Crypto and MISC Fundamentals

frostwing98

Trinity of Nanjing University

October 29, 2018

Table Of Contents I

Table Of Contents II

Table Of Contents III

Outline I

Outline II

Outline III

- *RSA
- Encrypt&Signature
- *Diffle-Hellman Key Exange
- *Common Modulus Attack

3 MISC

- Stegno
  - strings 与 binwalk
  - stegno 之文件 trick
  - Audio-Related(频谱图)
  - gif-related(01 串，morse)
  - 二维码)

Very Common Encodings

ASCII表

(American Standard Code for Information Interchange 美国标准信息交换代码)

高四位 / 低四位		ASCII控制字符											ASCII打印字符												
		0000						0001					0010		0011		0100		0101		0110		0111		
		0						1					2		3		4		5		6		7		
		十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	Ctrl	代码	转义字符	字符解释	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	十进制	字符	Ctrl
0000	0	0		^@	NUL	\0	空字符	16	▶	^P	DLE		数据链路转义	32		48	0	64	@	80	P	96	`	112	p	
0001	1	1	☺	^A	SOH		标题开始	17	◀	^Q	DC1		设备控制 1	33	!	49	1	65	A	81	Q	97	a	113	q	
0010	2	2	☻	^B	STX		正文开始	18	↕	^R	DC2		设备控制 2	34	"	50	2	66	B	82	R	98	b	114	r	
0011	3	3	♥	^C	ETX		正文结束	19	‼	^S	DC3		设备控制 3	35	#	51	3	67	C	83	S	99	c	115	s	
0100	4	4	♦	^D	EOT		传输结束	20	¶	^T	DC4		设备控制 4	36	$	52	4	68	D	84	T	100	d	116	t	
0101	5	5	♣	^E	ENQ		查询	21	§	^U	NAK		否定应答	37	%	53	5	69	E	85	U	101	e	117	u	
0110	6	6	♠	^F	ACK		肯定应答	22	▬	^V	SYN		同步空闲	38	&	54	6	70	F	86	V	102	f	118	v	
0111	7	7	•	^G	BEL	\a	响铃	23	↨	^W	ETB		传输块结束	39	'	55	7	71	G	87	W	103	g	119	w	
1000	8	8	◘	^H	BS	\b	退格	24	↑	^X	CAN		取消	40	(	56	8	72	H	88	X	104	h	120	x	
1001	9	9	○	^I	HT	\t	横向制表	25	↓	^Y	EM		介质结束	41	)	57	9	73	I	89	Y	105	i	121	y	
1010	A	10	◙	^J	LF	\n	换行	26	→	^Z	SUB		替代	42	*	58	:	74	J	90	Z	106	j	122	z	
1011	B	11	♂	^K	VT	\v	纵向制表	27	←	^[	ESC	\e	溢出	43	+	59	;	75	K	91	[	107	k	123	{	
1100	C	12	♀	^L	FF	\f	换页	28	∟	^\	FS		文件分隔符	44	,	60	<	76	L	92	\	108	l	124	|	
1101	D	13	♪	^M	CR	\r	回车	29	↔	^]	GS		组分隔符	45	-	61	=	77	M	93	]	109	m	125	}	
1110	E	14	♫	^N	SO		移出	30	▲	^^	RS		记录分隔符	46	.	62	>	78	N	94	^	110	n	126	~	
1111	F	15	☼	^O	SI		移入	31	▼	^-	US		单元分隔符	47	/	63	?	79	O	95	_	111	o	127	⌂	^Backspace 代码：DEL

注：表中的ASCII字符可以用“Alt + 小键盘上的数字键”方法输入。 2013/08/08

3byte to 4byte,”=” padding

- $2^6 = 64$
- 6bit 一个单元
- 将 3 个字符转换为 4 个字符
- 不能整除：加“=”

Very Common Encodings

文本	M								a								n							
ASCII编码	77								97								110							
二进制位	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
索引	19								22								5							
Base64编码	T								W								F							

