
第三届
XMAN夏令营
XMAN
Something about classic cryptography
汇报时间：2018年1月
讲师：1phan

目录

CATALOG

01 单表替换加密

02 多表替换加密

03 置换

04 其他算法

05 算法求逆

目录

CATALOG

01 单表替换加密

- 添加相关标题文字
- 添加相关标题文字
- 添加相关标题文字
- 添加相关标题文字

单表替换

- 一种映射
- P--->C

单表替换的破解

- 密钥空间过小时：爆破
- 给的样本足够长时：http://quipqiup.com/

凯撒密码

- 明文字母表：ABCDEFGHIJKLMNOPQRSTUVWXYZ
- 密文字母表：DEFGHIJKLMNOPQRSTUVWXYZABC

- 明文：THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
- 密文：WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

凯撒密码

- 怎么攻击?
  - 直接爆破

- ASCII表凯撒密码
- 怎么攻击?
  - 直接爆破
  - 计算密文间瀚明距离

ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[ENG OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Atbash Cipher

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

- 明文：the quick brown fox jumps over the lazy dog
- 密文：gsv jfrxp yildm ulc qfnkh levi gsv ozab wlt

Polybius

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

仿射密码

- E(x) = a*x + b mod 26
- gcd(a, 26) == 1

- D(c) = a^(-1)*c - b

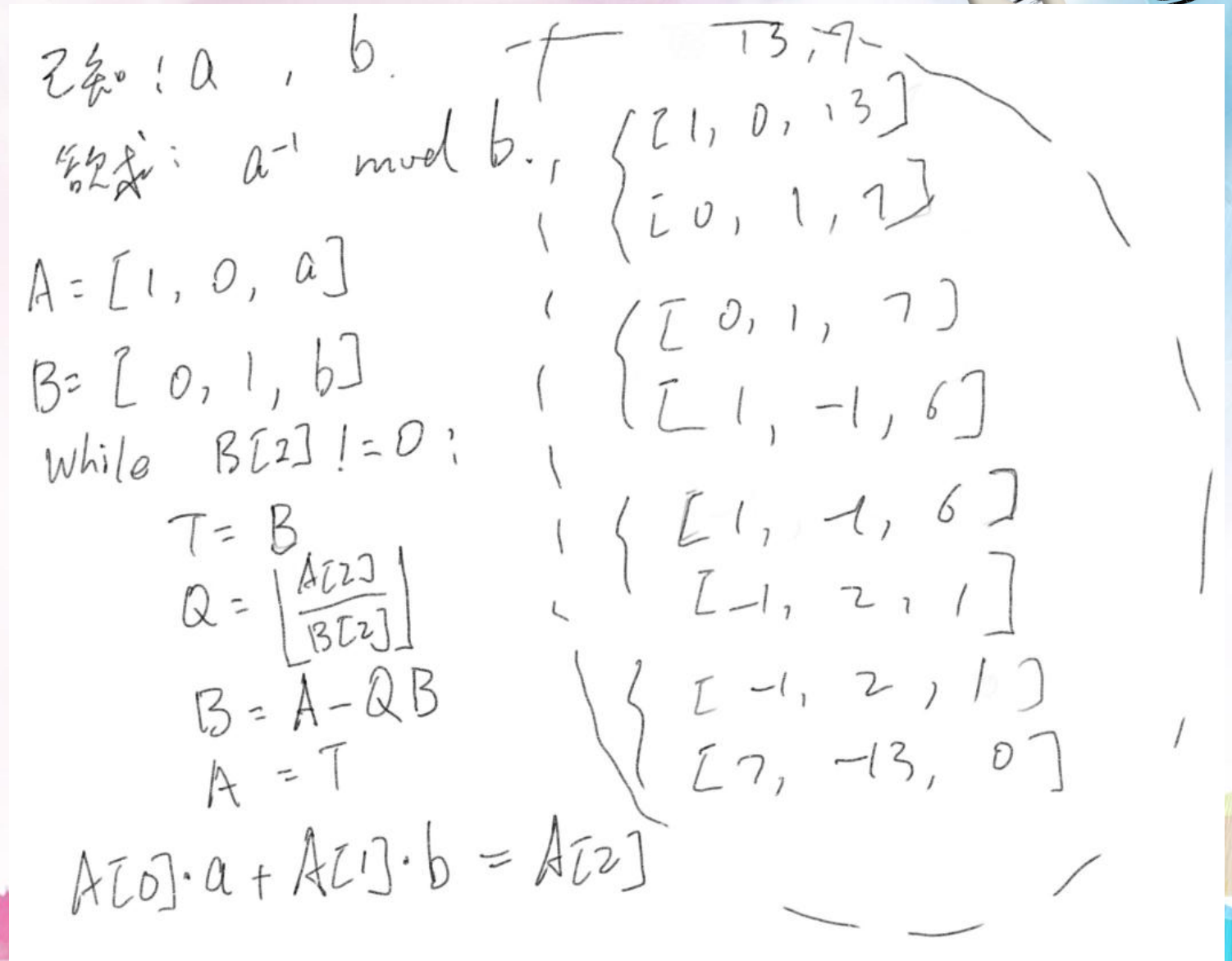
gcd

- 辗转相除法

- gcd(6, 8)
  - [6, 8]
  - [2, 6]
  - [0, 2]

求逆

- 扩展欧几里得算法



仿射密码

明文	A	F	F	I	N	E	C	I	P	H	E	R
x	0	5	5	8	13	4	2	8	15	7	4	17
$y = 5x + 8$	8	33	33	48	73	28	18	48	83	43	28	93
$y \mod 26$	8	7	7	22	21	2	18	22	5	17	2	15
