第一章　古典密码学

张 磊

华东师范大学 • 软件学院

§1.1　几个简单的密码体制

基本术语

1. 密码学作为数学的一个分支, 是密码编码学和密码分析学的统称. 其中使消息保密的技术和科学叫做密码编码学, 而破译密文的科学和技术就是密码分析学.
2. 作为加密算法输入的原始信息称为明文, 常用小写字母表示; 明文经加密变换后的结果称为密文, 常用大写字母表示.
3. 密钥: 参与密码变换的参数, 通常用 K 表示.
4. 加密算法: 将明文变换为密文的变换函数, 相应的变换过程称为加密, 通常用 E 表示, 即

$$y = E_K(x).$$

5. 解密算法: 将密文恢复为明文的变换函数, 相应的变换过程称为解密, 通常用 D 表示, 即

$$x = D_K(y).$$

基本术语

1. 密码学作为数学的一个分支, 是密码编码学和密码分析学的统称. 其中使消息保密的技术和科学叫做密码编码学, 而破译密文的科学和技术就是密码分析学.
2. 作为加密算法输入的原始信息称为明文, 常用小写字母表示; 明文经加密变换后的结果称为密文, 常用大写字母表示.
3. 密钥: 参与密码变换的参数, 通常用 K 表示.
4. 加密算法: 将明文变换为密文的变换函数, 相应的变换过程称为加密, 通常用 E 表示, 即

$$y = E_K(x).$$

5. 解密算法: 将密文恢复为明文的变换函数, 相应的变换过程称为解密, 通常用 D 表示, 即

$$x = D_K(y).$$

基本术语

1. 密码学作为数学的一个分支, 是密码编码学和密码分析学的统称. 其中使消息保密的技术和科学叫做密码编码学, 而破译密文的科学和技术就是密码分析学.
2. 作为加密算法输入的原始信息称为明文, 常用小写字母表示; 明文经加密变换后的结果称为密文, 常用大写字母表示.
3. 密钥: 参与密码变换的参数, 通常用 K 表示.
4. 加密算法: 将明文变换为密文的变换函数, 相应的变换过程称为加密, 通常用 E 表示, 即

$$y = E_K(x).$$

5. 解密算法: 将密文恢复为明文的变换函数, 相应的变换过程称为解密, 通常用 D 表示, 即

$$x = D_K(y).$$

基本术语

1. 密码学作为数学的一个分支, 是密码编码学和密码分析学的统称. 其中使消息保密的技术和科学叫做密码编码学, 而破译密文的科学和技术就是密码分析学.
2. 作为加密算法输入的原始信息称为明文, 常用小写字母表示; 明文经加密变换后的结果称为密文, 常用大写字母表示.
3. 密钥: 参与密码变换的参数, 通常用 K 表示.
4. 加密算法: 将明文变换为密文的变换函数, 相应的变换过程称为加密, 通常用 E 表示, 即

$$y = E_K(x).$$

5. 解密算法: 将密文恢复为明文的变换函数, 相应的变换过程称为解密, 通常用 D 表示, 即

$$x = D_K(y).$$

基本术语

1. 密码学作为数学的一个分支, 是密码编码学和密码分析学的统称. 其中使消息保密的技术和科学叫做密码编码学, 而破译密文的科学和技术就是密码分析学.
2. 作为加密算法输入的原始信息称为明文, 常用小写字母表示; 明文经加密变换后的结果称为密文, 常用大写字母表示.
3. 密钥: 参与密码变换的参数, 通常用 K 表示.
4. 加密算法: 将明文变换为密文的变换函数, 相应的变换过程称为加密, 通常用 E 表示, 即

$$y = E_K(x).$$

5. 解密算法: 将密文恢复为明文的变换函数, 相应的变换过程称为解密, 通常用 D 表示, 即

$$x = D_K(y).$$

密码体制定义

一个密码体制是满足以下条件的五元组 $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$:

1. $\mathcal{P}$ 表示明文空间, 即由所有可能的明文组成的有限集.
2. $\mathcal{C}$ 表示密文空间, 即由所有可能的密文组成的有限集.
3. $\mathcal{K}$ 表示密钥空间, 即由所有可能的密钥组成的有限集.
4. 对每一个 $K \in \mathcal{K}$, 都存在一个加密规则 $E_K \in \mathcal{E}$ 和相应的解密规则 $D_K \in \mathcal{D}$, 使得对每一对

$$E_K : \mathcal{P} \to \mathcal{C}, \ D_K : \mathcal{C} \to \mathcal{P},$$

满足条件

$$D_K(E_K(x)) = x, \quad \forall\, x \in \mathcal{P}.$$

强调

1. 前面定义中, 最关键的是条件 4, 它保证了如果用 E_K 对明文 x 进行了加密的话, 则可使用相应的 D_K 对得到的密文进行解密, 从这可以看出加密函数 E_K 必须是一个单射函数.

