信息安全~密码学

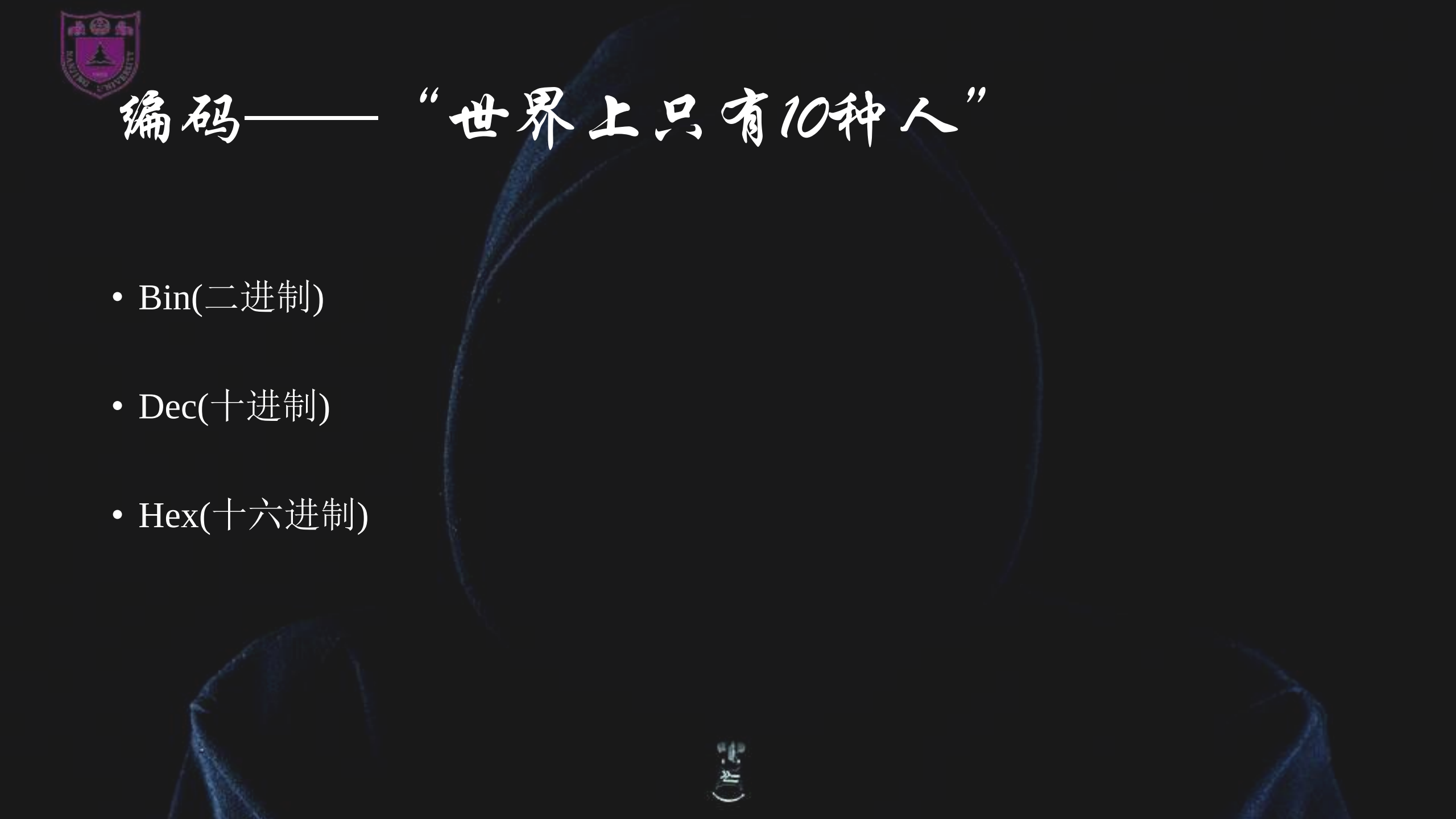
王润川

2021.11.10

编码

编码——“世界上只有10种人”

- Bin(二进制)
- Dec(十进制)
- Hex(十六进制)



编码——ASCII编码

- ASCII编码
  - 0~9、A~Z、a~z

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 0000 0						ASCII控制字符 0001 1						ASCII打印字符 0010 2		ASCII打印字符 0011 3		ASCII打印字符 0100 4		ASCII打印字符 0101 5		ASCII打印字符 0110 6		ASCII打印字符 0111 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

编码——ASCII编码

- 摩尔斯编码
  - 点(·)：基本单位
  - 划(-)：3个点的长度
  - 点与划之间的间隔：2个点的长度
  - 字母&数字之间的间隔：7个点的长度

编码——Base全家桶

- Base界的“翘楚”——Base64
- 2^6=64，6位(bit)为一个单元
- 3字节对应4个单元
- 单元可以是A~Z、a~z、0~9、+、/
- 不能整除，添加“=”
  - 辨别法，但不是万能方法

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
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	/

编码——Base全家桶

A：0x41
0100 0001
010000 010000
16 16
QQ(==)

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							

编码——Base全家桶

- Base32
  - A~Z、2~7，添加“=”
- Base16
  - A~F、0~9，不添加“=”
- https://www.qqxiuzi.cn/bianma/base64.htm

编码——UUencode编码

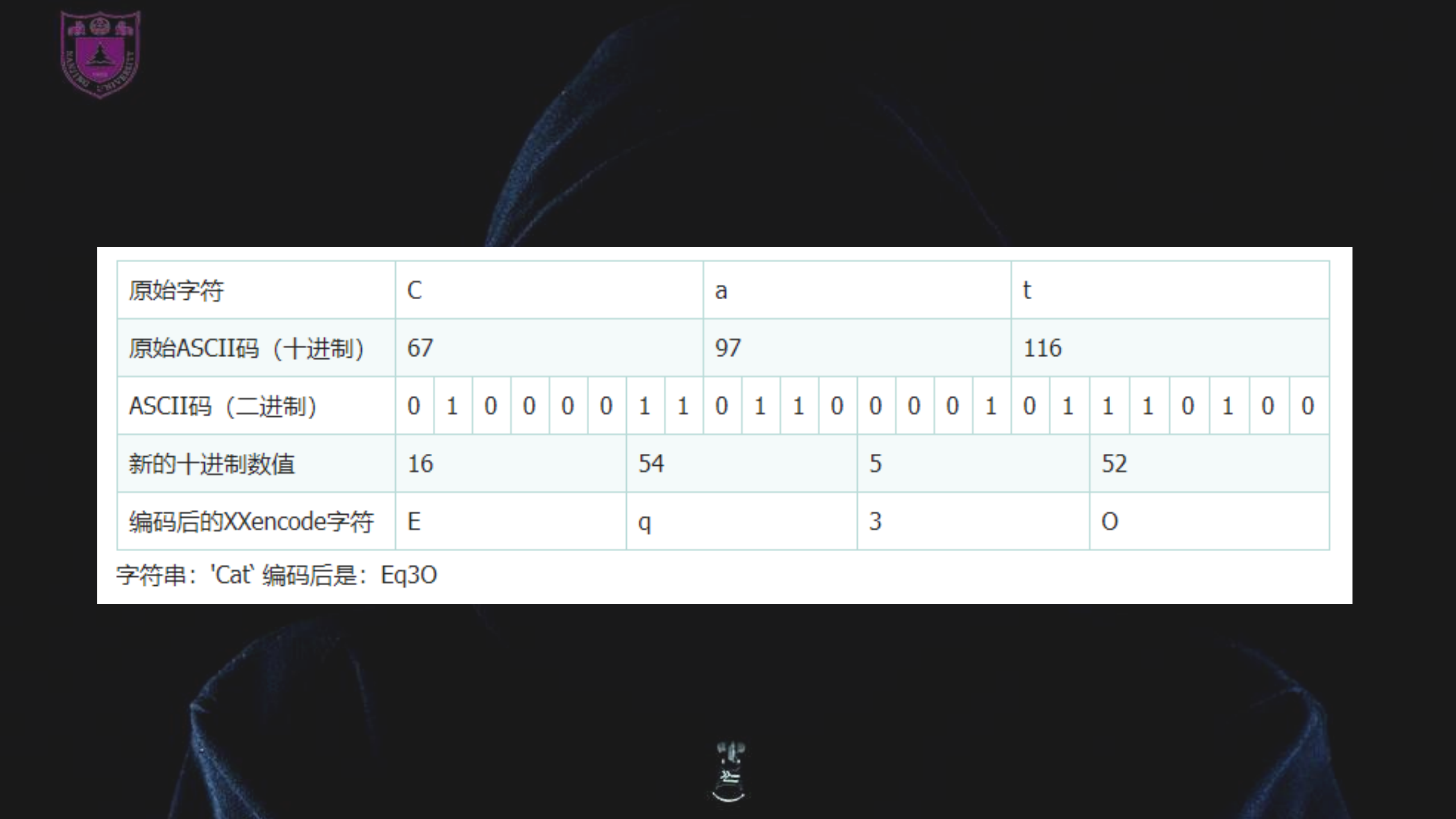
- 3个字符(字节)转换为4个字符
- 每个字符a占6位
- a -> [0, 63]
- a + 32 -> [32, 95] -> [‘ ’, ‘_’]
- 特殊符号很多

原始字符	C			a			t		
原始ASCII码（十进制）	67			97			116		
ASCII码（二进制）	0 1 0 0 0 0 1 1			0 1 1 0 0 0 0 1			0 1 1 1 0 1 0 0		
新的十进制数值	16			54			5		52
+32	48			86			37		84
编码后的Uuencode字符	0			V			%		T

字符串：’Cat‘ 编码后是：cV%T

编码——XXencode编码

- 3个字符(字节)转换为4个字符
- 每个字符a占6位
- a -> [0, 63] -> +、-、0~9、A~Z、a~z
- 60个字符(45字节)输出为一行
- 头部添加字节长度对应字符，尾部补+
- 没有特殊符号



原始字符	C								a								t							
原始ASCII码（十进制）	67								97								116							
ASCII码（二进制）	0	1	0	0	0	0	1	1	0	1	1	0	0	0	0	1	0	1	1	1	0	1	0	0
新的十进制数值	16						54						5				52							
编码后的XXencode字符	E						q						3				O							