Very Common Encodings

数值	字符	数值	字符	数值	字符	数值	字符
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

Very Common Encodings

文本（1 Byte）	A																							
二进制位	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
二进制位（补0）	0	1	0	0	0	0	0	1	**0**	**0**	**0**	**0**	0	0	0	0	0	0	0	0	0	0	0	0
Base64编码	Q								Q				=				=							
文本（2 Byte）	B								C															
二进制位	0	1	0	0	0	0	1	0	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0
二进制位（补0）	0	1	0	0	0	0	1	0	0	1	0	0	0	0	1	1	**0**	**0**	0	0	0	0	0	0
Base64编码	Q								k				M				=							

The RFC 4648 Base 32 alphabet

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

Table 5: The Base 16 Alphabet

Value	Encoding	Value	Encoding	Value	Encoding	Value	Encoding
0	0	4	4	8	8	12	C
1	1	5	5	9	9	13	D
2	2	6	6	10	A	14	E
3	3	7	7	11	B	15	F

Outline I

Outline II

- Curve Cipher 曲折加密
- Columnar Transposition Cipher 列移位密码
- Polybius Square Cipher 波利比奥斯方阵密码
- *ADFGX/ADFGVX 码
- *Vignere 弗吉尼亚密码
- *Hill 希尔密码
- Pigpen Cipher 猪圈密码
- Templar Cipher 圣堂武士密码

Contemporary Cryptography: Symmetric

- md5
- SHA
- *DES
- 3DES
- *AES

Contemporary Cryptography: Asymmetric

Outline III

- *RSA
- Encrypt&Signature
- *Diffle-Hellman Key Exange
- *Common Modulus Attack

3 MISC

- Stegno
  - strings 与 binwalk
  - stegno 之文件 trick
  - Audio-Related(频谱图)
  - gif-related(01 串，morse)
  - 二维码)

XXencode 3-byte to 4 byte encode, 0-padding

- for 6-bit code *a*
- a -> [0,63]
- 将 3 个字符转换为 4 个字符
- 分别映射到 +-0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghi

原文本：The quick brown fox jumps over the lazy dog 编码后：hJ4VZ653pOKBf647mPrRi64NjS0-eRKpkQm-jRaJm65FcNG-gMLdt64FjNkc+

UUencode 3-byte to 4 byte encode, 0-padding, offset=32

- for 6-bit code a
- a -> [0,63]
- a+32 -> [32,95] -> [‘ ‘,‘_‘]
- 将 3 个字符转换为 4 个字符