强调

1. 前面定义中, 最关键的是条件 4, 它保证了如果用 E_K 对明文 x 进行了加密的话, 则可使用相应的 D_K 对得到的密文进行解密, 从这可以看出加密函数 E_K 必须是一个单射函数.
2. 如果 Alice 想发送消息串

$$\mathbf{x} = x_1 x_2 \cdots x_n$$

给 Bob, 则她需先对每一个消息 x_i 加密得到 $y_i = E_K(x_i)$, $1 \leq i \leq n$, 然后将密文串

$$\mathbf{y} = y_1 y_2 \cdots y_n$$

发送给 Bob.

强调

1. 前面定义中, 最关键的是条件 4, 它保证了如果用 E_K 对明文 x 进行了加密的话, 则可使用相应的 D_K 对得到的密文进行解密, 从这可以看出加密函数 E_K 必须是一个单射函数.
2. 如果 Alice 想发送消息串

$$\mathbf{x} = x_1 x_2 \cdots x_n$$

给 Bob, 则她需先对每一个消息 x_i 加密得到 $y_i = E_K(x_i)$, $1 \leq i \leq n$, 然后将密文串

$$\mathbf{y} = y_1 y_2 \cdots y_n$$

发送给 Bob.
3. 如果 $\mathcal{P} = \mathcal{C}$, 则加密函数 E_K 就是一个置换.

模同余

1. 假设 a 和 b 均为整数, m 是一正整数. 若 m 整除 $b-a$, 则可将其表示为

$$a \equiv b \pmod{m},$$

读作 a 与 b 模 m 同余, 正整数 m 称为模数.

模同余

1. 假设 a 和 b 均为整数, m 是一正整数. 若 m 整除 $b-a$, 则可将其表示为

$$a \equiv b \pmod{m},$$

读作 a 与 b 模 m 同余, 正整数 m 称为模数.

2. 若将 a 和 b 分别表示为

$$a = q_1 m + r_1, \quad b = q_2 m + r_2, \quad 0 \le r_1, r_2 \le m-1,$$

则有

$$a \equiv b \pmod{m} \Leftrightarrow r_1 = r_2.$$

模同余

1. 假设 a 和 b 均为整数, m 是一正整数. 若 m 整除 $b-a$, 则可将其表示为

$$a \equiv b \pmod{m},$$

读作 a 与 b 模 m 同余, 正整数 m 称为模数.

2. 若将 a 和 b 分别表示为

$$a = q_1 m + r_1, \quad b = q_2 m + r_2, \quad 0 \le r_1, r_2 \le m-1,$$

则有

$$a \equiv b \pmod{m} \Leftrightarrow r_1 = r_2.$$

3. $a \bmod m$: a 除以 m 的余数, 即上面中的 r_1.

模运算

令

$$\mathbb{Z}_m = \{0, 1, 2, \cdots, m-1\},$$

在其上定义加法 $\oplus$ 和乘法 $\otimes$ 如下: $\forall\ a, b \in \mathbb{Z}_m$,

$$\begin{cases} a \oplus b \stackrel{\triangle}{=} (a + b) \bmod m, \\ a \otimes b \stackrel{\triangle}{=} (a \times b) \bmod m. \end{cases}$$

说明

1. 上面定义 $\mathbb{Z}_m$ 上的加法和乘法运算其实与普通整数上的加法和乘法相类似, 只是所得的值是取模以后的余数.

说明

1. 上面定义 $\mathbb{Z}_m$ 上的加法和乘法运算其实与普通整数上的加法和乘法相类似, 只是所得的值是取模以后的余数.
2. 上面定义的加法和乘法运算满足许多性质, 使得 $(\mathbb{Z}_m, \oplus)$ 构成一个群, $(\mathbb{Z}_m, \oplus, \otimes)$ 构成一个环.

