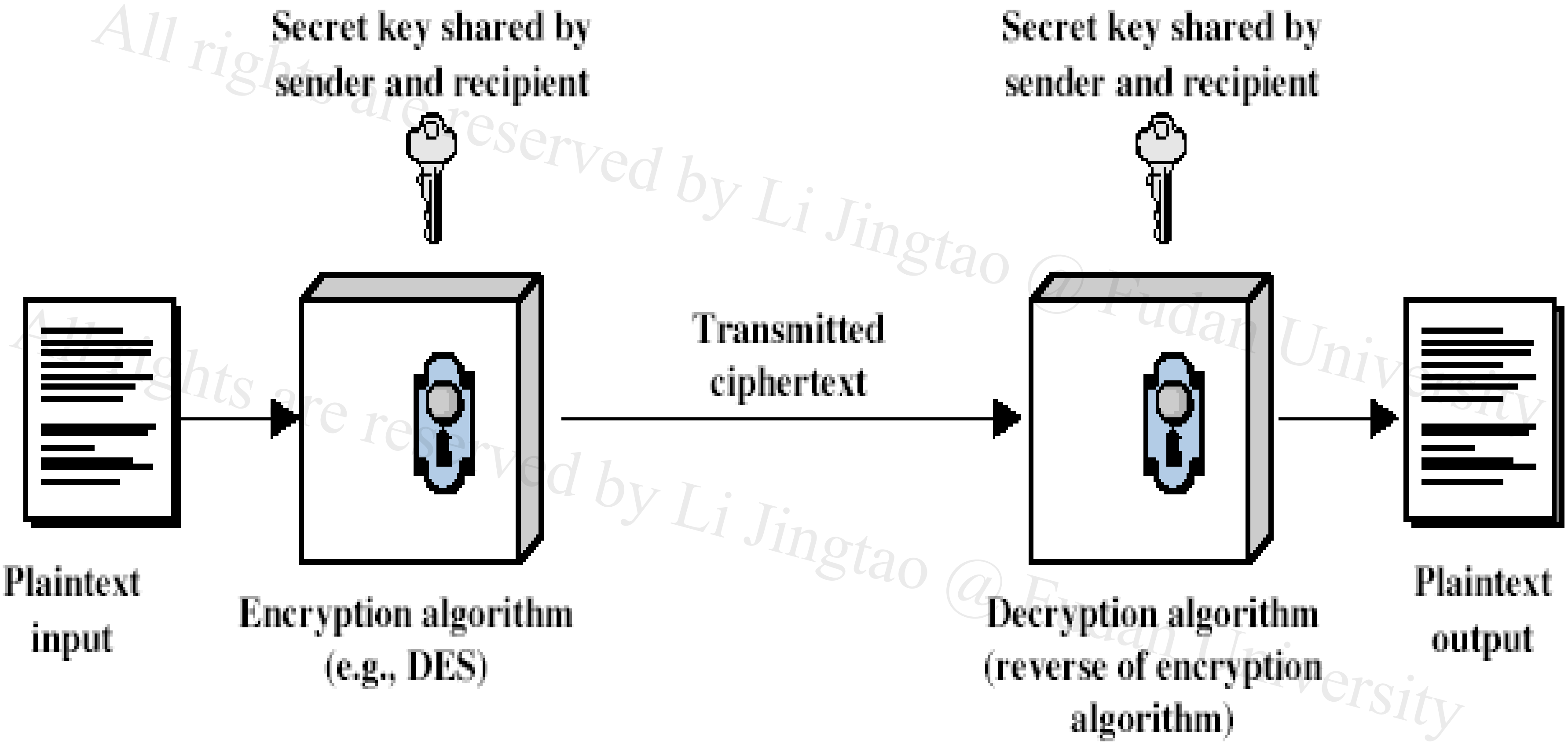
Terminologies (cont.)

- **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

All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Symmetric Cipher Model


Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Definition

- A **cryptosystem** is a **5-tuple (E, D, p, K, C),** **where**
  - **p is the set of plaintexts,**
  - **K the set of keys,**
  - **C is the set of cipher texts,**
  - **E: M×K→C is the set of Encryption algorithms,**
  - **D: C×K→M is the set of Decryption algorithms.**

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

三个古典系统的再讨论

- **Caesar**
- 羊皮传书
- 藏头诗

All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Caesar Cipher

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

- p, C, K, E, D?

