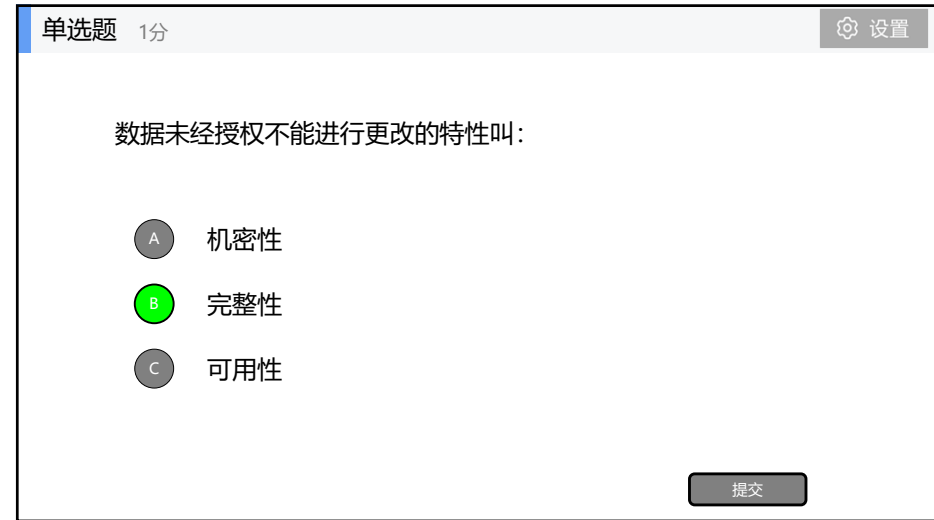
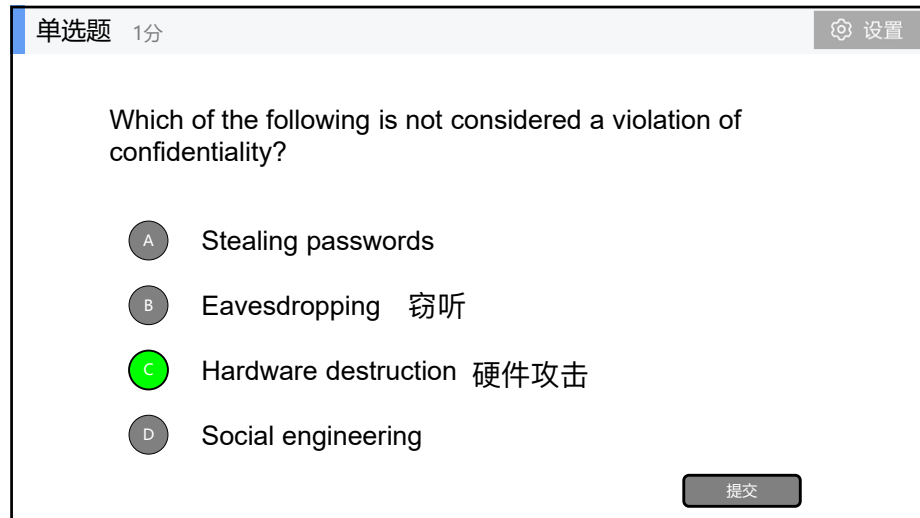