说明

1. 上面定义 $\mathbb{Z}_m$ 上的加法和乘法运算其实与普通整数上的加法和乘法相类似, 只是所得的值是取模以后的余数.
2. 上面定义的加法和乘法运算满足许多性质, 使得 $(\mathbb{Z}_m, \oplus)$ 构成一个群, $(\mathbb{Z}_m, \oplus, \otimes)$ 构成一个环.
3. 在不引起混淆的情况下, $\mathbb{Z}_m$ 上的这两种运算也记作 $+$ 和 $\times$. 另外, 在 $\mathbb{Z}_m$ 上我们可以定义减法为

$$a \ominus b \stackrel{\triangle}{=} (a - b) \bmod m.$$

群论导引

一个非空集合 G 关于一个二元运算 (通常叫做乘法) 称为群, 如果

1. 结合律成立, 即对于 G 中任意三个元素 a, b, c, 有

$$a(bc) = (ab)c;$$

2. G 中包含一个单位元 1, 对于 G 中每个元素 a, 有

$$1a = a1 = a;$$

3. 对于 G 中每个元素 a, 在 G 中存在逆元 a^{-1}, 使

$$aa^{-1} = a^{-1}a = 1.$$

群论导引

一个非空集合 G 关于一个二元运算 (通常叫做乘法) 称为群, 如果

1. 结合律成立, 即对于 G 中任意三个元素 a, b, c, 有

$$a(bc) = (ab)c;$$

2. G 中包含一个单位元 1, 对于 G 中每个元素 a, 有

$$1a = a1 = a;$$

3. 对于 G 中每个元素 a, 在 G 中存在逆元 a^{-1}, 使

$$aa^{-1} = a^{-1}a = 1.$$

可以验证, 集合 $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ 关于数的乘法构成群.

移位密码 (Shift Cipher)

令 $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. 对任意 $0 \leq K \leq 25$, 定义

$$E_K(x) = (x + K) \bmod 26$$

和

$$D_K(y) = (y - K) \bmod 26.$$

移位密码 (Shift Cipher)

令 $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. 对任意 $0 \leq K \leq 25$, 定义

$$E_K(x) = (x + K) \bmod 26$$

和

$$D_K(y) = (y - K) \bmod 26.$$

若取 $K = 3$, 则上述移位密码体制通常叫作恺撒密码 (Caesar Cipher).

英文字母的编码和解码

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

Examp-1-1-1

试用移位密码加密下列明文

we will meet at midnight.

这里假设密钥为 $K = 11$.

Examp-1-1-1

试用移位密码加密下列明文

we will meet at midnight.

这里假设密钥为 $K = 11$.

密文为: HPHT WWXP PELE XTOY TRSE

加密体制必须满足的条件

1. 加密函数 E_K 和解密函数 D_K 都应该易于计算;

加密体制必须满足的条件

1. 加密函数 E_K 和解密函数 D_K 都应该易于计算;
2. 对任何敌手来说, 即使他获得了密文 y, 也不可能由此确定出密钥 K 或者明文 x;

加密体制必须满足的条件

1. 加密函数 E_K 和解密函数 D_K 都应该易于计算;
2. 对任何敌手来说, 即使他获得了密文 y, 也不可能由此确定出密钥 K 或者明文 x;
3. 特别的, 必须能够抵抗穷尽密钥搜索攻击.

Examp-1-1-2

试用穷尽密钥搜索方法破译如下利用移位密码加密的密文

PHHW PH DIWHU WKH WRJD SDUWB

密钥穷尽搜索

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

代换密码 (Substitution Cipher)

令 $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, $\mathcal{K}$ 是由 26 个数字 $0, 1, \cdots, 25$ 的所有可能的置换组成. 对任意的置换 $\pi \in \mathcal{K}$, 定义

$$E_\pi(x) = \pi(x)$$

和

$$D_\pi(y) = \pi^{-1}(y),$$

这里 π^{-1} 表示置换 π 的逆置换.

代换密码 (Substitution Cipher)

令 $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, $\mathcal{K}$ 是由 26 个数字 $0, 1, \cdots, 25$ 的所有可能的置换组成. 对任意的置换 $\pi \in \mathcal{K}$, 定义

$$E_\pi(x) = \pi(x)$$

和

$$D_\pi(y) = \pi^{-1}(y),$$

这里 π^{-1} 表示置换 π 的逆置换.