如果 a==0, 应转换为单引号（0x60)，因为其优于‘ ‘

ppencode

ppencode-Perl 把 Perl 代码转换成只有英文字母的字符串。

rrencode

rrencode 可以把 ruby 代码全部转换成符号

jjencode

jjencode 将 JS 代码转换成只有符号的字符串

aaencode

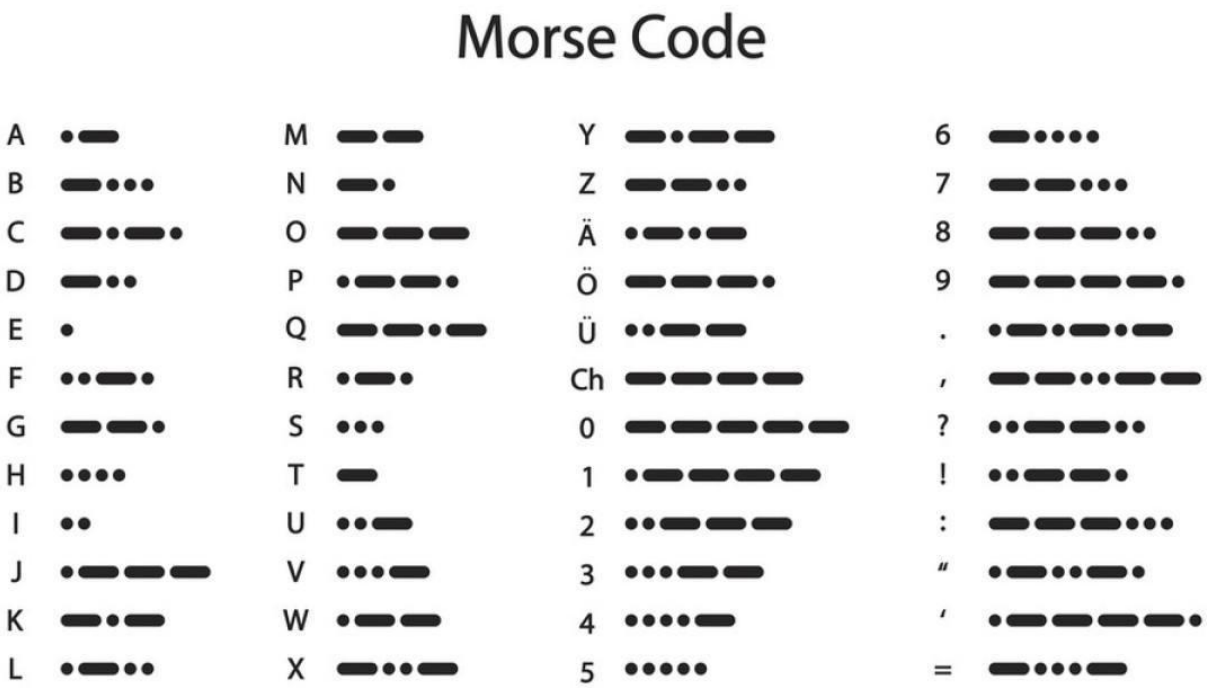
传说中的颜文字 js 加密

brainfuck

- a minimized language
- 8 symbols:> < + - . , [ ]
- > 寄存器指针 +1
- < 寄存器指针-1
- + 寄存器内容 +1
- − 寄存器内容-1
- . 输出
- , 输入
- [若指向单元值 ==0 跳出到对应方括号后第一个指令
-] 若指向单元值!=0 向前跳到对应方括号

Ook. Ook?
Move the Memory Pointer to the next array cell.
Ook? Ook.
Move the Memory Pointer to the previous array cell.
Ook. Ook.
Increment the array cell pointed at by the Memory Pointer.
Ook! Ook!
Decrement the array cell pointed at by the Memory Pointer.
Ook. Ook!
Read a character from STDIN and put its ASCII value into the cell pointed at by the Memory Pointer.
Ook! Ook.
Print the character with ASCII value equal to the value in the cell pointed at by the Memory Pointer.
Ook! Ook?
Move to the command following the matching Ook? Ook! if the value in the cell pointed at by the Memory Pointer is zero. Note that Ook! Ook? and Ook? Ook! commands nest like pairs of parentheses, and matching pairs are defined in the same way as for parentheses.
Ook? Ook!
Move to the command following the matching Ook! Ook? if the value in the cell pointed at by the Memory Pointer is non-zero.

Oook!


Morse Code
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
Ä
Ö
Ü
Ch
0
1
2
3
4
5
6
7
8
9
.
,
?
!
:
"
'
=


Esc 27
F1 112
F2 113
F3 114
F4 115
F5 116
F6 117
F7 118
F8 119
F9 120
F10 121
F11 122
F12 123
` 192
1 49
2 50
3 51
4 52
5 53
6 54
7 55
8 56
9 57
0 48
- 189
= 187
\ 220
8
TAB 9
Q 81
W 87
E 69
R 82
T 84
Y 89
U 85
I 73
O 79
P 80
[219
] 221
Enter 13
Caps L 20
A 65
S 83
D 68
F 70
G 71
H 72
J 74
K 75
L 76
; 186
' 222
Shift 16
Z 90
X 88
C 67
V 86
B 66
N 78
M 77
, 188
. 190
\ 191
Shift 16
Ctrl 17
Win 91
Alt 18
Space 32
Alt 18
Win 92
RightK 93
Ctrl 17

Outline I

Outline II

- Curve Cipher 曲折加密
- Columnar Transposition Cipher 列移位密码
- Polybius Square Cipher 波利比奥斯方阵密码
- *ADFGX/ADFGVX 码
- *Vignere 弗吉尼亚密码
- *Hill 希尔密码
- Pigpen Cipher 猪圈密码
- Templar Cipher 圣堂武士密码