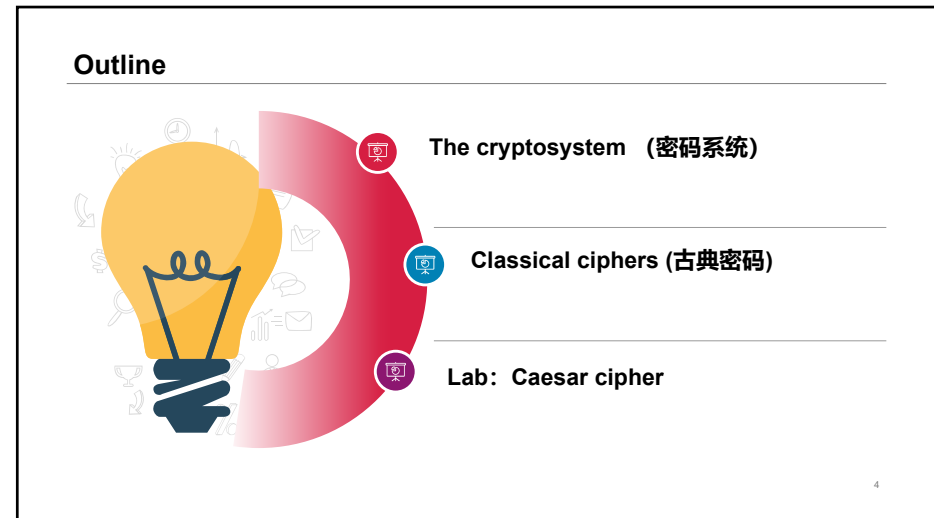
1



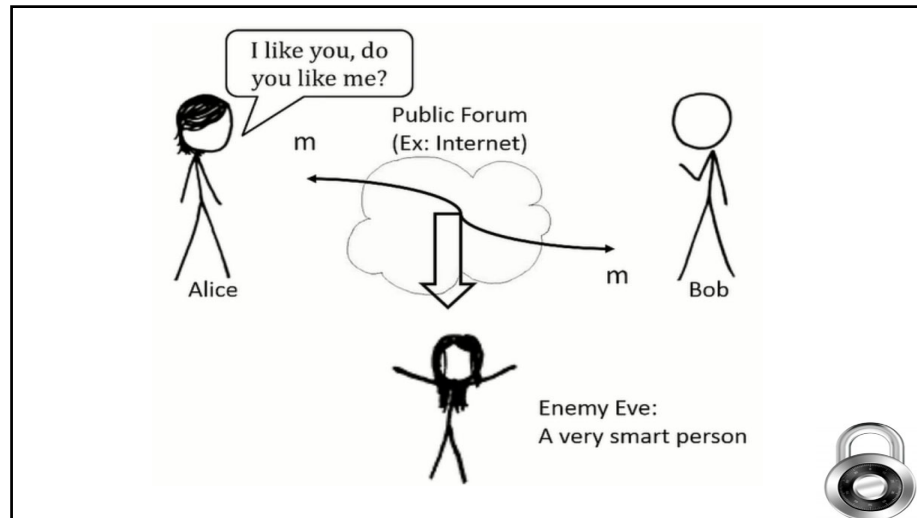
2



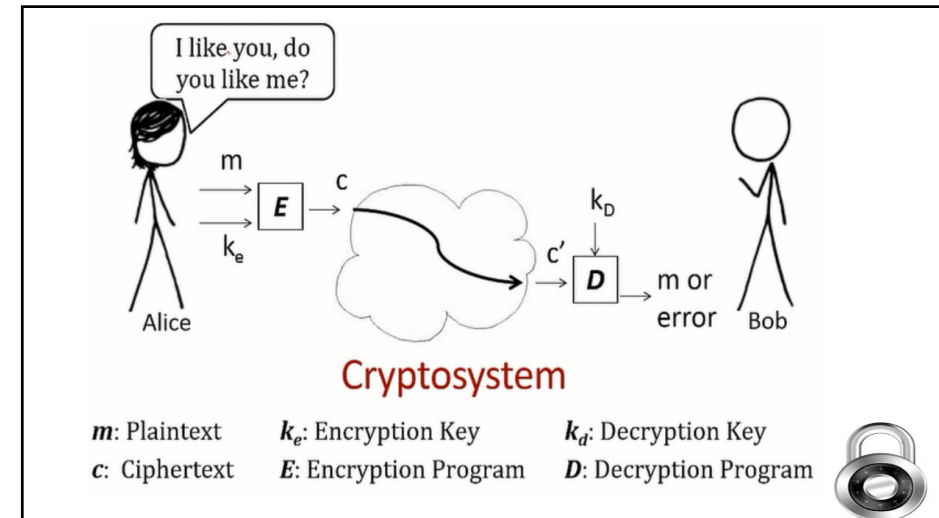
3



4



5



6

Cryptosystem (密码系统)