字符串：'Cat' 编码后是：Eq3O

古典密码

古典密码

- 替换加密
  - 单表替换加密
  - 多表替换加密
- 置换加密
- 其它加密

单表替换加密——埃特巴什码

- Atbash Cipher

- 字母倒序排序作为特殊密钥的替换加密
- 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

单表替换加密——凯撒密码

- Caesar cipher

- 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。

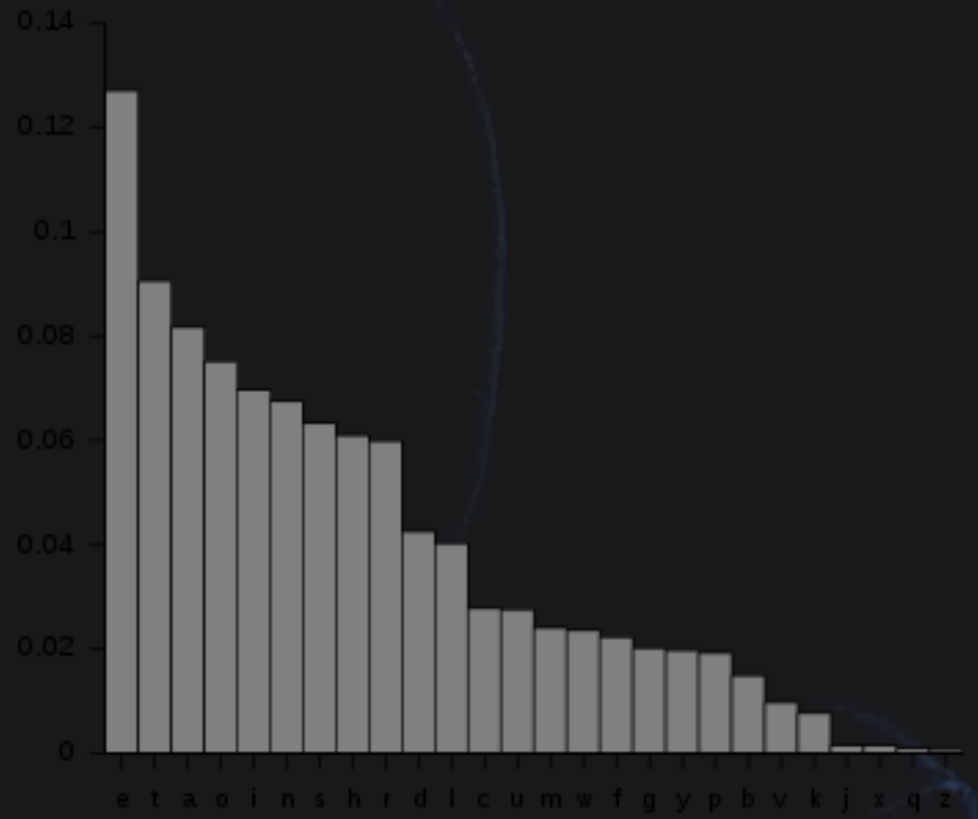
- 狭义凯撒密码——offset：3

明文：The quick brown fox jumps over the lazy dog　　offset：1

密文：Uif rvjdl cspxo gpy kvnqt pwfs uif mbaz eph

单表替换加密の爆破方法

- 密文长度较小：爆破
- 密文长度较大：词频统计



替换加密——波利比奥斯方阵密码

- Polybius Square Cipher
- 棋盘密码的一种
- 改良方案：ADFGX密码

	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

	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

明文： The quick brown fox jumps over the lazy dog

密文：442315 4145241325 1242345233 213453 2445323543 442315 31115554 143422

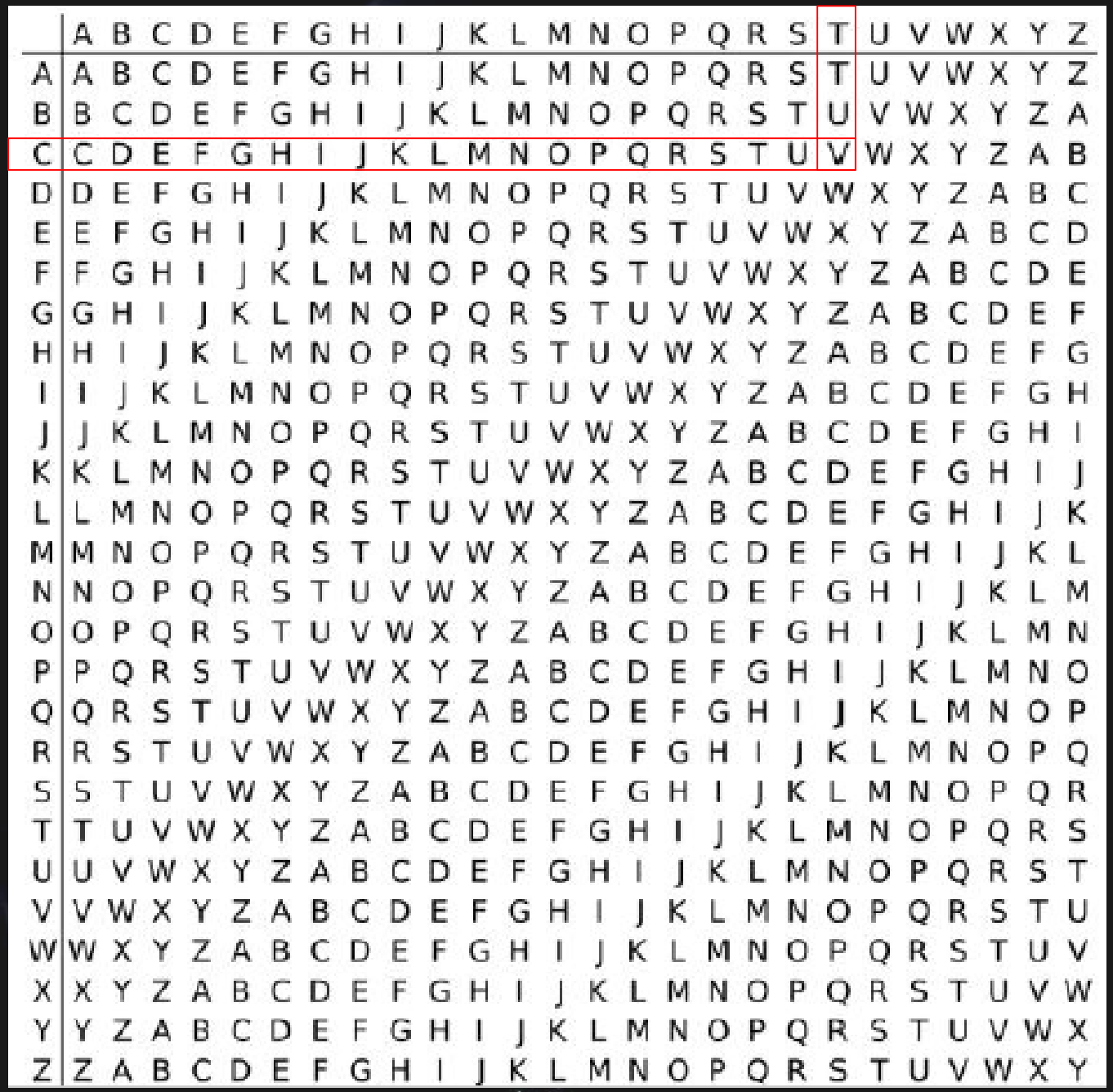
替换加密——维吉尼亚密码

- Vigenère Cipher

- 单一的凯撒密码基础上扩展出的多表替换密码
- 根据密码决定使用哪一行的密表来替换
- 当密钥长度小于明文长度时可以重复使用

明文：THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

密钥：CULTURE



	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

三维呢！

替换加密——维吉尼亚密码

- Vigenère Cipher

- 单一的凯撒密码基础上扩展出的多表替换密码
- 根据密码决定使用哪一行的密表来替换
- 当密钥长度小于明文长度时可以重复使用

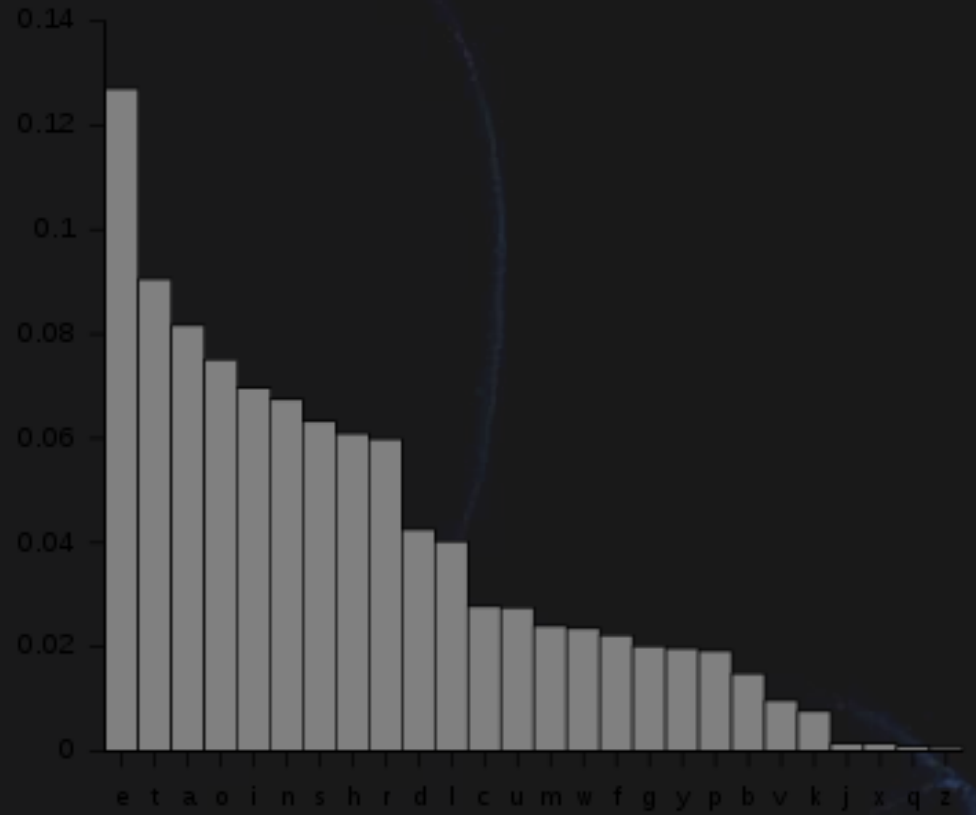
明文：THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

密钥：CULTURE

密文：VBP JOZGM VCHQE JQR UNGGW QPPK NYI NUKR XFK

维吉尼亚密码の爆破方法

- 思想：爆破 & 词频统计
  - 间隔密钥长度字符使用的替换表相同
- 方法：试验 or 网址
  - 卡西斯基试验：常用单词如果使用重复的密钥加密，那么两个相同的连续串间隔将是密钥长度的倍数
  - 弗里德曼试验：凯撒加密不改变所有字母的概率平方和
  - 商业网址：https://www.quipqiup.com/