密文	I	H	H	W	V	C	S	W	F	R	C	P

密文	I	H	H	W	V	C	S	W	F	R	C
y	8	7	7	22	21	2	18	22	5	17	2
$x = 21(y - 8)$	0	-21	-21	294	273	-126	210	294	-63	189	-12
$x \mod 26$	0	5	5	8	13	4	2	8	15	7	4
明文	A	F	F	I	N	E	C	I	P	H	E

欧拉函数

- $\phi(p) = (p-1)$
- $\phi(p*q) = (p-1)*(q-1)$

对仿射密码的攻击

- $\phi(26) = \phi(2) * \phi(13) = 12 \times 26 = 312$
- 爆破！爆破！爆破！

- $y1 = a*x1 + b \bmod p$
- $y2 = a*x2 + b \bmod p$

- $y1 - y2 = a*(x1 - x2) \bmod p$

```
>>> for a, b in zip([1, 2, 3], [4,5,6]):
...  print(a, b)
...
1 4
2 5
3 6
```

```python
import sys
key = '****CENSORED****************'
flag = 'TWCTF{*******CENSORED********}'

if len(key) % 2 == 1:
    print("Key Length Error")
    sys.exit(1)

n = len(key) / 2
encrypted = ''
for c in flag:
    c = ord(c)
    for a, b in zip(key[0:n], key[n:2*n]):
        c = (ord(a) * c + ord(b)) % 251
    encrypted += '%02x' % c

print encrypted
```

真·单表替换

- 明文字母 : abcdefghijklmnopqrstuvwxyz
- 密钥字母 : phqgiumeaylnofdxjkrcvstzwb

- 明文：the quick brown fox jumps over the lazy dog
- 密文：cei jvaql hkdtf udz yvoxr dsik cei npbw gdm

真·单表替换

- 怎么攻击?
  - 爆破?
    - 26!

```
>>> t = 1
>>> for i in range(1, 27):
...     t = t*i
...
>>> t
403291461126605635584000000
>>> len(bin(t))-2
89
```