- Quintuple $(\mathcal{E}, \mathcal{D}, \mathcal{M}, \mathcal{K}, \mathcal{C})$ (密码系统五元组)
 - \mathcal{M} set of plaintexts (明文)
 - \mathcal{K} set of keys (密钥)
 - \mathcal{C} set of ciphertexts (密文)
 - \mathcal{E} set of encryption functions $e: \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{C}$ (加密函数)
 - \mathcal{D} set of decryption functions $d: \mathcal{C} \times \mathcal{K} \rightarrow \mathcal{M}$ (解密函数)

7

outline

- The Cryptosystem (密码系统)
- Classical ciphers (古典密码)
- Wrap up

8

古典密码中最基本的方法

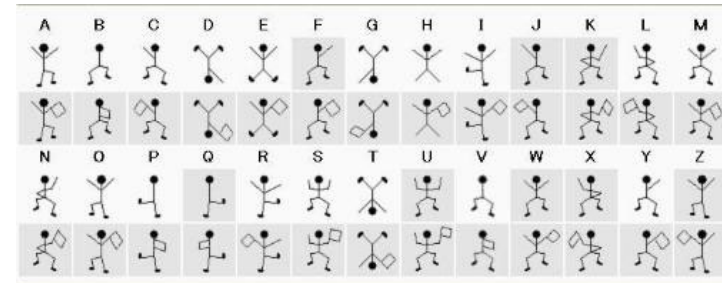
Substitution cipher (替换密码)

将明文中的一个字母由其它字母、数字或符号替代的一种方法。



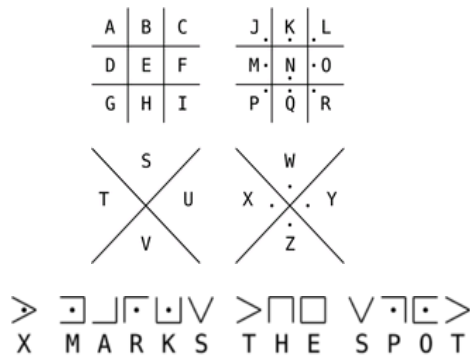
9

福尔摩斯全集——跳舞的小人



10

其他单表(mono-alphabetic) 替换加密-pigpen cipher



11

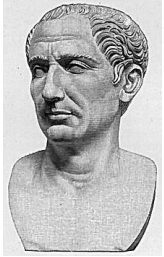
Substitution cipher

- Monoalphabetic cipher(单字母表密码):
– Caesar cipher
- Polyalphabetic cipher(多字母表密码):
– Vigenère cipher
– Hill cipher



12

1. Caesar Cipher



I come, i see, i conquer.

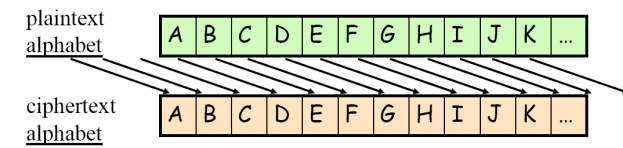


1. Caesar Cipher

video

Part one of the Caesar cipher

Shift by three (no key)



13

14

General Caesar Cipher

- Let's assign a numerical equivalent to each letter:

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

- Caesar cipher can be expressed as:
 - $c = E(3, p) = (p + 3) \bmod 26$ $D(3, c) = (c - 3) \bmod 26$
- The general Caesar algorithm is:
 - $C = E(k, p) = (p + k) \bmod 26$ k : in the range 1 to 25
 - $p = D(k, C) = (C - k) \bmod 26$



15


How to break Caesar Cipher?
(如何破解凯撒密码)

Brute force attack



16

Decryption shift	Candidate plaintext
0	exxegoexsrgi
1	dwdfndwrqfh
2	cvvcemcvqpeg
3	buubdlbupodf
4	attackatonce
5	zsszbjzsnmbd
6	yrryaiyrlac
...	
23	haahjrhavujl
24	gzzgiqgzutik
25	fyyfhpftshj



17

- Caesar cipher can be generalized even further.
- E.g., A permutation of the 26 alphabets. (26个字母的一种排列)