Contemporary Cryptography: Symmetric

- md5
- SHA
- *DES
- 3DES
- *AES

Contemporary Cryptography: Asymmetric

Outline III

- *RSA
- Encrypt&Signature
- *Diffle-Hellman Key Exange
- *Common Modulus Attack

3 MISC

- Stegno
  - strings 与 binwalk
  - stegno 之文件 trick
  - Audio-Related(频谱图)
  - gif-related(01 串，morse)
  - 二维码)

Atbash 埃特巴什码

埃特巴什码 (Atbash Cipher) 是一种以字母倒序排列作为特殊密钥的替换加密，也称也就是下面的对应关系：

ABCDEFGHIJKLMNOPQRSTUVWXYZ
ZYXWVUTSRQPONMLKJIHGFEDCBA

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

Caesar 凯撒密码

凯撒密码是一种替换加密，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。
例，当偏移量是 3 的时候，所有的字母 A 将被替换成 D，B 变成 E，以此类推.
明文：The quick brown fox jumps over the lazy dog
offset：1
密文：Uif rvjdl cspxo gpy kvnqt pwfs uif mbaz eph
狭义的 Caesar 密码，offset 为 3

ROT ROT 码

ROT5/13/18/47 是一种简单的码元位置顺序替换暗码。此类编码具有可逆性，可以自我解密，主要用于应对快速浏览，或者是机器的读取。

ROT5：+5, 只对数字进行编码. e.g. 0->5,1->6

ROT13：+13, 只对字母进行编码. e.g. A->N B->O

ROT18：combination of ROT-5 and ROT-13

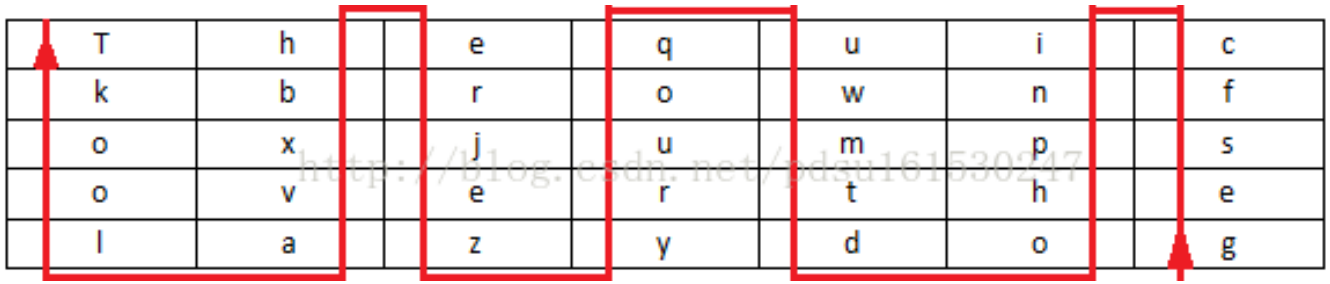
ROT47：+47, 对 ASCII 进行。

Rail-Fence 栅栏密码

把要加密的明文分成 N 个一组，然后把每组的第 i 个字符组合之后链接。

Example(N=2):
明文：The quick brown fox jumps over the lazy dog
去空格：Thequickbrownfoxjumpsoverthelazydog
分组：Th eq ui ck br ow nf ox ju mp so ve rt he la zy do g
密文：Teucbonojmsvrhlzdghqikrwfxupoeteayo

Curve Cipher 曲折加密



T	h		e		q	u	i		c
k	b		r		o	w	n		f
o	x		j		u	m	p		s
o	v		e		r	t	h		e
l	a		z		y	d	o		g

Columnar Transposition Cipher 列移位密码列移位密码
通过一个简单的规则将明文打乱混合成密文. 例如：原文：The quick brown fox jumps over the lazy dog

T	h	e	q	u	i	c
k	b	r	o	w	n	f
o	x	j	u	m	p	s
o	v	e	r	t	h	e
l	a	z	y	d	o	g

密钥：how are u

h	o	w	a	r	e	u
3	4	7	1	5	2	6

T	h	e	q	u	i	c
k	b	r	o	w	n	f
o	x	j	u	m	p	s
o	v	e	r	t	h	e
l	a	z	y	d	o	g

按 how are u 在字母表中的出现的先后顺序进行编号，我们就有 a 为 1,e 为 2，h 为 3，o 为 4，r 为 5，u 为 6，w 为 7，所以先写出 a 列，其次 e 列，以此类推写出的结果便是密文：
qoury inpho Tkool hbxva uwmtd cfseg erjez

Polybius Square Cipher 波利比奥斯方阵密码

波利比奥斯方阵密码（Polybius Square Cipher 或称波利比奥斯棋盘）是棋盘密码的一种.