真·单表替换·字频分析

Puzzle:

cei jvaql hkdtf udz yvoxr dsik cei npbw gdm

Clues: For example G=R QVW=THE

cei=the

dictionary

Solve

8	-2.521	the jumps brown god quick over the lazy fox
9	-2.521	the quick brown god jumps over the lazy fox
10	-2.521	the jumps brown fox quick over the lazy god
11	-2.521	the quick brown fox jumps over the lazy god

目录

CATALOG

02 多表替换加密

- 添加相关标题文字
- 添加相关标题文字
- 添加相关标题文字
- 添加相关标题文字

多表加密

- what is it?
- 怎么让多表有意义?

XMAN XMAN XMAN

Vigenere

	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

Vigenere

- 明文：come greatwall
- 密钥：crypto

- 明文：c o m e g r e a t w a l l
- 密钥：c r y p t o c r y p t o c

	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	明文
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	
密钥																											

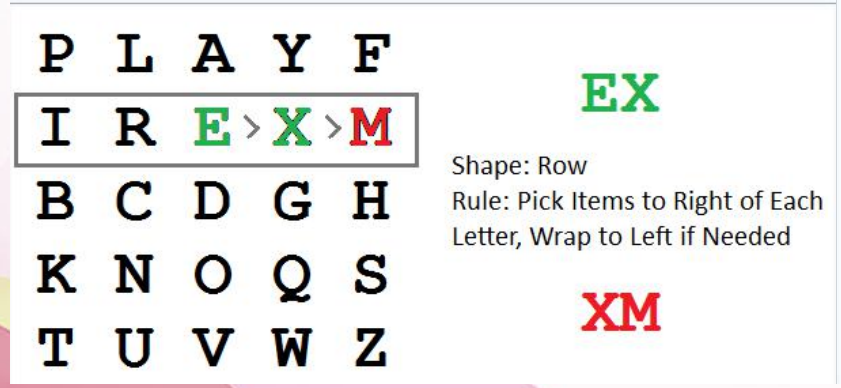
攻击Vigenere

- 卡西斯基试验
  - 一定间隔的相同字符串被加密成相同密文
- 弗里德曼试验
  - 凯撒加密不改变所有字母的概率平方和

Playfair

- "Hide the gold in the tree stump"
- HI DE TH EG OL DI NT HE TR EX ES TU MP

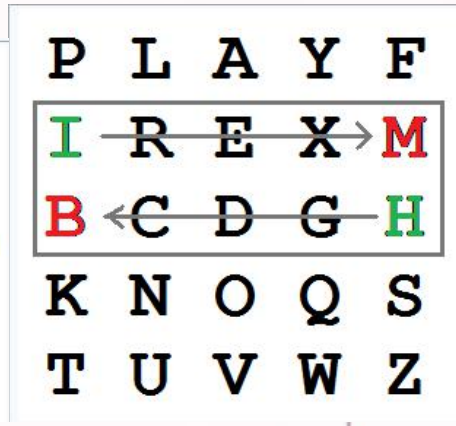
P	L	A	Y	F A
I	R	E	X	A M PLE A
B	C	D	EF G	H I=J
K LM	N	O	P Q	R S
T	U	V	W XY	Z



EX

Shape: Row
Rule: Pick Items to Right of Each Letter, Wrap to Left if Needed

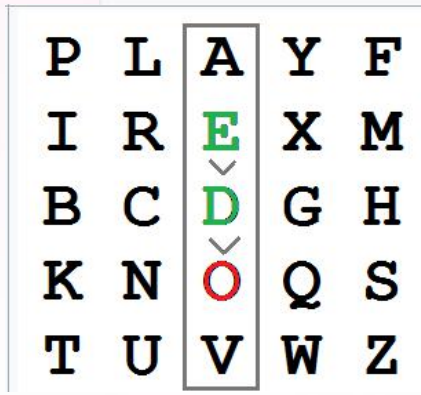
XM



HI