置换加密——栅栏密码

- Rail-Fence

- 把要加密的明文分成N个一组，然后把每组的第i个字符组合后链接

明文：The quick brown fox jumps over the lazy dog

分组：Th eq ui ck br ow nf ox ju mp so ve rt he la zy do g（N：2）

密文：Teucbonojmsvrhlzdghqikrwfxupoeteayo

置换密码——曲折加密

- Curve Cipher

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

明文：The quick brown fox jumps over the lazy dog

密文：gesfcinphodtmwuqouryzejrehbxvalookT

置换密码——列移位密码

- Columnar Transposition Cipher

- 通过一个简单的规则将明文打乱混合成密文

明文：The quick brown fox jumps over the lazy dog

密钥：how are u

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

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

置换密码——列移位密码

- Columnar Transposition Cipher

- 通过一个简单的规则将明文打乱混合成密文

明文：The quick brown fox jumps over the lazy dog

密钥：how are u

密文：qoury inpho Tkool hbxva uwmtd cfseg erjez

列移位密码の爆破方法

- 移位密码的核心：字符变换的顺序

- 常用的方法：爆破方法 & 语义分析
  - 爆破顺序：
    - 先爆破字段长度、再爆破顺序
  - 语义分析例子：
    - 密文：lafgea{s_eyay_scyprt}o
    - 字段长度：lafg => flag，长度为4，顺序为1234 => 3124
    - 明文：flag{easy_easy_crypto}

其它加密——希尔密码

- Hill Cipher
- 将字母转换成0~25的n维数字向量，与一个n×n的矩阵相乘，再将得出的结果mod 26

- 例如明文为ACT，密钥为GYBNQKUR，密码为POH

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

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

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

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

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

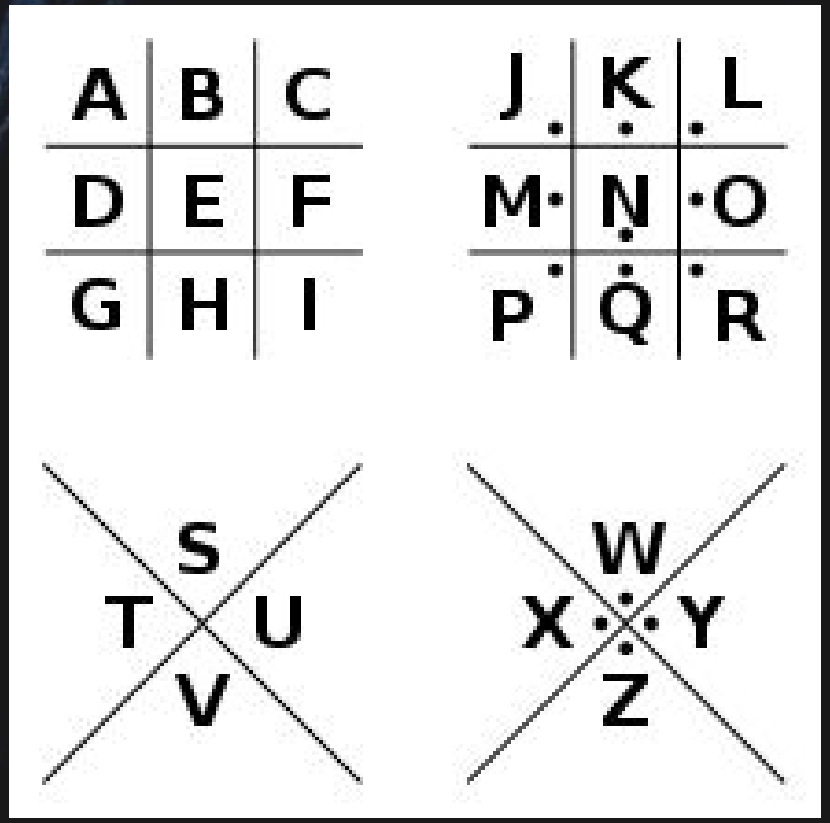
其它加密——BrainFuck

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

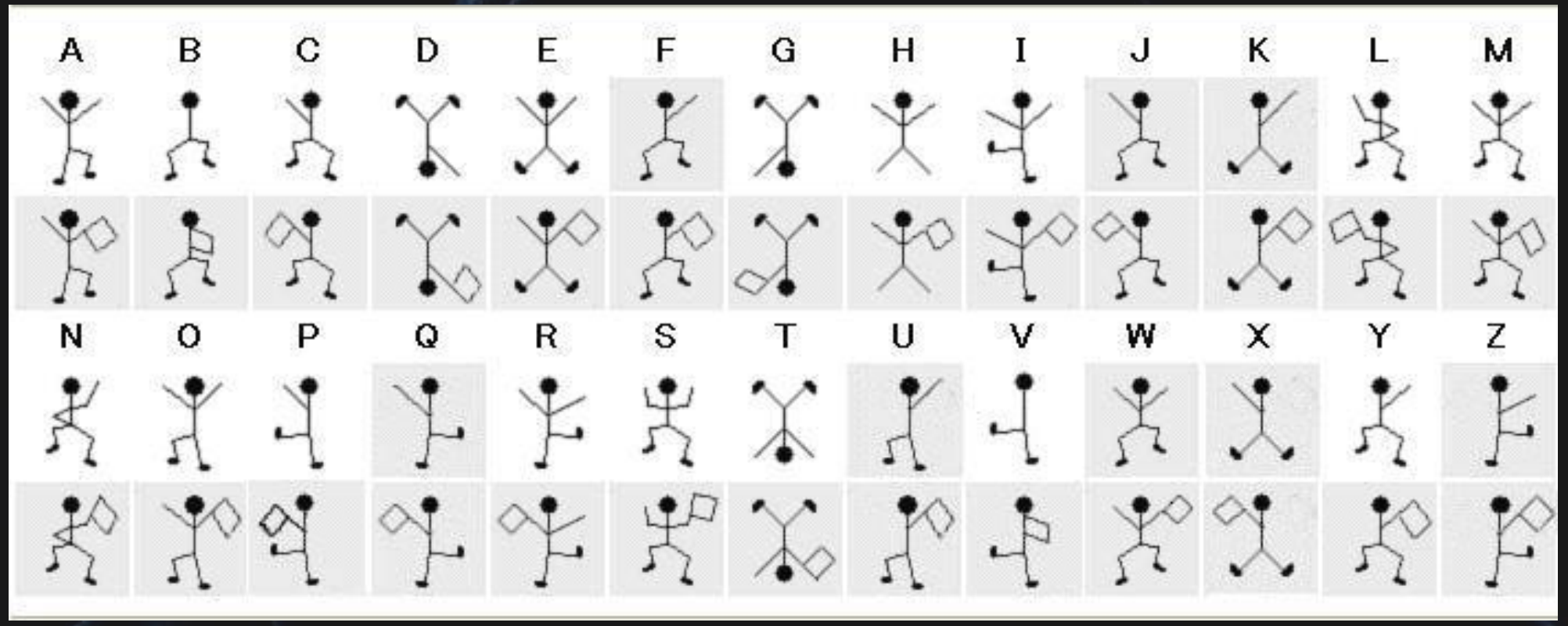
其它加密——JSFuck

```
[][(![]+[])[+[[+[]]]]+([][[]]+[])[+[[!+[]+!+[]+!+[]+!+[]+!+[]]]]+(![]+[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+(!![]+[])[+[[!+[]+!+[]
+!+[]]]]+(!![]+[])[+[[+!+[]]]]][([][(![]+[])[+[[+[]]]]+([][[]]+[])[+[[!+[]+!+[]+!+[]+!+[]+!+[]]]]+(![]+[])[+[[!+[]+!+[]]]]+(!![]+[])
[+[[+[]]]]+(!![]+[])[+[[!+[]+!+[]+!+[]]]]+(!![]+[])[+[[+!+[]]]]]+[])[+[[!+[]+!+[]+!+[]]]]+([][(![]+[])[+[[+[]]]]+([][[]]+[])[+[[!+[]
+!+[]+!+[]+!+[]+!+[]]]]+(![]+[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+(!![]+[])[+[[!+[]+!+[]+!+[]]]]+(!![]+[])[+[[+!+[]]]]]+[])[+[[!
+[]+!+[]+!+[]+!+[]+!+[]+!+[]]]]+([][[]]+[])[+[[+!+[]]]]+(![]+[])[+[[!+[]+!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+(!![]+[])[+[[+!+[]]]]+
([][[]]+[])[+[[+[]]]]+([][(![]+[])[+[[+[]]]]+([][[]]+[])[+[[!+[]+!+[]+!+[]+!+[]+!+[]]]]+(![]+[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+
(!![]+[])[+[[!+[]+!+[]+!+[]]]]+(!![]+[])[+[[+!+[]]]]]+[])[+[[!+[]+!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+([][(![]+[])[+[[+[]]]]+([][[]]+[])
[+[[!+[]+!+[]+!+[]+!+[]+!+[]]]]+(![]+[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+(!![]+[])[+[[!+[]+!+[]+!+[]]]]+(!![]+[])[+[[+!+[]]]]]
+[])[+[[!+[]+!+[]+!+[]+!+[]+!+[]+!+[]]]]+(!![]+[])[+[[+!+[]]]]]((![]+[])[+[[+!+[]]]]+(![]+[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[!+[]+!
+[]+!+[]]]]+(!![]+[])[+[[+!+[]]]]+(!![]+[])[+[[+[]]]]+([][(![]+[])[+[[+[]]]]+([][[]]+[])[+[[!+[]+!+[]+!+[]+!+[]+!+[]]]]+(![]+[])[+[[!
+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+(!![]+[])[+[[!+[]+!+[]+!+[]]]]+(!![]+[])[+[[+!+[]]]]]+[])[+[[+!+[]]]+[[!+[]+!+[]+!+[]+!+[]+!+[]]]]
+[+!+[]]+([][(![]+[])[+[[+[]]]]+([][[]]+[])[+[[!+[]+!+[]+!+[]+!+[]+!+[]]]]+(![]+[])[+[[!+[]+!+[]]]]+(!![]+[])[+[[+[]]]]+(!![]+[])[+
[[!+[]+!+[]+!+[]]]]+(!![]+[])[+[[+!+[]]]]]+[])[+[[+!+[]]]+[[!+[]+!+[]+!+[]+!+[]+!+[]+!+[]]]])()
```