	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

明文：THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

密文：442315 4145241325 1242345233 213453 2445323543 442315 31115554 143422

ADFGX

ADFGX 密码 (ADFGX Cipher) 是结合了改良过的 Polybius 方格替代密码与单行换位密码的矩阵加密密码，使用了 5 个合理的密文字母：A，D，F，G，X

ADFGVX 密码实际上就是 ADFGX 密码的扩充升级版，一样具有 ADFGX 密码相同的特点，加密过程也类似，不同的是密文字母增加了 V

Example:

	A	D	F	G	X
A	p	h	q	g	m
D	e	a	y	n	o
F	f	d	x	k	r
G	c	v	s	z	v
X	b	u	t	i/j	l

text:THE QUICK BROWN FOX
password:XF AD DA AF XD XG GA FG XA FX DX GX DG FA DX FF
with 列移位密钥：howareu

h	o	w	a	r	e	u
3	4	7	1	5	2	6
X	F	A	D	D	A	A
F	X	D	X	G	G	A
F	G	X	A	F	X	D
X	G	X	D	G	F	A
D	X	F	F			

密文：DXADF AGXF XFFXD FXGGX DGFG AADA ADXXF

Viginere

维吉尼亚密码 (Vigenère Cipher) 是在单一恺撒密码的基础上扩展出多表代换密码，根据密钥 (当密钥长度小于明文长度时可以循环使用) 来决定用哪一行的密表来进行替换，以此来对抗字频统计

Classic Crytography

	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

明文：THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

密钥 (循环使用，密钥越长相对破解难度越大)：CULTURE

加密过程：如果第一行为明文字母，第一列为密钥字母，那么明文字母’T’列和密钥字母’C’行的交点就是密文字母’V’，以此类推。

密文：VBP JOZGM VCHQE JQR UNGGW QPPK NYI NUKR XFK

破解方法：使用卡方检验和重合指数算法：

http://www.practicalcryptography.com/cryptanalysis/stochast
searching/cryptanalysis-vigenere-cipher/

Hill

希尔密码 (Hill Cipher) 将每个字母转换成 26 进制数字的 n 维向量跟一个 n×n 的矩阵相乘，再将得出的结果 MOD26
例如明文为 ACT，密钥为 GYBNQKURP。
加密过程：

$$M = \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} \quad K = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

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

密码为 FIN

解密过程：

$$K^{-1} = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} (mod\ 26)$$

$$M = K^{-1}C = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix}$$

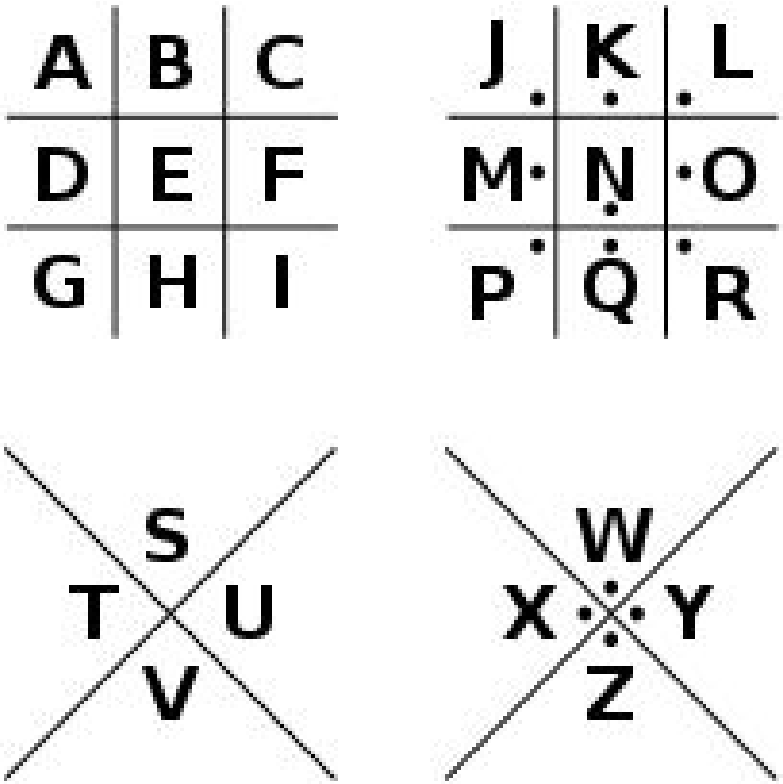
$$\equiv \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} (mod\ 26)$$