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

BM



DE

Shape: Column
Rule: Pick Items Below Each Letter, Wrap to Top if Needed

OD

Playfair

- 顺序相反的两个字母会泄露信息：
  - AB BA

- CrypTool，CAP4

目录

CATALOG

03 置换加密

- 添加相关标题文字
- 添加相关标题文字
- 添加相关标题文字
- 添加相关标题文字

栅栏加密

- 明文：THERE IS A CIPHER

- THEREISACIPHER
- TH ER EI SA CI PH ER

- TEESCPE
- HRIAIHR

- TEESCPEHRIAIHR

栅栏加密

- 密钥是?
- 密钥空间?

- 爆破！爆破！爆破！

目录

CATALOG

04 其他算法

- 添加相关标题文字
- 添加相关标题文字
- 添加相关标题文字
- 添加相关标题文字

Hill

- 一种矩阵运算
- 'ACT'

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

- (or GYBNQKURP in letters):

Hill

- 'A' is 0, 'C' is 2 and 'T' is 19

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

Hill

- How about 'CAT'?
- difussion!

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} \pmod{26}$$

Hill

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \pmod{26}$$

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \pmod{26}$$

培根加密

a	AAAAA	g	AABBA	n	ABBAA	t	BAABA
b	AAAAB	h	AABBB	o	ABBAB	u-v	BAABB
c	AAABA	i-j	ABAAA	p	ABBBA	w	BABAA
d	AAABB	k	ABAAB	q	ABBBB	x	BABAB
e	AABAA	l	ABABA	r	BAAAA	y	BABBA
f	AABAB	m	ABABB	s	BAAAB	z	BABBB

To encode a message each letter of the plaintext is replaced by a group of five of the letters 'A' or 'B'.