其它加密——猪圈密码



其它加密——舞动的小人



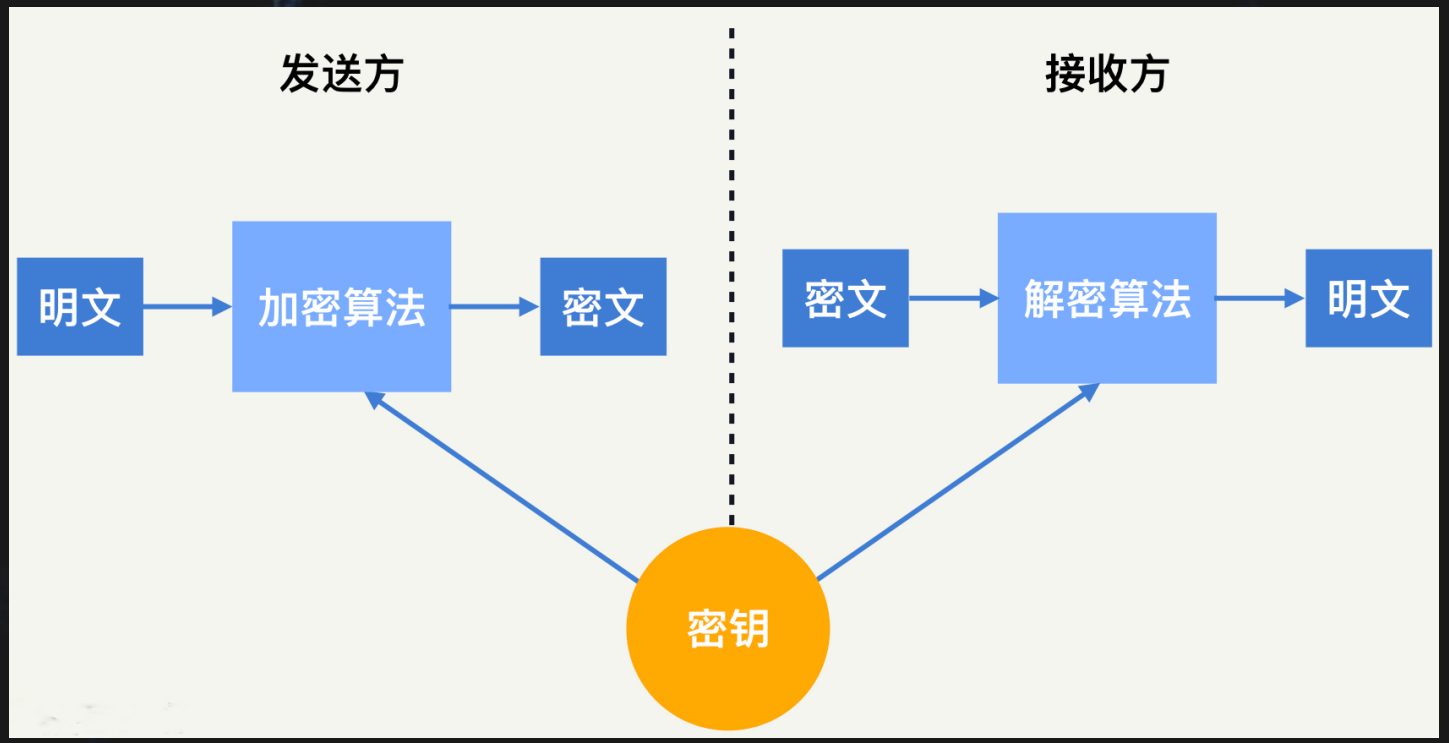
现代密码

现代密码

- 对称加密
  - 分组密码
- 非对称加密
  - 公钥密码
- 其它密码

对称加密算法

- 加密和解密使用的是同一个密钥

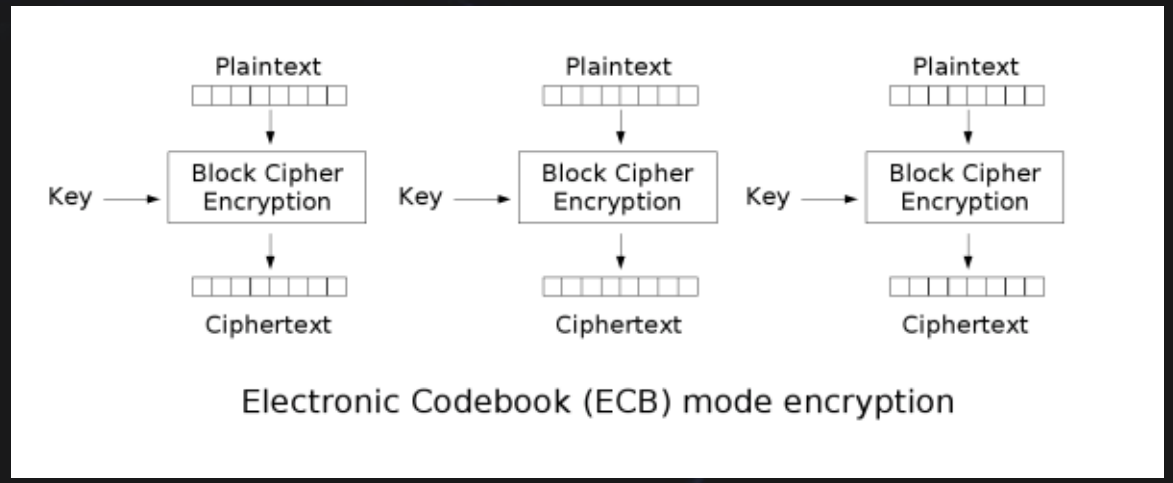


分组密码

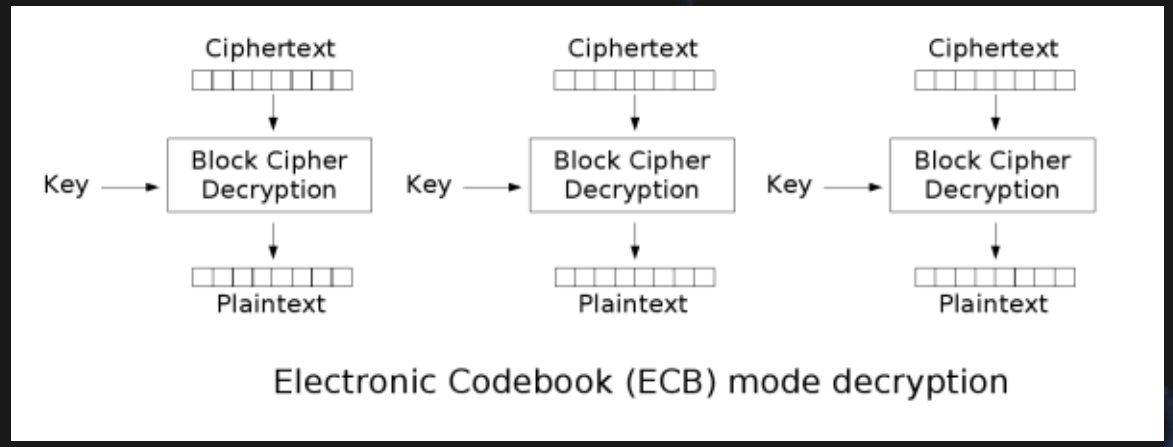
ECB

(Electronic Code Book)

电子密码本



Electronic Codebook (ECB) mode encryption



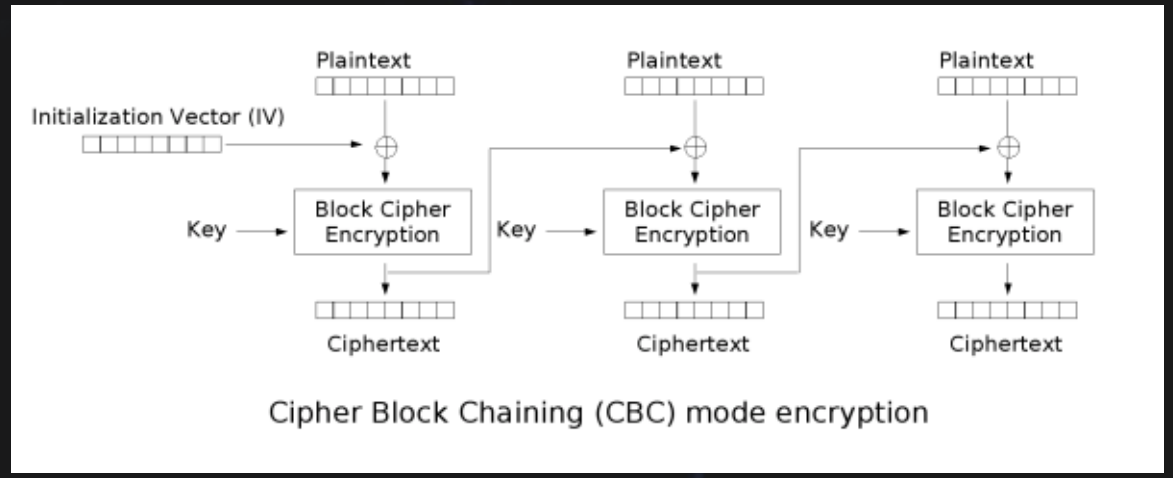
Electronic Codebook (ECB) mode decryption

分组密码

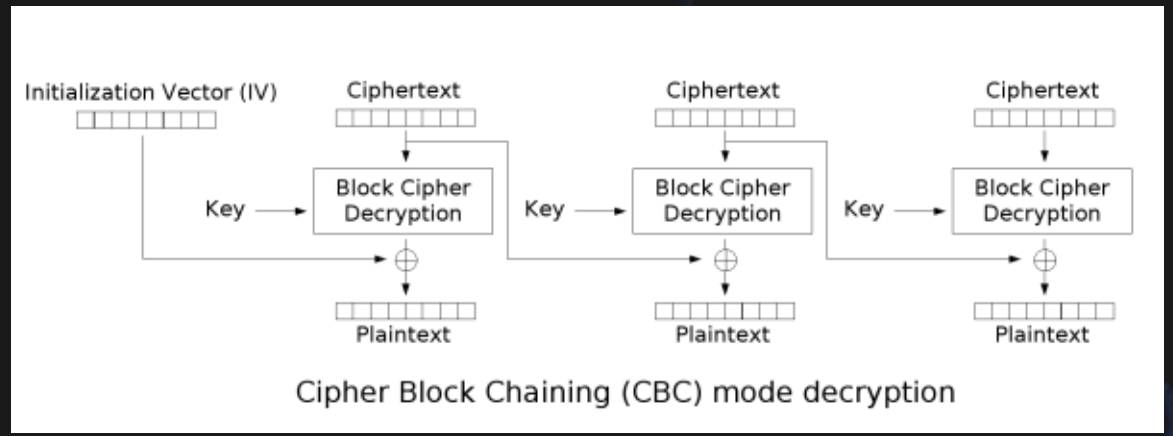
CBC

(Cipher Block Chaining)

密码分组链接



Cipher Block Chaining (CBC) mode encryption



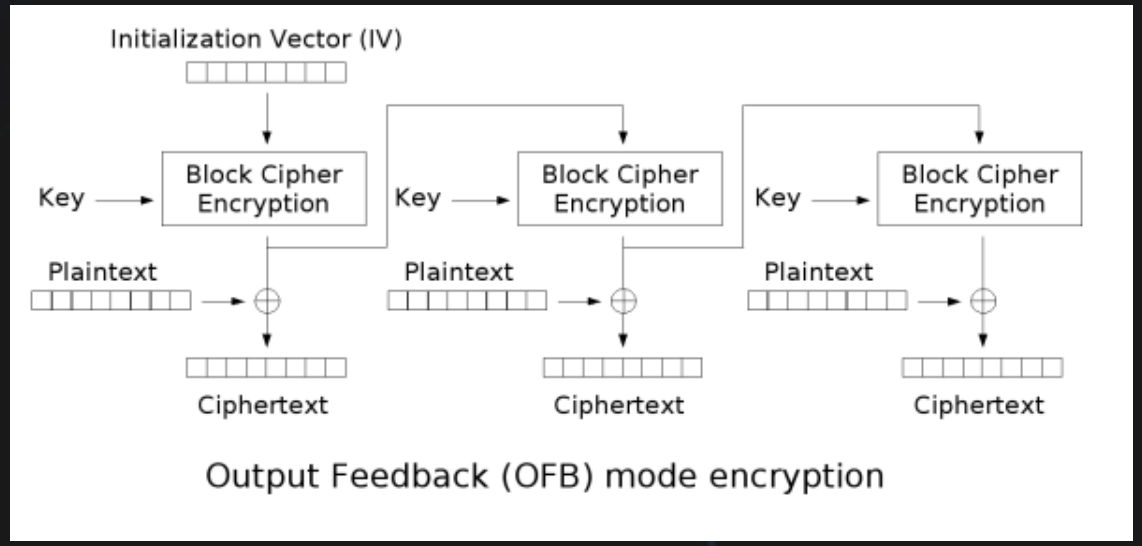
Cipher Block Chaining (CBC) mode decryption