Encryption


a	b	c	d	e	f	g	h	i	j	k	l	m
D	K	V	Q	F	I	B	J	W	P	E	S	C

n	o	p	q	r	s	t	u	v	w	x	y	z
X	H	T	M	Y	A	U	O	L	R	G	Z	N

Decryption

A	B	C	D	E	F	G	H	I	J	K	L	M
s	g	m	a	k	e	x	o	f	h	b	v	q

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
z	u	j	d	w	l	p	t	c	i	n	r	y



18

What is the size of key space in the substitution cipher assuming 26 letters? (如何密钥是26个字母的一种全排列, 那么密钥空间有多大?)

$$|\mathcal{K}| = 26$$

$$|\mathcal{K}| = 26! \quad (26 \text{ factorial}) \quad \rightarrow \quad \approx 2^{88}$$

$$|\mathcal{K}| = 2^{26}$$

$$|\mathcal{K}| = 26^2$$

19

How to break?

Frequency analysis (频率分析)

video Part two of The Caesar cipher



20

单选题 1分

设置

What is the most common letter in English text?

- A "X"
- B "L"
- C "E"**
- D "H"

提交

21

How to break a substitution cipher?

(1) Use frequency of English letters

"e":12.7%, "t":9.1%, "a": 8.1%

(2) Use frequency of pairs of letters (digrams)

"he", "th", "an", "in"

22

An Example

UKBYBIOUZBCUFEEBORUKBYBHOBFRFESPVKBWFOFERVNBVCBZPRUBOFERVNBVCBPYYFVUFO
FEIKNWFRFIJUNUPWRFIPOUNVNIPUBRNCUKBEFWWFDNCHXCBOHOPYXPUBNCUBOYNRVNIWN
CPOJIOFHOPZRVFZIXUBORJUBZRBCHNCBBONCHRJZSFWNVRJUBZRPCYZPUKBZPUNVPWPCYVF
ZIXUPUNFCPWVRVNBVCBVRPYYNUNFCPWVWJUKBYBIOUZBCUIPOUNVNIPUBRNCBOPYPXUBNCUB
OYNRVNIWNCPOJIOFHOPZRNCRVNBCUNENVVFZIXUNCHPCYVFZIXUPUNFCPWZPUKBZPUNVR

B	36	→ E
N	34	
U	33	→ T
P	32	→ A
C	26	

NC	11	→ IN
PU	10	→ AT
UB	10	
UN	9	

digrams

UKB	6	→ THE
RVN	6	
FZI	4	

trigrams

Cipher only attack! (唯密文攻击)

23

2. Vigenere cipher (16th century, Rome)

video

Polyalphabetic cipher

k = **C R Y P T O** C R Y P T O C R Y P T (+ mod 26)

m = W H A T A N I C E D A Y T O D A Y

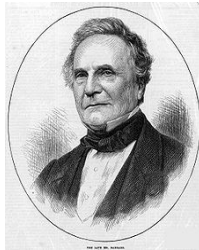
c = Y Y Y I T B K T C S T M V F B P R

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

24

Vigenère Cipher: Unbreakable?

Charles Babbage, 1791-1871 (查理斯.巴贝奇)
In 1846 , Babbage broke **Vigenère cipher**



Part of Babbage's difference engine

http://en.wikipedia.org/wiki/Charles_Babbage

25

25

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 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 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 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 Square

26

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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	
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	

Key:
GOOGLE
Plaintext:
BUY YOUTUBE
Ciphertext:
HIMEZYIPK

Vigenère Square

27

频率统计分析: Vigenère(维基尼亚) cipher

If we encrypt the same piece of text using the monoalphabetic substitution cipher and the Vigenère cipher, we can see why the latter cipher is so much stronger than the former. Let us use a short text about Vigenère to see the difference. Start by encrypting it with the monoalphabetic cipher.