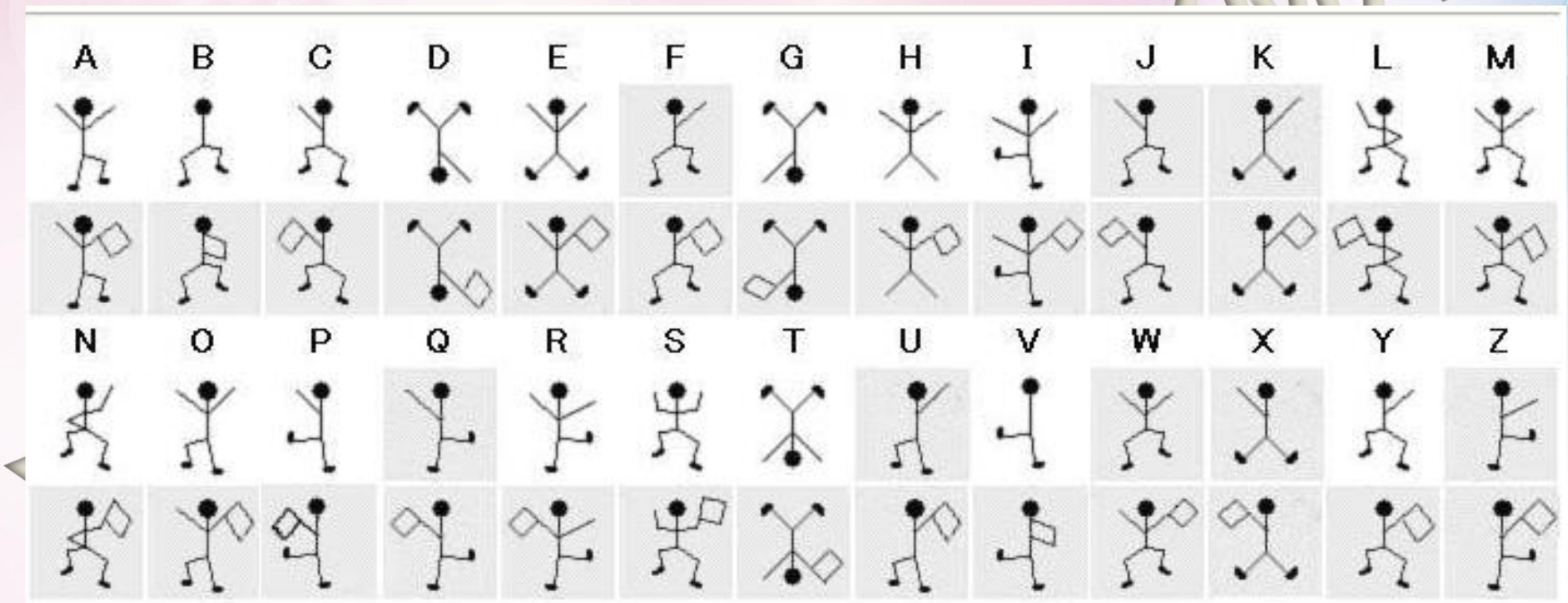
BrainFuck

- ++++++++++[>+++++++>++++++++++>+++>+<<<<-]
- >++.>+.+++++++..+++.>++.<<+++++++++++++++.
- >.+++.------.--------.>+.>.

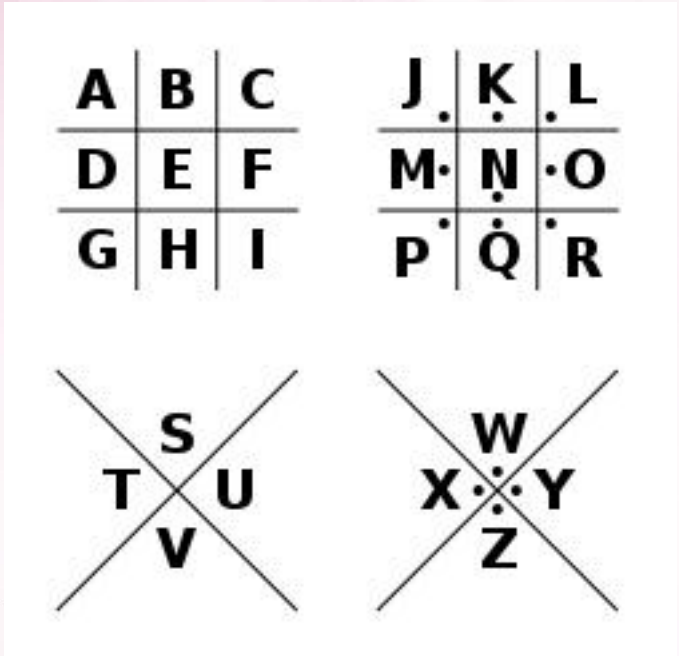
JSFuck

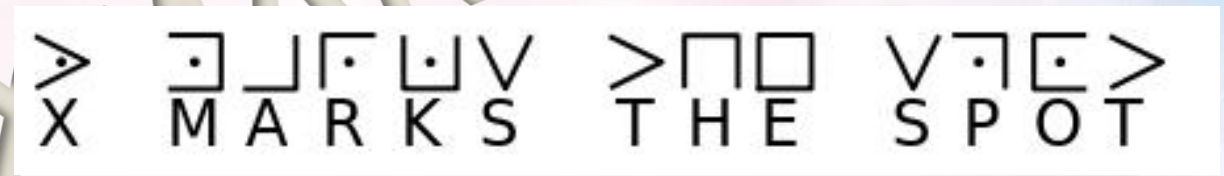
- []