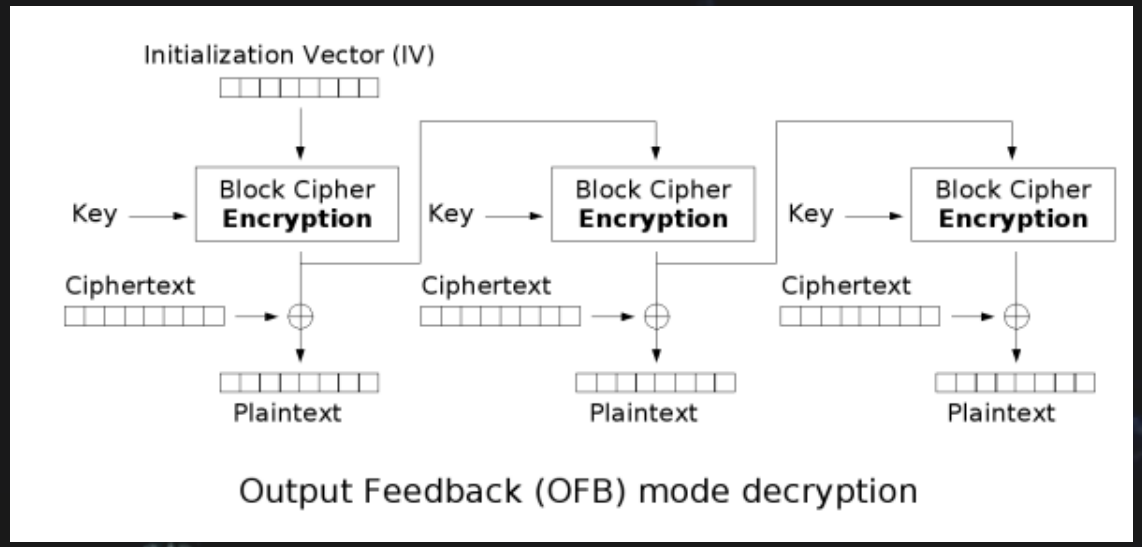
分组密码

OFB

(Output FeedBack)

输出反馈模式



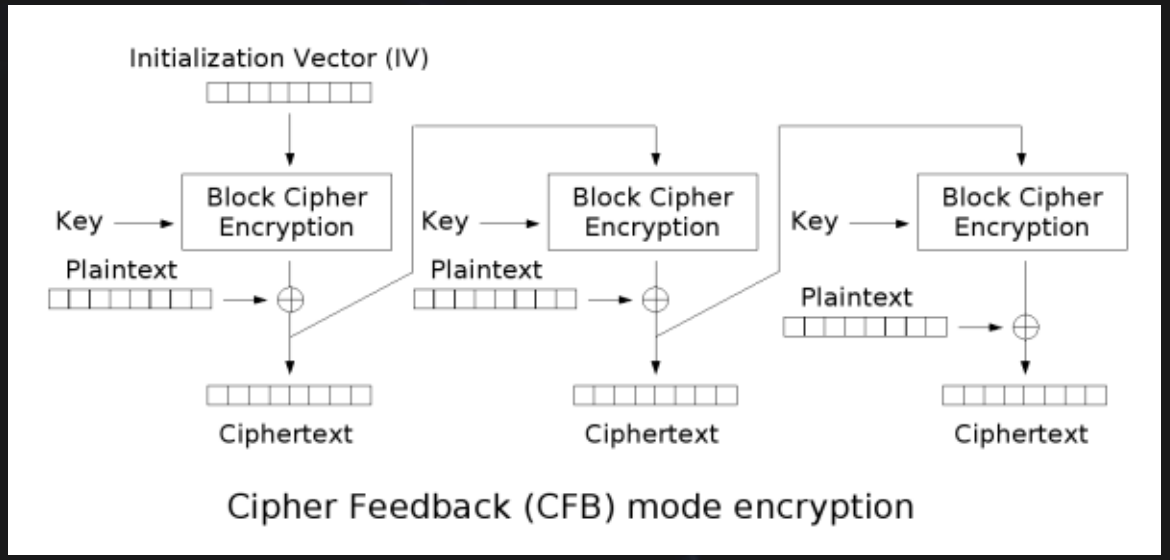


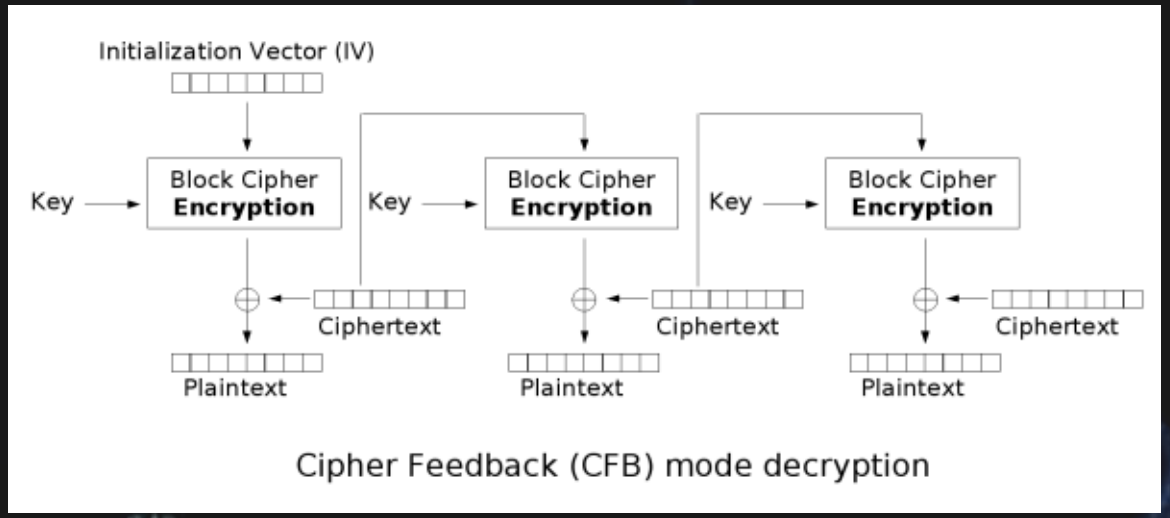
分组密码

CFB

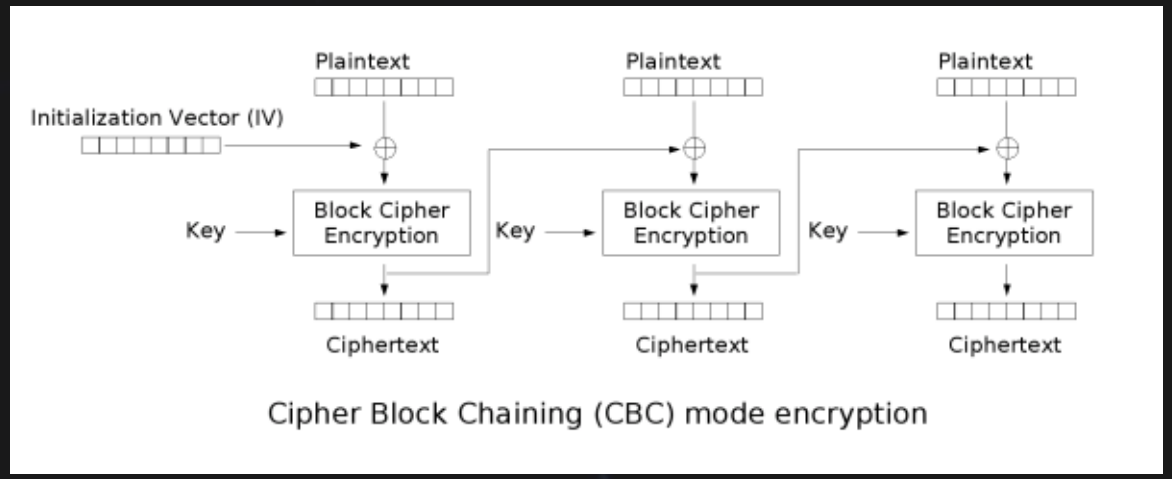
(Cipher FeedBack)

密文反馈





CBC模式下的攻击

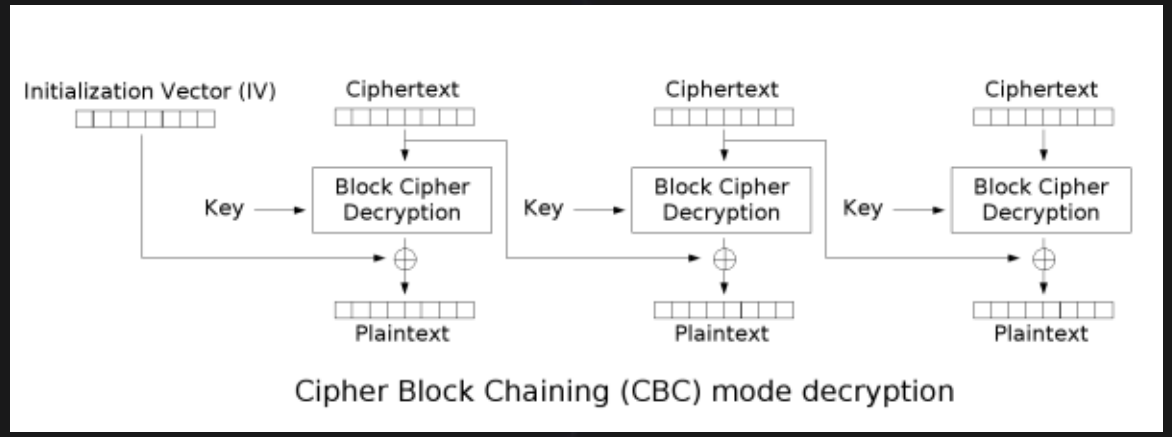


- Byte-at-a-Time
- 第一个块加密数据是明文异或IV后的数据，IV固定
- 第一块16字节：id + password；第二块16字节：cookie
- 减少id + password的字节数目，cookie的字节逐个比对、爆破