原文为 ACT

破解方法：已知明文攻击

http://www.practicalcryptography.com/cryptanalysis/stochast
searching/cryptanalysis-hill-cipher/

Pigpen Cipher



>ΠΟ ΡΑ<ΓΙ⊔Ο ⊔ΡΕVΟ ⊏Ε> ⅃Α<ϽΓV ΕΛΟ
Γ >ΠΟ ⊔⅃Λ<ϽΕΓ

Templar Cipher

Outline I

Outline II

Outline III

- *RSA
- Encrypt&Signature
- *Diffle-Hellman Key Exange
- *Common Modulus Attack

3 MISC

- Stegno
  - strings 与 binwalk
  - stegno 之文件 trick
  - Audio-Related(频谱图)
  - gif-related(01 串，morse)
  - 二维码)

MD5 Message-Digest Algorithm 是一种被广泛使用的密码散列函数，可以产生出一个 128 位（16 字节）的散列值（hash value），用于确保信息传输完整一致。
MD5 以 512 位分组来处理输入的信息，且每一分组又被划分为 16 个 32 位子分组，经过了一系列的处理后，算法的输出由四个 32 位分组组成，将这四个 32 位分组级联后将生成一个 128 位散列值

- 只要改动极小的部分，就会使得 md5 发生巨大的变化。
- 不可逆

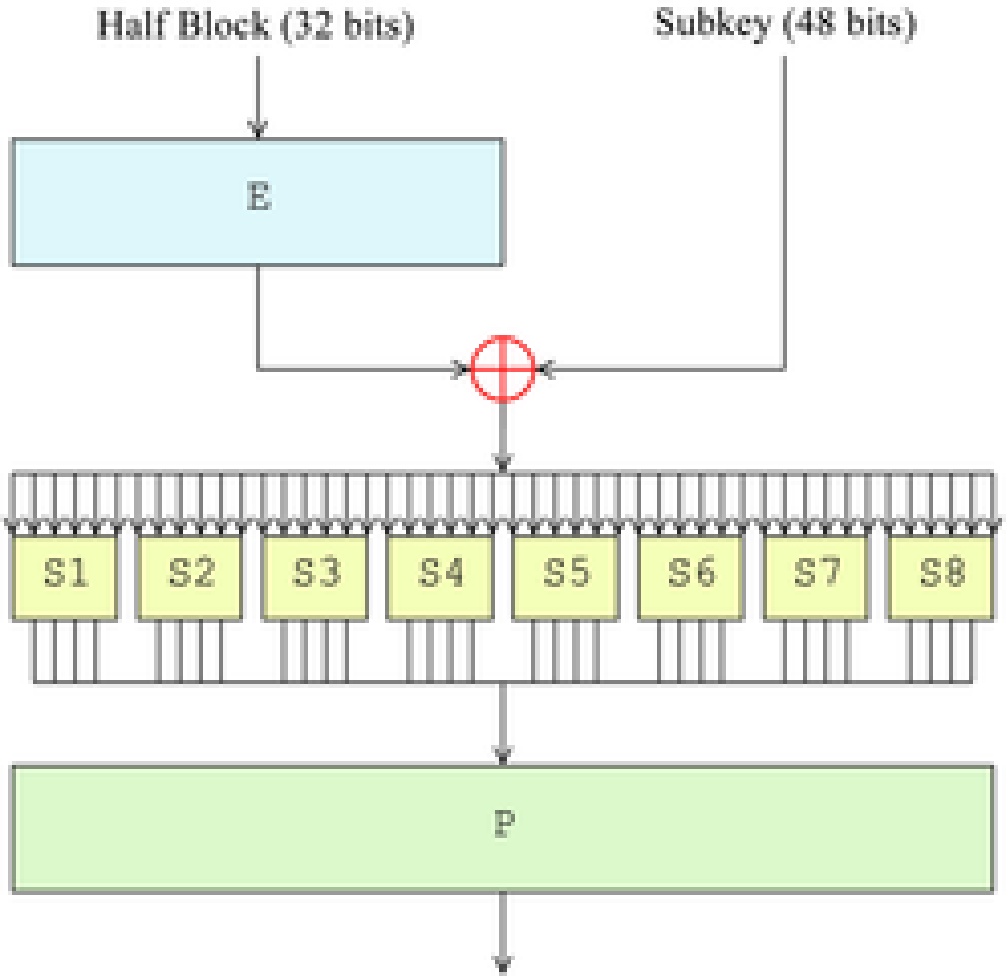
Secure Hash Algorithm

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

- 补位
- 补长度
- 准备使用的常量
- 准备需要使用的函数
- 计算消息摘要

参见
https://blog.csdn.net/jingcheng345413/article/details/549692