Plaintext

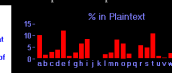
Aged twenty six, Vigenere was sent to Rome on a diplomatic mission. It was here that he became acquainted with the writings of Alberti, Trithemius and Porta, and his interest in cryptography was ignited. For many years, cryptography was nothing more than a tool that helped him in his diplomatic work, but, at the age of thirty nine, Vigenere decided that he had amassed enough money to be able to abandon his career and concentrate on a life of study. It was only then that he began research into a new cipher.

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

Monalphabetic Ciphertext

NUJOPKJRPDTAXYUJRGJDNKDJPFFGHBJHRRQAEHBNPALBADDHAPKND.
 IPSNSJCIJLBNJFMNAPRJOKAPSPJGAPARUDHWNOCGJAPGAPGJBJMNDROE
 GPNRNSODAPRJGJDPARJGTEPHUGNESTKNDIAURPJOWJGNBRTJINDGJLTPH
 GNESTKNDHAPRJGJDPARJGTEPHUGNESTKNDIAURPJOWJGNBRTJINDGJLTPH
 MNPNSJCIJLBNJFMNAPRJOKAPSPJGAPARUDHWNOCGJAPGAPGJBJMNDROE
 JTPHCJCOJPHNCGHRSADJNGJGNRLOLJRPJNSPJHRNNOBJHJWOPMTJPH

As you can see, the frequency distribution is now much flatter. The peaks are less obvious, because each letter has been encrypted in different ways, because the keyword is 8 letters long. The peak that was at E has been shared among 8 other letters. A flatter frequency distribution means a much stronger cipher.

[illegible]

28

28

7

如果我们知道key的长度...

Plaintext: **ATTAC KATDA WNONE ATTAC K.....**

Key: **LEMON LEMON LEMON LEMON.....**

Ciphertext: **LXFOP VEFRN HR... LXFOP.....**

- If the length of the keyword is 5, then we know that the 1st, 6th, 11th, ... letters are encoded by the same row in the Polyalphabetic substitution,
- This equals a mono-alphabetic cipher.

The [Kasiski examination](https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher) and [Friedman test](https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher) can help determine the key length.
https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

29

填空题 5分

设置

密码系统五元组包括：[填空1]、[填空2]、[填空3]、[填空4]、[填空5]。

正常使用填空题需3.0以上版本雨课堂

作答

30

单选题 1分

设置

Caesar密码属于：

- ☐ A 置换密码
- ☒ B 单表替换密码
- ☐ C 多表替换密码
- ☐ D 公钥密码

提交

31

单选题 1分

设置

Vigenere密码属于：

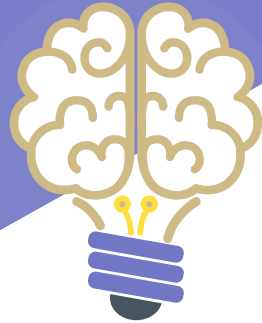
- ☐ A 置换密码
- ☐ B 单表替换密码
- ☒ C 多表替换密码
- ☐ D 公钥密码

提交

32

Lab two

 Caesar cipher



33

Tasks:

01-caesarCipher

02-caesarHacker

34

Python environment

01-Python setup

02-Python editor: Spyder3

35

Exercises

• Using **caesarCipher**, encrypt the following sentences with the given keys:

- ✓ ""You can show black is white by argument," said Filby, "but you will never convince me."" with key 8
- ✓ '1234567890' with key 21

• Using **caesarCipher**, decrypt the following ciphertexts with the given keys:

- ✓ 'Kv?uqwpfu?rncwukdng?gpqwijB' with key 2
- ✓ 'XCBSw88S18A1S 2SB41SE .8zSEwAS50D5A5x81V' with key 22

36

实验报告

- 实验方案中需要包含**程序设计流程图**。
- 实验结果中要有运行结果**截图**。
- 实验报告包含（实验目的、实验环境、实验小组分工、实验方案、实验步骤（**部分源代码**）、实验结果及分析、实验总结及体会）
- 实验报告成绩**评分标准**（满分100分）：完整性（30分）、提交及时（10分）、实验结果合理性（20分）、实验设计与分析翔实（30分）、小组成员分工完成（10分）。
- 实验报告提交日期： 2019年9月26日(纸质版)