CBC模式下的攻击

- CBC-IV-Delection

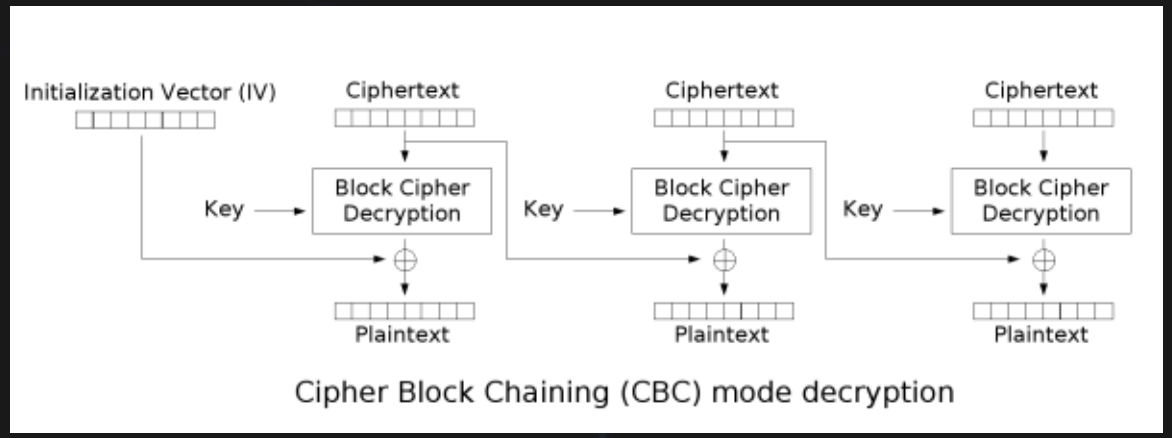
- $P_1=D(C_1)\oplus IV$
- $P_2=D(C_2)\oplus C_1$
- $P_3=D(C_3)\oplus C_2$



Cipher Block Chaining (CBC) mode decryption

- 若$C_1=C_3$，$C_2=0$，$P_3=D(C_1)$，$IV= P_1\oplus D(C_1)= P_1 \oplus P_3$

CBC模式下的攻击



- CBC-Bit-Flipping

- IV向量影响第一个明文分组、第n个密文分组可以影响第n + 1个明文分组

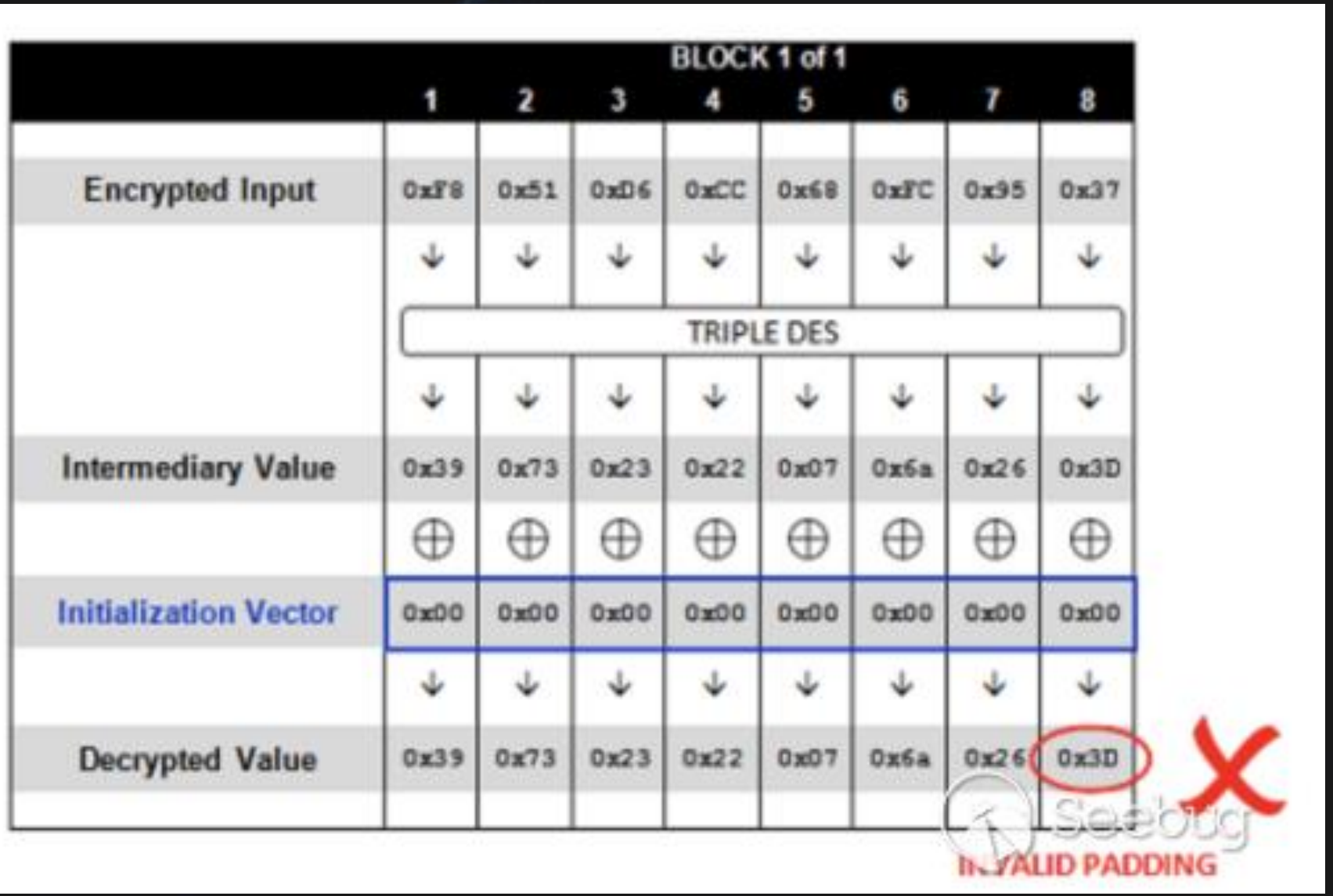
- 第n个密文分组为C_n，解密后的第n个明文分组为为P_n。
- $P_{n+1}=C_n$ xor $f(C_{n+1})$，$C_{n[new]}$改为C_n xor P_{n+1} xor A
- $P_{n+1[new]}$则变为C_n xor P_{n+1} xor A xor $f(C_{n+1})$ = A

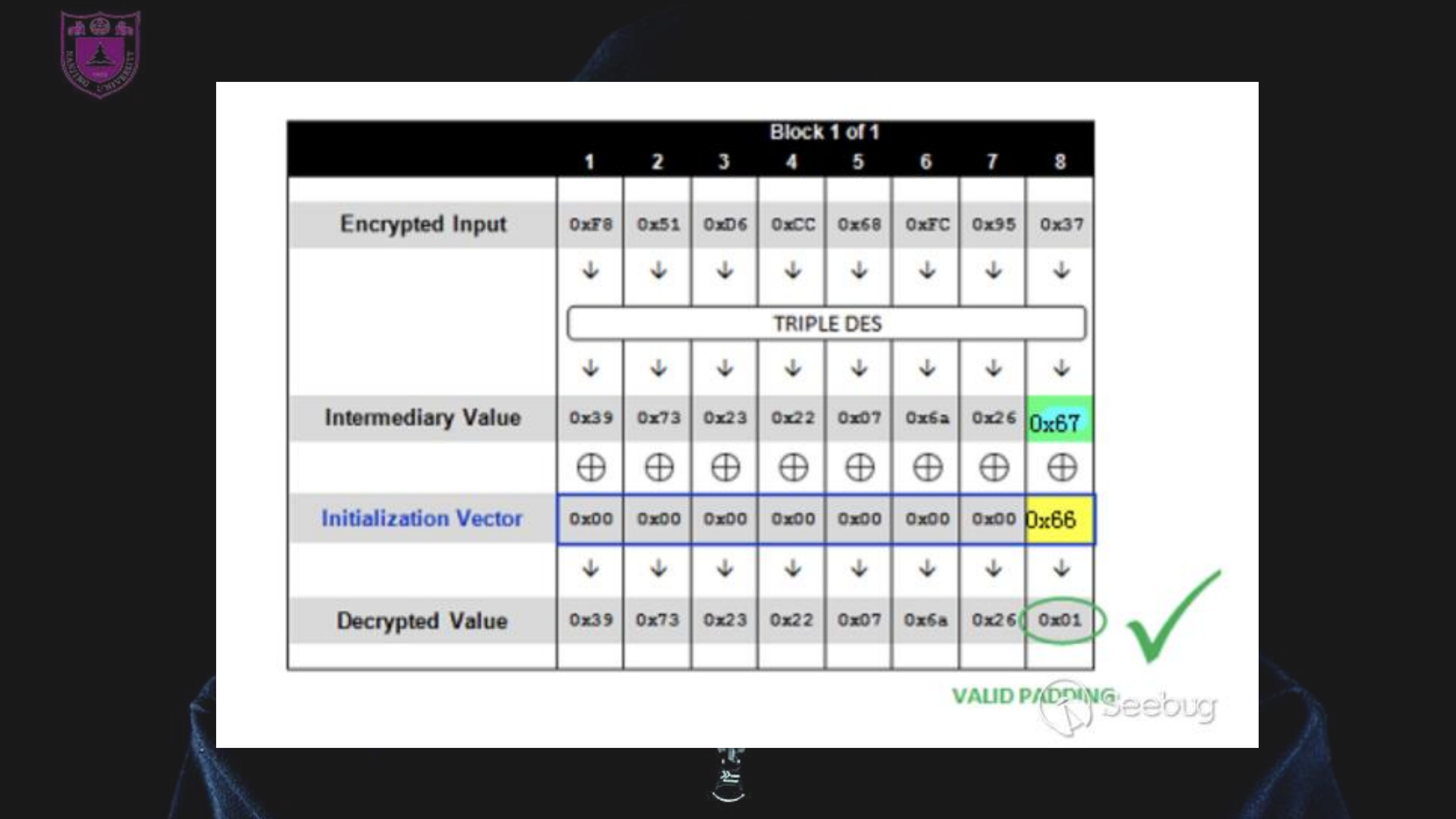
CBC模式下的攻击

- CBC-Padding-Oracle
- 可以控制IV
- 可以与服务器交互
  - 填充位正确、业务逻辑正确：200
  - 填充位正确、业务逻辑错误：300
  - 填充位错误、业务逻辑错误：500

	BLOCK #1								BLOCK #2							
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Ex 1	F	I	G													
Ex 1 (Padded)	F	I	G	0x05	0x05	0x05	0x05	0x05								
Ex 2	B	A	N	A	N	A										
Ex 2 (Padded)	B	A	N	A	N	A	0x02	0x02								
Ex 3	A	V	O	C	A	D	O									
Ex 3 (Padded)	A	V	O	C	A	D	O	0x01								
Ex 4	P	L	A	N	T	A	I	N								
Ex 4 (Padded)	P	L	A	N	T	A	I	N	0x08	0x08	0x08	0x08	0x08	0x08	0x08	0x08
Ex 5	P	A	S	S	I	O	N	F	R	U	I	T				
Ex 5 (Padded)	P	A	S	S	I	O	N	F	R	U	I	T	0x04	0x04	0x04	0x04