舞动的小人

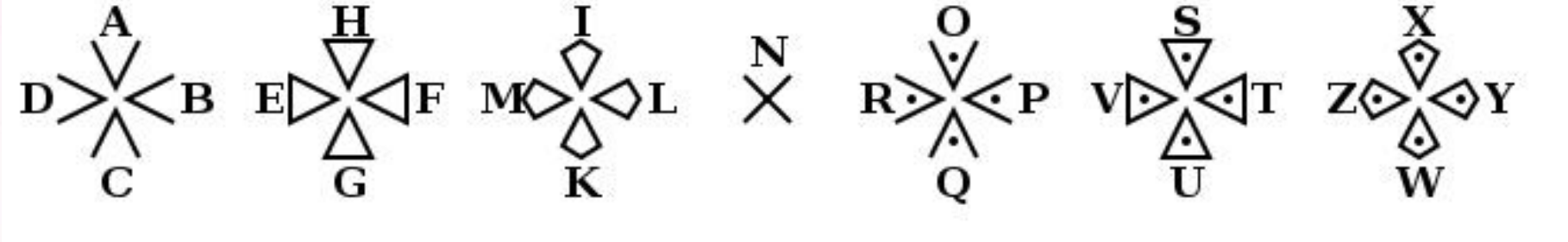


猪圈密码