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

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
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- then have Caesar cipher as:

$$C = E(p) = (p + k) \bmod (26)$$

$$p = D(C) = (C - k) \bmod (26)$$

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

羊皮传书

- E, D, p, C, K?

All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

藏头诗

- 真真宰相,老老元臣,乌纱戴顶,龟鹤遐林.
- E, D, p, C, K?

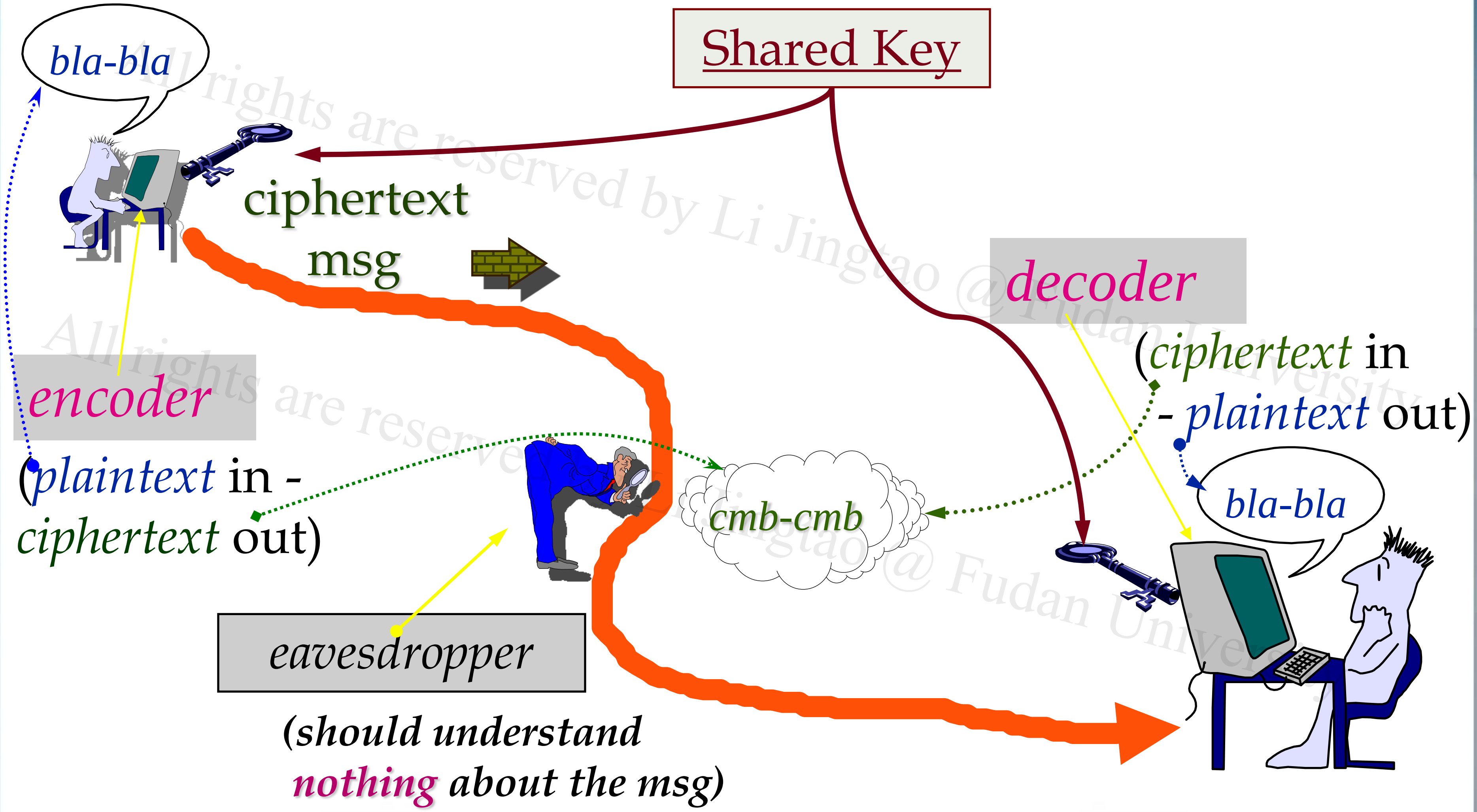
All rights are reserved by Li Jingtao @ Fudan University