置换和逆置换

1. 有限集上 X 上的一个置换是一个双射函数 $\pi: X \to X$, 比如 $X = \{1, 2, 3, 4, 5, 6\}$, 以下定义了 X 上的两个置换 π_1, π_2:

x	1	2	3	4	5	6
π_1	3	5	1	6	4	2

x	1	2	3	4	5	6
π_2	6	4	3	2	5	1

代换密码 (Substitution Cipher)

令 $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, $\mathcal{K}$ 是由 26 个数字 $0, 1, \cdots, 25$ 的所有可能的置换组成. 对任意的置换 $\pi \in \mathcal{K}$, 定义

$$E_\pi(x) = \pi(x)$$

和

$$D_\pi(y) = \pi^{-1}(y),$$

这里 π^{-1} 表示置换 π 的逆置换.

置换和逆置换

1. 有限集上 X 上的一个置换是一个双射函数 $\pi: X \to X$, 比如 $X = \{1, 2, 3, 4, 5, 6\}$, 以下定义了 X 上的两个置换 π_1, π_2:

x	1	2	3	4	5	6
π_1	3	5	1	6	4	2

x	1	2	3	4	5	6
π_2	6	4	3	2	5	1

2. 置换 π 的逆置换 π^{-1} 定义为: $\pi^{-1}(x) = x' \iff \pi(x') = x$.

安全性说明

1. 代换密码的密钥空间大小是 $26! > 4.0 \times 10^{26}$, 是一个很大的数. 因此采用穷尽密钥搜索的攻击方法, 即使是使用计算机, 也是计算上不可行的.

安全性说明

1. 代换密码的密钥空间大小是 $26! > 4.0 \times 10^{26}$, 是一个很大的数. 因此采用穷尽密钥搜索的攻击方法, 即使是使用计算机, 也是计算上不可行的.
2. 但是, 采用其它的密码分析方法, 代换密码可以很容易地被攻破.

Examp-1-1-3

试用代换密码加密下列明文

we will meet at midnight,

这里假设 π 是定义在 $\mathbb{Z}_{26}$ 上的如下置换:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\pi(x)$	23	13	24	0	7	15	14	6	25	16	22	1	19

x	13	14	15	16	17	18	19	20	21	22	23	24	25
$\pi(x)$	18	5	11	17	2	21	12	20	4	10	9	3	8

Examp-1-1-3

试用代换密码加密下列明文

we will meet at midnight,

这里假设 π 是定义在 $\mathbb{Z}_{26}$ 上的如下置换:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\pi(x)$	23	13	24	0	7	15	14	6	25	16	22	1	19

x	13	14	15	16	17	18	19	20	21	22	23	24	25
$\pi(x)$	18	5	11	17	2	21	12	20	4	10	9	3	8

密文为: KHKZ BBTH HMXM TZAS ZOGM

置换的逆和简化表示

上题中置换 π 的逆置换 π^{-1} 为:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\pi^{-1}(x)$	3	11	17	24	21	14	7	4	25	23	22	15	19

x	13	14	15	16	17	18	19	20	21	22	23	24	25
$\pi^{-1}(x)$	1	6	5	9	16	13	12	20	18	10	0	2	8

置换的逆和简化表示

上题中置换 π 的逆置换 π^{-1} 为:

x	0	1	2	3	4	5	6	7	8	9	10	11	12
$\pi^{-1}(x)$	3	11	17	24	21	14	7	4	25	23	22	15	19

x	13	14	15	16	17	18	19	20	21	22	23	24	25
$\pi^{-1}(x)$	1	6	5	9	16	13	12	20	18	10	0	2	8

π^{-1} 和 π 也可分别表示为

$\pi^{-1} =$

3	11	17	24	21	14	7	4	25	23	22	15	19
1	6	5	9	16	13	12	20	18	10	0	2	8

$\pi =$

23	13	24	0	7	15	14	6	25	16	22	1	19
18	5	11	17	2	21	12	20	4	10	9	3	8

同余方程唯一解定理

设 $a \in \mathbb{Z}_m$, 对任意的 $b \in \mathbb{Z}_m$, 同余方程

$$ax \equiv b \pmod{m}$$

有唯一解 $x \in \mathbb{Z}_m$ 的充分必要条件是

$$\gcd(a, m) = 1.$$

欧拉函数和欧拉定理

设 $a \geq 1, m \geq 2$. 如果 $\gcd(a, m) = 1$, 则称 a 与 m 互素. $\mathbb{Z}_m$ 中所有与 m 互素元素个数用 $\phi(m)$ 来表示 (函数 ϕ 也称为欧拉函数).