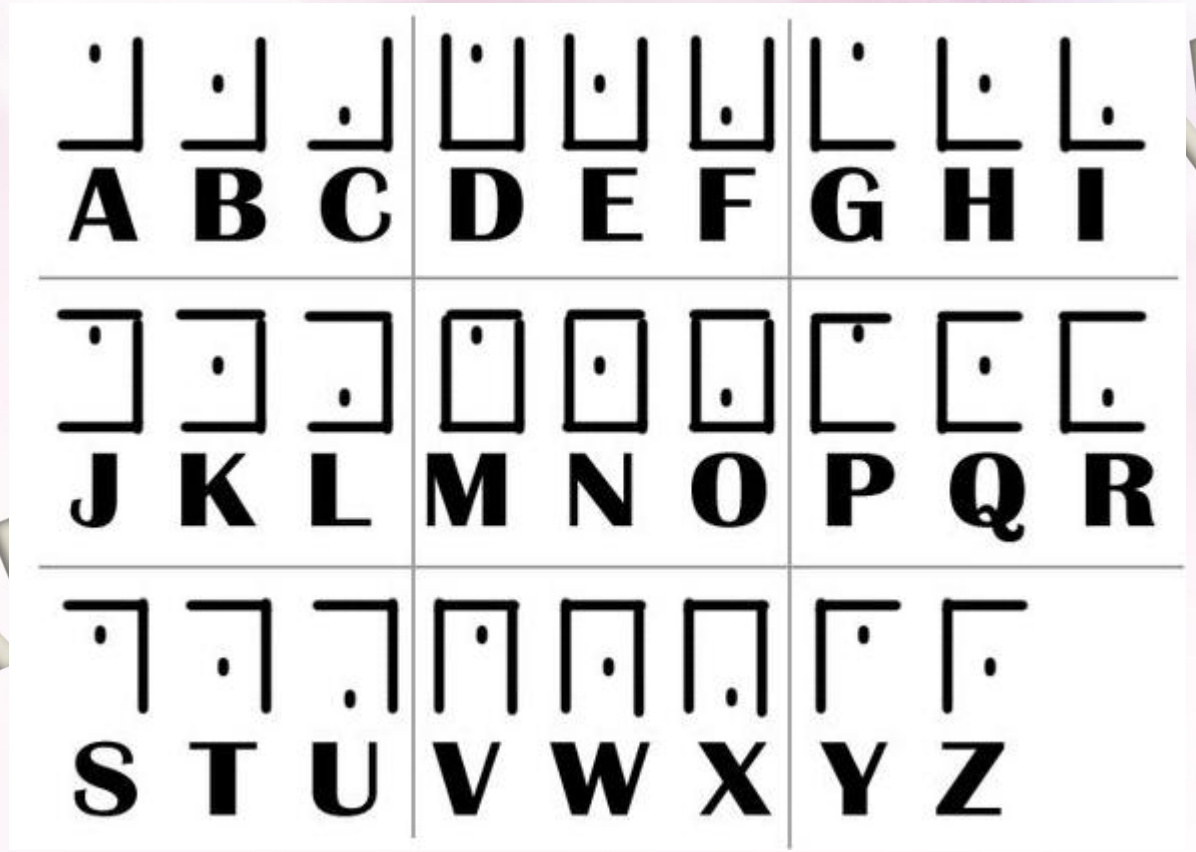


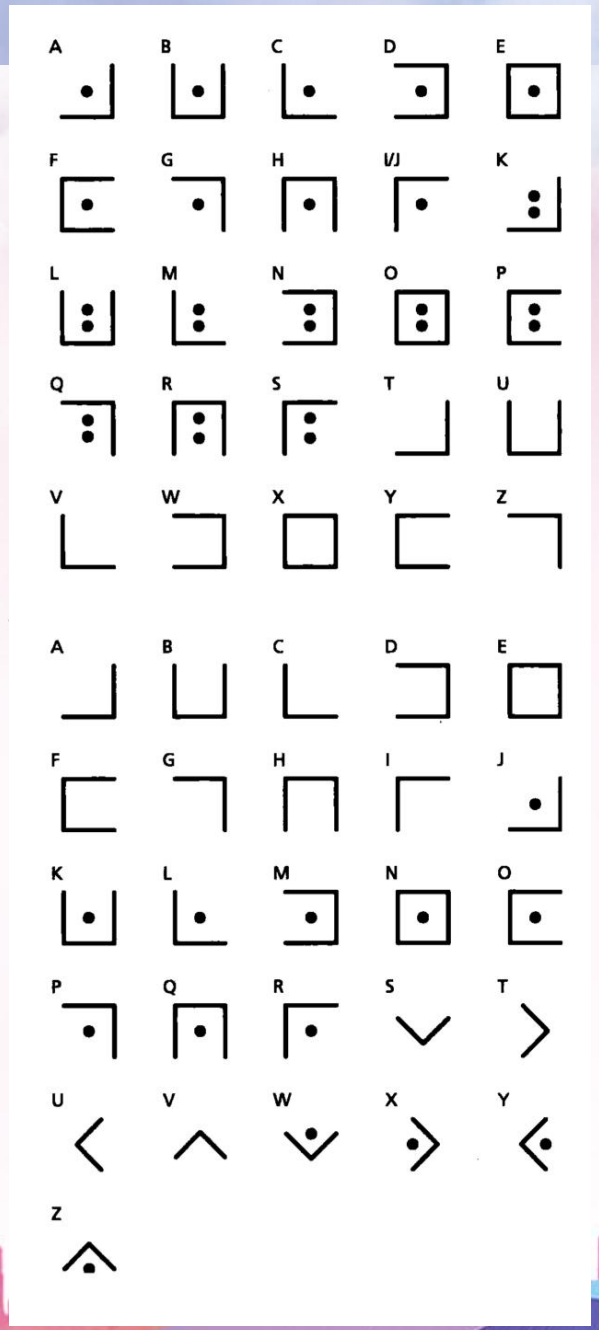


圣堂武士?