- 全诗为"密文”,其"密钥”是每句诗的首字,可串接成义,作者的真意就隐藏在诗句的首字串接文("明文”)中.
- **Steganography，隐写术**

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

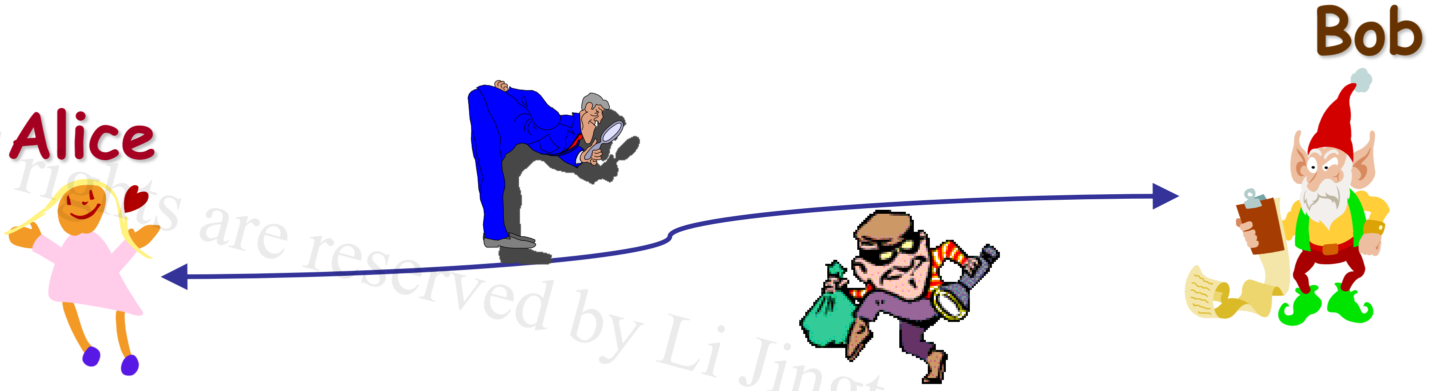
Rethinking of the Model



All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Need key exchange



All rights are reserved by Li Jingtao @ Fudan University

- Alice and Bob want to establish a **<u>shared secret (key)</u>** when other people (*eavesdroppers*) are listening
- How to?
  - inbound Vs. outbound

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Discussion

- 模型合理吗？

- 什么当保密；什么当公开？
  - 19世纪荷兰人A.Kerckhoffs就提出了一个在密码学界被公认为基础的假设，也就是著名的“Kerckhoffs假设”：秘密必须全寓于密钥。
  - Kerckhoffs假设密码分析者已有密码算法及其实现的全部详细资料，在该假设前提下实现安全的密码体制

- **Other Models?**

All rights are reserved by Li Jingtao@Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Discussion

“谁是我们的敌人，谁是我们的朋友，这个问题是革命的首要问题”——毛选

- 易用性
- 秘密全部寓于密钥≠算法当公开，要看应用环境(商用，军用，……)
- 开放的系统更安全，??

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Cryptography Catalog

- **The type of operations used for transforming plaintext to ciphertext**
  - **Substitution**: each element in the plaintext is mapped into another element
  - **Transposition**: elements in the plaintext are rearranged
  - **Product**: multiple stages of substitutions and transpositions
- **The number of the keys used**
  - **Symmetric** , **single-key**, **secret-key**, **conventional encryption**: Both sender and receiver use the **same** key
  - **Asymmetric**, **two-key**, or **public-key encryption**: the sender and receive each uses a **different** key