1 2 3 4 5 6 7 8
Encrypted Input
0xF0 0x51 0xD6 0xCC 0x60 0xFC 0x95 0x37
TRIPLE DES
Intermediary Value
0x39 0x73 0x23 0x22 0x07 0x6a 0x26 0x3D
Initialization Vector
0x6D 0x36 0x70 0x76 0x03 0x6E 0x22 0x39
Decrypted Value
? E S ? 0x04 0x04 0x04 0x04
我们输入的密文
加/解密算法 例如DES
计算的中间结果 这是只要的攻击需要的 我们给它一个名字 Intermediary Value
我们输入的初始化向量IV
解密的明文
Seebug


BLOCK 1 of 1
1 2 3 4 5 6 7 8
Encrypted Input
0xF8 0x51 0xD6 0xCC 0x68 0xFC 0x95 0x37
TRIPLE DES
Intermediary Value
0x39 0x73 0x23 0x22 0x07 0x6a 0x26 0x3D
Initialization Vector
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Decrypted Value
0x39 0x73 0x23 0x22 0x07 0x6a 0x26 0x3D
INVALID PADDING

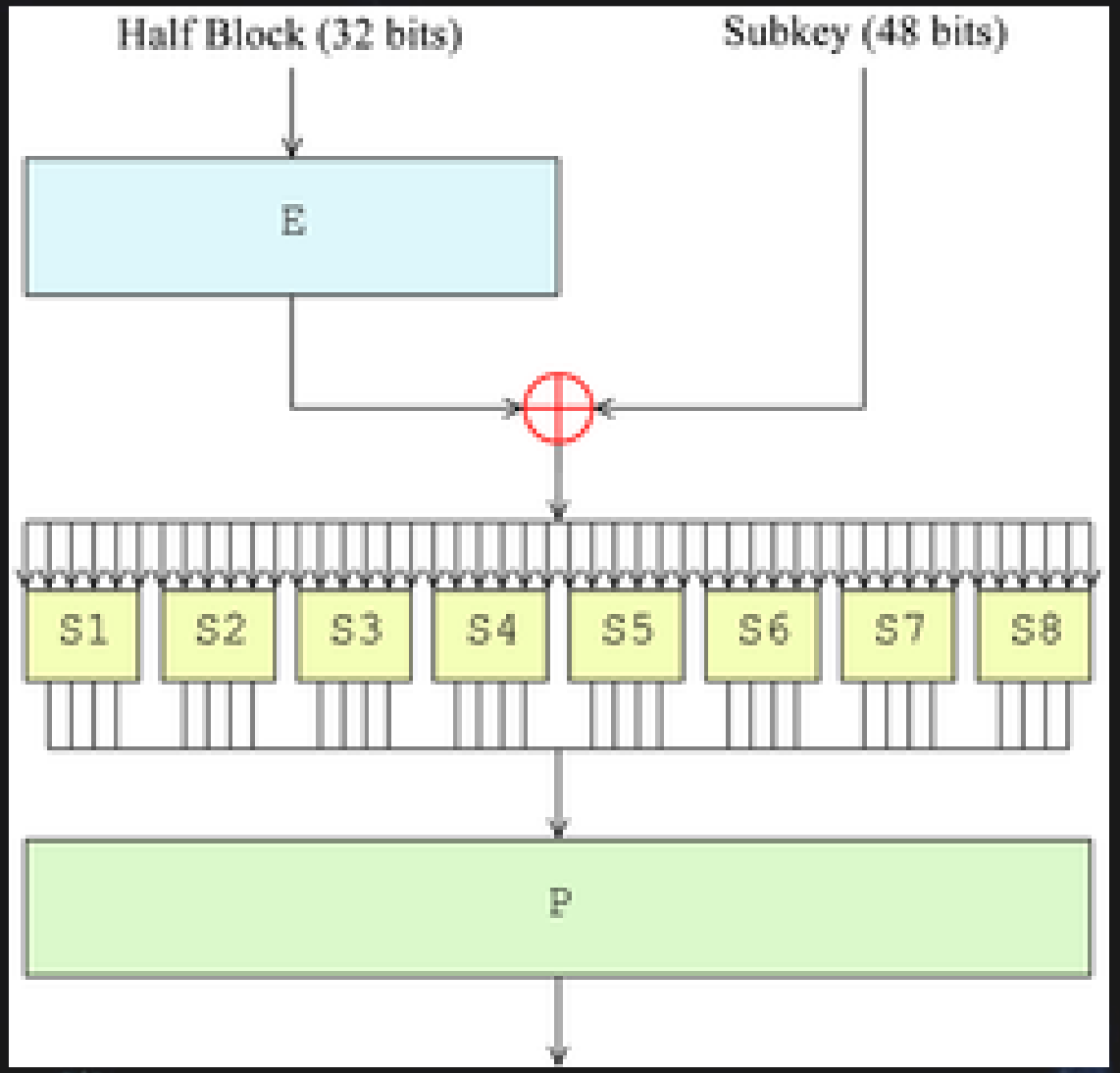

Block 1 of 1
1 2 3 4 5 6 7 8
Encrypted Input
0xF8 0x51 0xD6 0xCC 0x68 0xFC 0x95 0x37
TRIPLE DES
Intermediary Value
0x39 0x73 0x23 0x22 0x07 0x6a 0x26 0x67
Initialization Vector
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x66
Decrypted Value
0x39 0x73 0x23 0x22 0x07 0x6a 0x26 0x01
VALID PADDING
Seebug