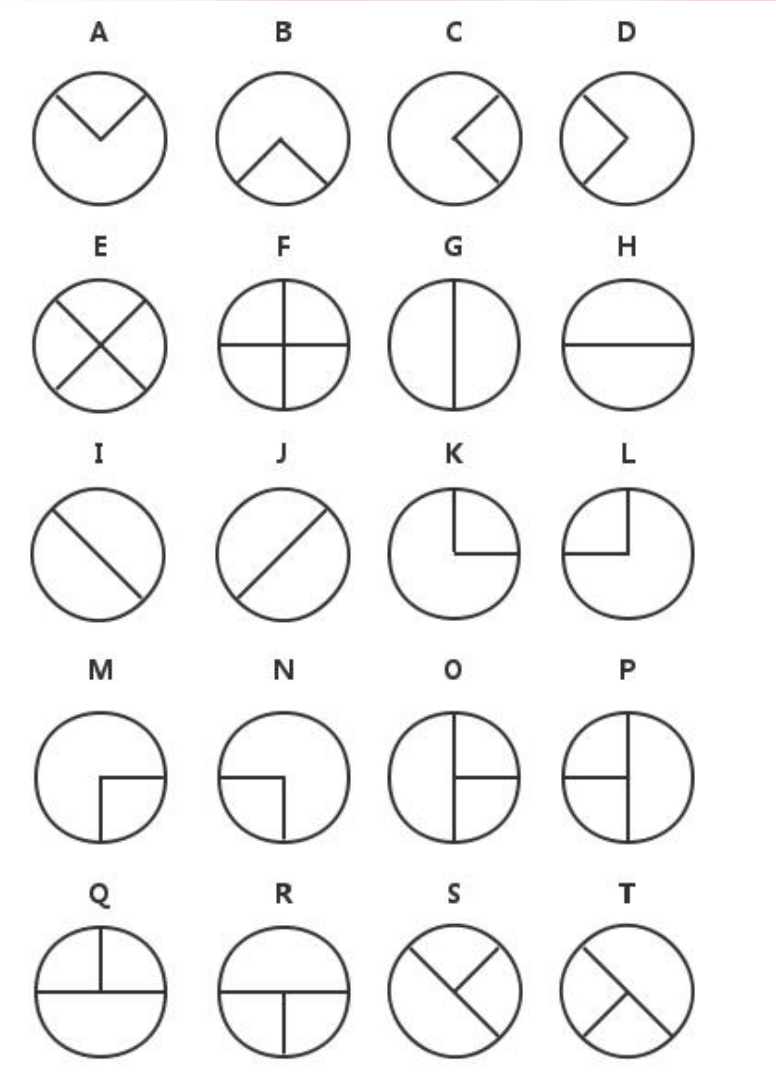


? ?


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
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

夏多?



目录

CATALOG

05 算法求逆

- 添加相关标题文字
- 添加相关标题文字
- 添加相关标题文字
- 添加相关标题文字

怎么解决古典密码？

- 1. 识别它
- 2. 攻破它（在前人的肩膀上？）

怎么识别它?

- CTF中那些脑洞大开的编码和加密
  - http://t.cn/ReRqyI7

base64

Index	Char	Index	Char	Index	Char	Index	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

base64编码

Source text (ASCII)	M								a																			
Source octets	77 (0x4d)								97 (0x61)																			
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0				
Index	19								22								4								(padding)			
Base64-encoded	T								W								E								=			
Encoded octets	84 (0x54)								87 (0x57)								69 (0x45)								61 (0x3D)			

base64隐写

Source text (ASCII)	M								a																			
Source octets	77 (0x4d)								97 (0x61)																			
Bit pattern	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0				
Index	19								22								4								(padding)			
Base64-encoded	T								W								E								=			
Encoded octets	84 (0x54)								87 (0x57)								69 (0x45)								61 (0x3D)			

Source text (ASCII)	M																											
Source octets	77 (0x4d)																											
Bit pattern	0	1	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0				
Index	19								16								(padding)								(padding)			
Base64-encoded	T								Q								=								=			
Encoded octets	84 (0x54)								81 (0x51)								61 (0x3D)								61 (0x3D)			

base32

The RFC 4648 Base 32 alphabet

Value	Symbol	Value	Symbol	Value	Symbol	Value	Symbol
0	A	8	I	16	Q	24	Y
1	B	9	J	17	R	25	Z
2	C	10	K	18	S	26	2
3	D	11	L	19	T	27	3
4	E	12	M	20	U	28	4
5	F	13	N	21	V	29	5
6	G	14	O	22	W	30	6
7	H	15	P	23	X	31	7
padding	=						

base16?

- HEX

谢　谢