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Cryptography Catalog

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

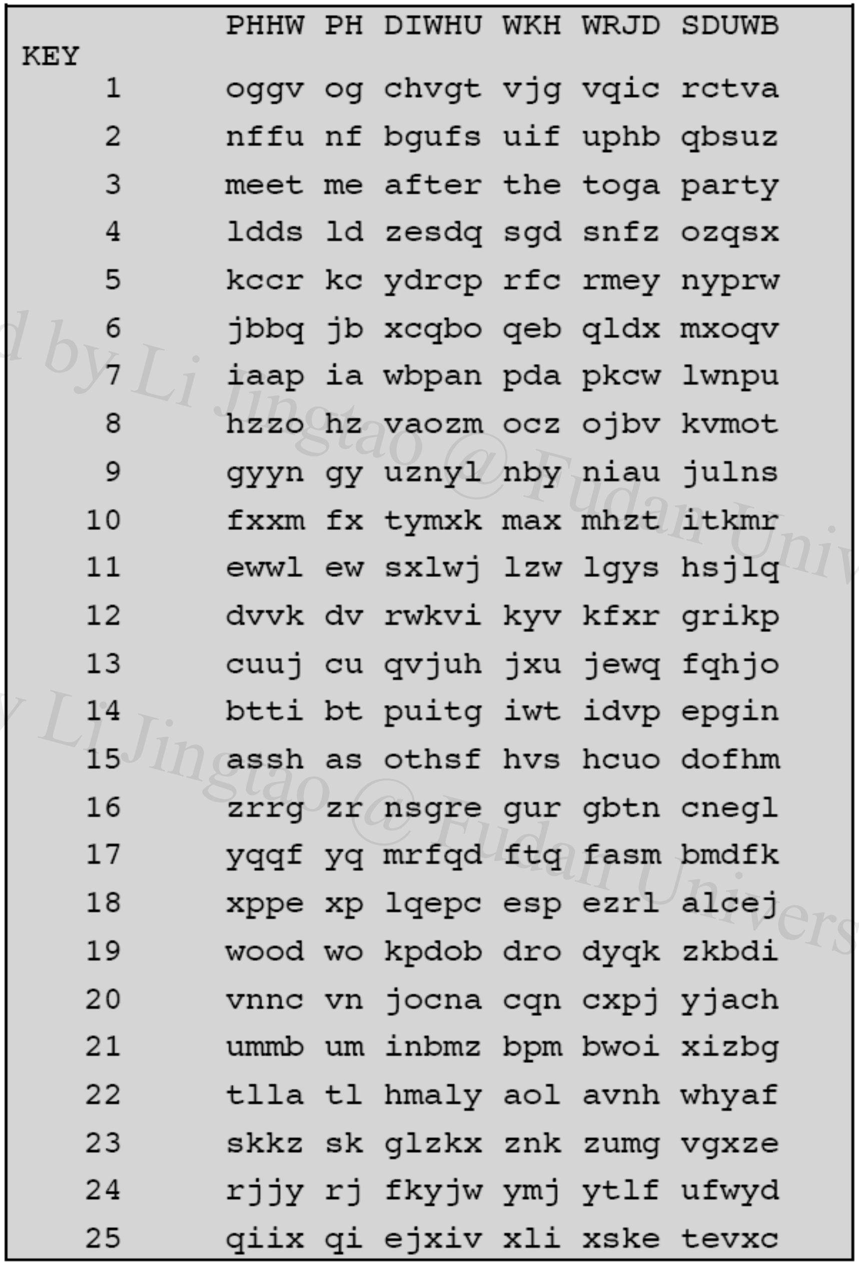
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Substitution Techniques

- Caesar cipher
  - Easy to break!



KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrcp	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Cryptanalysis of Caesar Cipher

- There are only 25 keys to try
  - A maps to A,B,..Z
  - could simply try each in turn
  - a **brute force search**
- given ciphertext, just try all shifts of letters
  - The language of Plaintext is known and easily recognizable
  - do need to recognize when have plaintext eg. break ciphertext "GCUA VQ DTGCM"

All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Monoalphabetic Cipher

- Improvement on Caesar Cipher
  - Rather than substituting according to a regular pattern – any letter can be substituted for any other letter, as long as each letter has a unique substitute letter, and vice versa.

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Monoalphabetic Cipher

```
K:
  Plain:   abcdefghijklmnopqrstuvwxyz
  Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN


Plaintext:
  ifwewishtoreplaceletters
Ciphertext:
  WIRFRWAJUHYFTSDVFSFUUFYA
```

- **hence key is 26 letters long**

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Monoalphabetic Cipher Security

All rights are reserved by Li Jingtao @ Fudan University

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

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Language Redundancy and Cryptanalysis