分组密码——DES

输入置换

密钥置换

轮函数



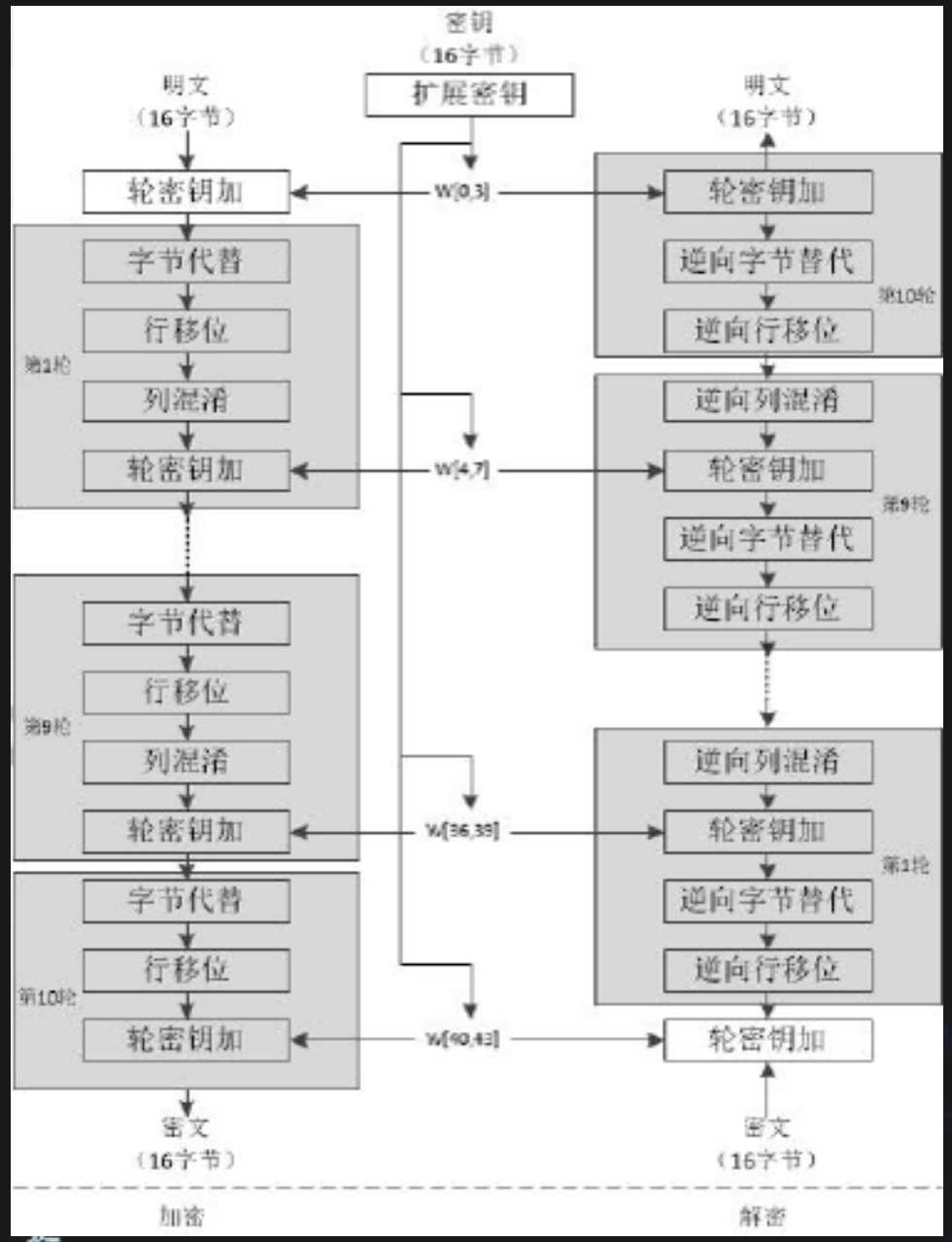
分组密码——AES

轮密钥加

字节代换

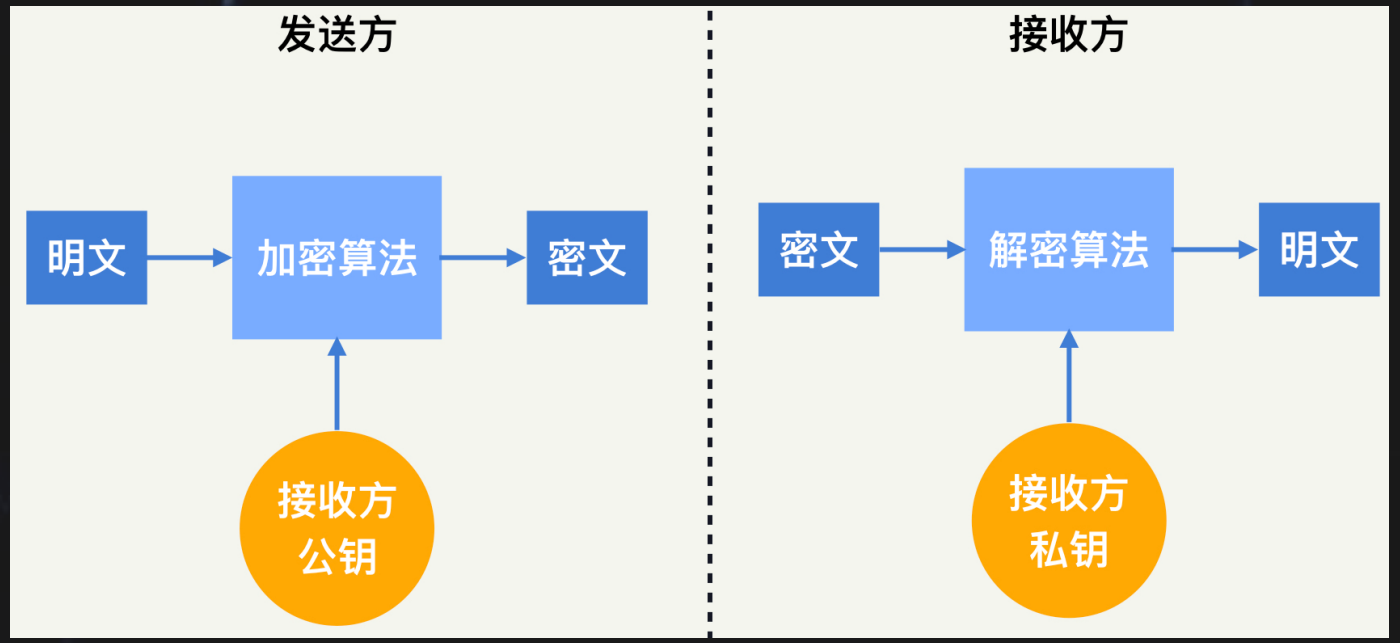
行移位

列混合



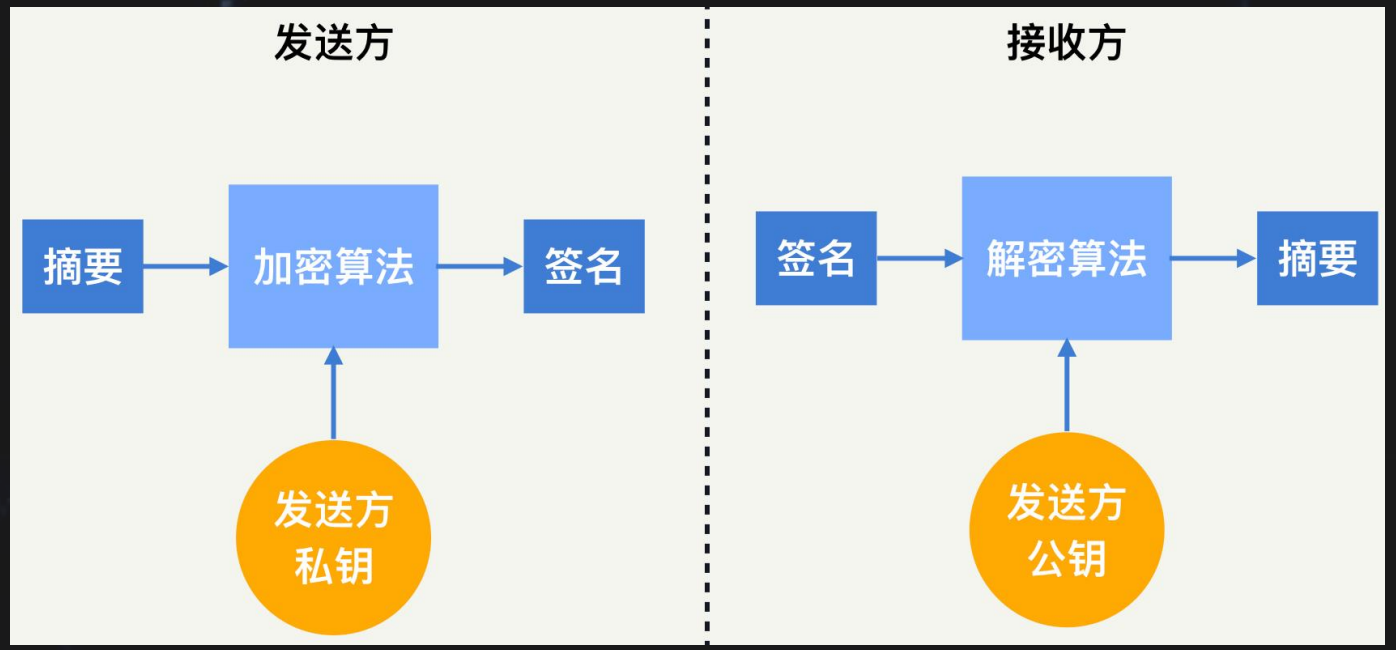
非对称加密算法

- 加密和解密使用不同的密钥
  - 公钥加密，私钥解密



非对称加密算法

- 大部分的非对称算法提供签名功能
  - 私钥加密，公钥解密



欧拉函数&欧拉定理

- 欧拉函数：
- Φ(m)表示1~m-1中与m互素的整数个数
- 特别的，若m是素数，则φ(m) = m – 1

- 欧拉定理：
- 若m>1，gcd(a,m) = 1
- 则$a^{\varphi(m)} = 1(\mathrm{mod}\ m)$

公钥密码——RSA

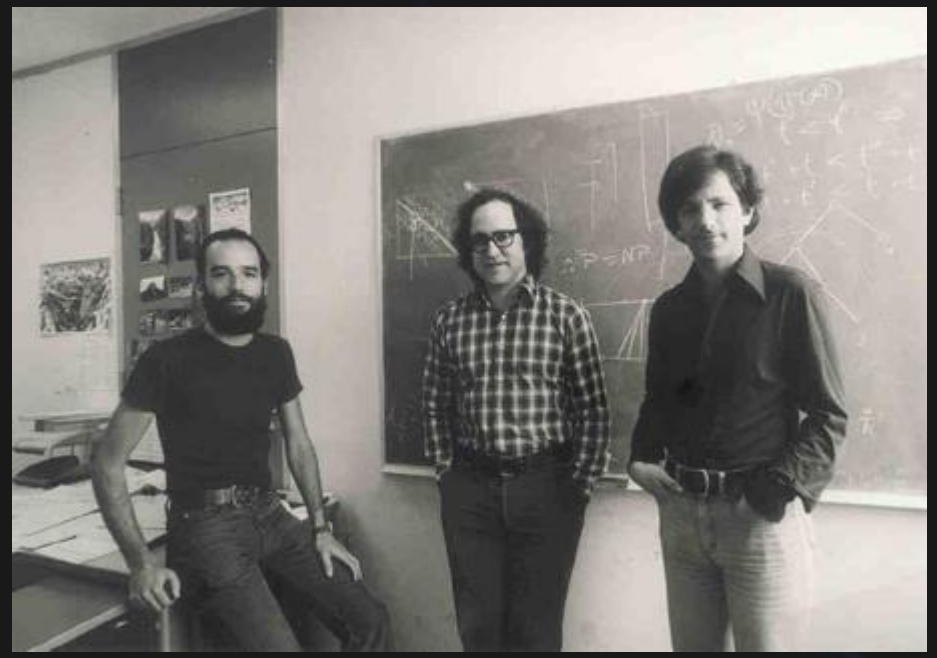
- 随机选择两个不同大质数p和q，计算N=p×q
- 根据欧拉函数，求得φ(N)=φ(p)φ(q)=(p−1)(q−1)
- 选择一个小于φ(N) 的整数 e，使e和φ(N)互质。并求得e关于φ(N)的模反元素，命名为 d，有ed≡1(modφ(N))
- 将p和q的记录销毁
- 此时，(N,e)是公钥，(N,d)是私钥。

公钥密码——RSA

- m表示明文，c表示密文：

- 消息加密：
- $c = m^e \bmod N$

- 消息解密：
- $m = c^d \bmod N$



公钥密码——RSA还能飞多久

Fast Factoring Integers by SVP Algorithms

Claus Peter Schnorr

Fachbereich Informatik und Mathematik,
Goethe-Universität Frankfurt, PSF 111932,
D-60054 Frankfurt am Main, Germany.
schnorr@cs.uni-frankfurt.de

Abstract. To factor an integer N we construct n triples of p_n-smooth integers $u, v, |u - vN|$ for the n-th prime p_n. Denote such triple a fac-relation. We get fac-relations from a nearly shortest vector of the lattice $\mathcal{L}(\mathbf{R}_{n,f})$ with basis matrix $\mathbf{R}_{n,f} \in \mathbb{R}^{(n+1)\times(n+1)}$ where $f : [1,n] \to [1,n]$ is a permutation of $[1,2,...,n]$ and $(Nf(1),...,Nf(n))$ is the diagonal of $\mathbf{R}_{n,f}$. We get an independent fac-relation from an independent permutation f'. We find sufficiently short lattice vectors by strong primal-dual reduction of $\mathbf{R}_{n,f}$. We factor $N \approx 2^{400}$ by n = 47 and $N \approx 2^{800}$ by n = 95. Our accelerated strong primal-dual reduction of [GN08] factors integers $N \approx 2^{400}$ and $N \approx 2^{800}$ by $4.2 \cdot 10^9$ and $8.4 \cdot 10^{10}$ arithmetic operations, much faster then the quadratic sieve **QS** and the number field sieve **NFS** and using much smaller primes p_n. This destroys the RSA cryptosystem.

Keywords. Primal-dual reduction, **SVP**, fac-relation.

RSA-共模攻击

- 如果使用相同的n，不同的模数e_1、e_2，且e_1、e_2互素，对同一组明文加密得到密文c_1、c_2

- $c_1 = m^{e1} \bmod n$
- $c_2 = m^{e2} \bmod n$

- 存在整数x和y，使得$xe_1 + ye_2 = 1$

- $c_1^x \times c_2^y \bmod n = m^{xe1} \times m^{ye2} \bmod n = m^1 \bmod n = m$

RSA-广播攻击

- 对于相同的明文m，使用相同的指数e和不同的模数n1、n2…ni，加密得到i组密文时，可以用中国剩余定理解出明文：
- $c_1=m^e \bmod n_1$， $c_2=m^e \bmod n_2$… $c_i=m^e \bmod n_i$联立得到：
- 可以求得一个c_x满足$c_i = m^e \bmod \Pi_1^j n_j$，其中$c_x$没有经过模操作

RSA可能用到的工具

- 因式分解：SageMath、Yafu
- 在线因子查询网站：factordb
- 计算公私密钥：Gmpy2Python库

其它密码

- MD5密码：
- Message-Digest Algorithm
- 输入：512 = 16 × 32
- 输出：128 = 4 × 32

- 只要改动极小的部分，就会使得md5 发生巨大的变化
- 不可逆

- SHA家族：
- Secure Hash Algorithm

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

课后作业

选做一

- 可选的课题：
  - ~~密码学发展的前世今生~~
  - 密码的攻击方式
  - 现代密码学的发展
  - 密码学的最新进展
  - ……
- 要求：
  - 独立完成，禁止抄袭
  - 提交报告，不少于1000字
  - 需要有2-3篇的论文支撑(最好是英文论文，这样你的分数会更高)
  - 截至时间：12月15前