DES(Data Encryption Standard) 是一种使用密钥加密的块算法

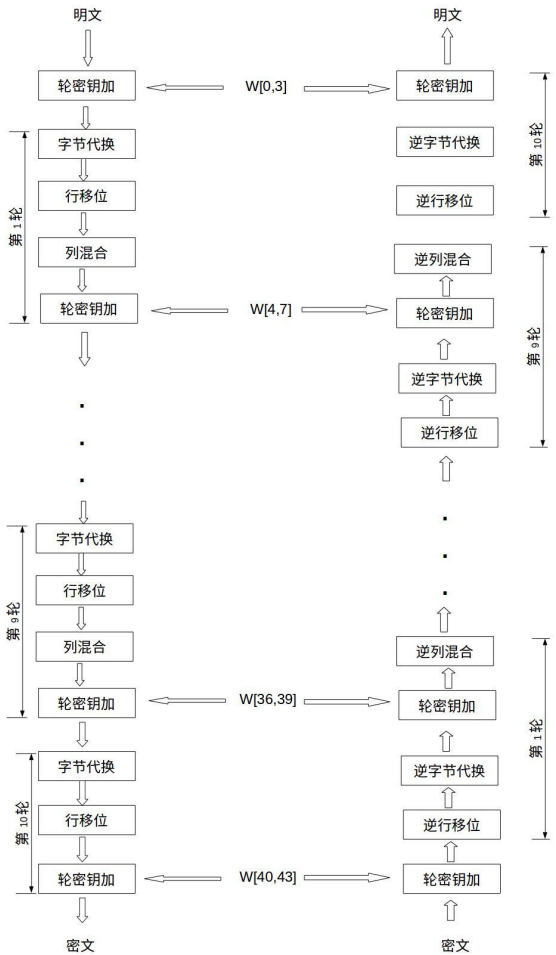


3DES 是 DES 向 AES 过渡的加密算法，使用 3 条 56 位的密钥对数据进行三次加密

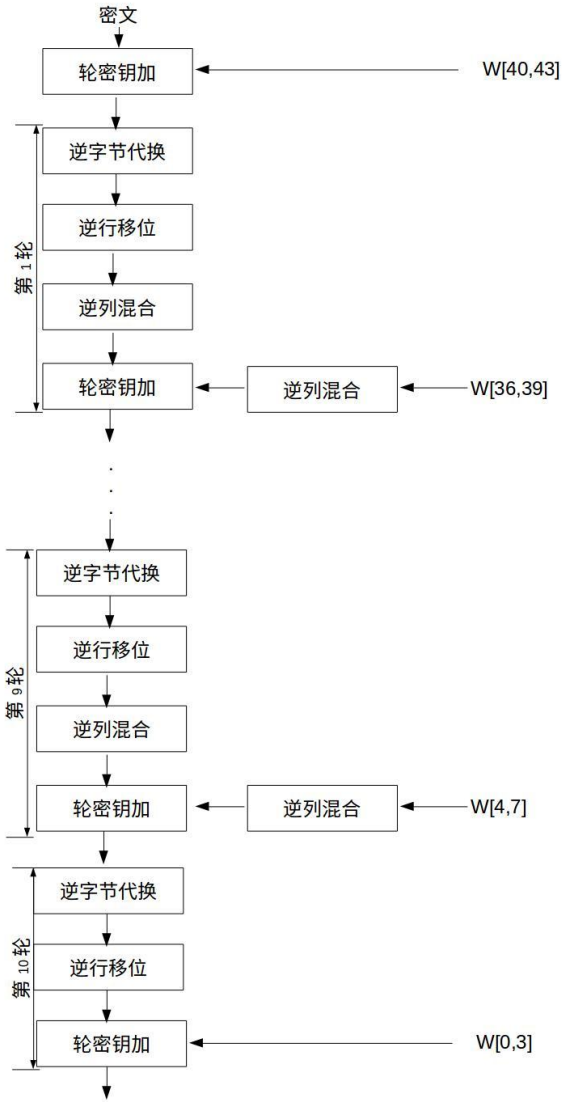
- 加密过程：C=Ek3(Dk2(Ek1(P)))
- 解密过程：P=Dk1(EK2(Dk3(C)))

- **易用性**两个密钥合起来有效密钥长度有 112bit，可以满足商业应用的需要，若采用总长为 168bit 的三个密钥，会产生不必要的开销。
- **兼容性**加密时采用加密-解密-加密，而不是加密-加密-加密的形式，这样有效的实现了与现有 DES 系统的向后兼容问题。因为当 K1=K2 时，三重 DES 的效果就和原来的 DES 一样，有助于逐渐推广三重 DES。
- **安全性**三重 DES 具有足够的安全性，目前还没有关于攻破 3DES 的报道。

AES(Advanced Encryption Standard)



Contemporary Cryptography: Symmetric



Outline I

Outline II

Outline III

- *RSA
- Encrypt&Signature
- *Diffle-Hellman Key Exange
- *Common Modulus Attack

3 MISC

- Stegno
  - strings 与 binwalk
  - stegno 之文件 trick
  - Audio-Related(频谱图)
  - gif-related(01 串，morse)
  - 二维码)

Rivest-Shamir-Adleman

Outline I

Outline II

- Curve Cipher 曲折加密
- Columnar Transposition Cipher 列移位密码