- human languages are redundant

All rights are reserved by Li Jingtao @ Fudan University

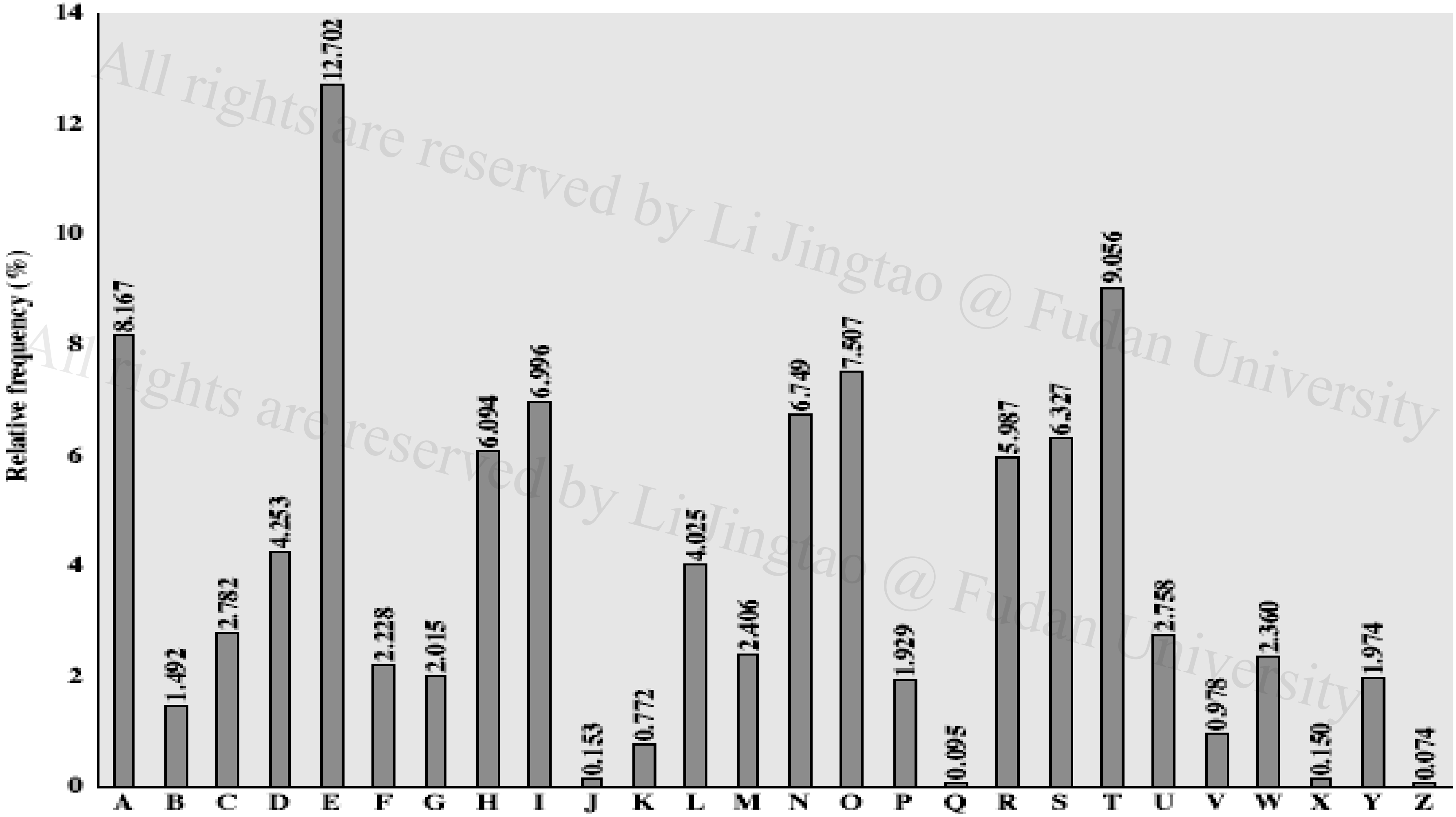
- letters are not equally commonly used
- in English e is by far the most common letter, then T,R,N,I,O,A,S
- some letters are fairly rare, eg. Z,J,X,Q

All rights are reserved by Li Jingtao @ Fudan University

- tables of single, double & triple letter frequencies

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Frequency of Letters in English Text



All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Use in Cryptanalysis

- **key concept** - monoalphabetic substitution ciphers do not change relative letter frequencies
- discovered by Arabian scientists in 9th century
- calculate letter frequencies for ciphertext
- compare counts/plots against known values
- if Caesar cipher look for common peaks/troughs
  - peaks at: A-E-I triple, NO pair, RST triple
  - troughs at: JK, X-Z
- for monoalphabetic must identify each letter
  - tables of common double/triple letters help

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

Example Cryptanalysis

- given ciphertext:

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
```

- count relative letter frequencies (see text)
- guess P & Z are e and t
- guess ZW is th and hence ZWP is the
- proceeding with trial and error finally get:

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

All rights are reserved by Li Jingtao @ Fudan University

All rights are reserved by Li Jingtao, and content may not be reproduced, downloaded, disseminated, published, or transferred in any form or by any means, except with the prior written permission of Li Jingtao.

An Improvement

- Homophone
- Assign each letter a number of different cipher symbols
- The number of symbols assigned to each letter is proportional to the relative frequency of that letter

All rights are reserved by Li Jingtao @ Fudan University
All rights are reserved by Li Jingtao @ Fudan University