- Polybius Square Cipher 波利比奥斯方阵密码
- *ADFGX/ADFGVX 码
- *Vignere 弗吉尼亚密码
- *Hill 希尔密码
- Pigpen Cipher 猪圈密码
- Templar Cipher 圣堂武士密码

Contemporary Cryptography: Symmetric

- md5
- SHA
- *DES
- 3DES
- *AES

Contemporary Cryptography: Asymmetric

Outline III

- *RSA
- Encrypt&Signature
- *Diffle-Hellman Key Exange
- *Common Modulus Attack

3 MISC

- Stegno
  - strings 与 binwalk
  - stegno 之文件 trick
  - Audio-Related(频谱图)
  - gif-related(01 串，morse)
  - 二维码)

strings 与 binwalk

strings: 打印文件中可打印的字符

binwalk: 用于搜索给定二进制镜像文件以获取嵌入的文件和代码

文件 trick：魔数 (magic number)

很多类型的文件，其起始的几个字节的内容是固定的:

JPEG	jpg;jpeg	0xFFD8FF
PNG	png	0x89504E470D0A1A0A
GIF	gif	GIF8
ZIP Archive	zip;jar	0x504B0304
MPEG	mpg;mpeg	0x000001BA

文件 trick: 奇怪的压缩包

- windows 全家桶 (.doc 与.xls)
- 真的只是一张图片而已 (图种)
- 我真的没加密啊! (伪加密)
  - 504B0102: dir entry
  - xxxxxxxx:
  - 0000: 伪加密

文件 trick: 奇怪的图片

- 魔数
- 大小
- CRC

Thank you!