欧拉函数和欧拉定理

设 $a \geq 1, m \geq 2$. 如果 $\gcd(a, m) = 1$, 则称 a 与 m 互素. $\mathbb{Z}_m$ 中所有与 m 互素元素个数用 $\phi(m)$ 来表示 (函数 ϕ 也称为欧拉函数).

欧拉定理

假定

$$m = \prod_{i=1}^{n} p_i^{e_i},$$

这里 p_i 均为素数且互不相同, $e_i > 0, 1 \leq i \leq n$. 则有

$$\phi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i - 1}).$$

乘法逆定义和性质

1. 设 $a \in \mathbb{Z}_m$, 若存在 $a' \in \mathbb{Z}_m$, 使得

$$aa' \equiv 1 \pmod{m},$$

则称 a 模 m 可逆, a' 为 a 的 (乘法) 逆元. a' 可记为 $a^{-1} \bmod m$, 在 m 固定的情形下, 简记为 a^{-1}.

乘法逆定义和性质

1. 设 $a \in \mathbb{Z}_m$, 若存在 $a' \in \mathbb{Z}_m$, 使得

$$aa' \equiv 1 \pmod{m},$$

则称 a 模 m 可逆, a' 为 a 的 (乘法) 逆元. a' 可记为 $a^{-1} \bmod m$, 在 m 固定的情形下, 简记为 a^{-1}.

2. a 模 m 可逆, 当且仅当 $\gcd(a, m) = 1$.

乘法逆定义和性质

1. 设 $a \in \mathbb{Z}_m$, 若存在 $a' \in \mathbb{Z}_m$, 使得

$$aa' \equiv 1 \pmod{m},$$

则称 a 模 m 可逆, a' 为 a 的 (乘法) 逆元. a' 可记为 $a^{-1} \bmod m$, 在 m 固定的情形下, 简记为 a^{-1}.

2. a 模 m 可逆, 当且仅当 $\gcd(a, m) = 1$.
3. 如果 p 为素数, 则 $\mathbb{Z}_p$ 上任一非零元素均可逆.

乘法逆定义和性质

1. 设 $a \in \mathbb{Z}_m$, 若存在 $a' \in \mathbb{Z}_m$, 使得

$$aa' \equiv 1 \pmod{m},$$

则称 a 模 m 可逆, a' 为 a 的 (乘法) 逆元. a' 可记为 $a^{-1} \bmod m$, 在 m 固定的情形下, 简记为 a^{-1}.

2. a 模 m 可逆, 当且仅当 $\gcd(a, m) = 1$.
3. 如果 p 为素数, 则 $\mathbb{Z}_p$ 上任一非零元素均可逆.
4. 如果 $\gcd(a, m) = 1$, 则同余方程

$$ax \equiv b \pmod{m}$$

在 $\mathbb{Z}_m$ 内有唯一解

$$x = (a^{-1}b) \bmod m.$$

仿射密码 (Affine Cipher)

令 $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, 且

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\}.$$

对任意的 $K = (a, b) \in \mathcal{K}$, 定义

$$E_K(x) = (ax + b) \bmod 26$$

和

$$D_K(y) = a^{-1}(y - b) \bmod 26.$$

仿射密码 (Affine Cipher)

令 $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, 且

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\}.$$

对任意的 $K = (a, b) \in \mathcal{K}$, 定义

$$E_K(x) = (ax + b) \bmod 26$$

和

$$D_K(y) = a^{-1}(y - b) \bmod 26.$$

密钥空间

因为满足条件 $\gcd(a, 26) = 1$ 的 a 个数为欧拉数 $\phi(26) = 12$, b 可以取 $\mathbb{Z}_{26}$ 中的任何数, 所以仿射密码的密钥空间大小为

$$12 \times 26 = 312.$$

故很不安全.

Examp-1-1-4

假设密钥 $K = (7, 3)$, 试用仿射密码体制加密单词 hot, 并对得到的密文进行解密.

Examp-1-1-4

假设密钥 $K = (7, 3)$, 试用仿射密码体制加密单词 hot, 并对得到的密文进行解密.

明文	h	o	t

Examp-1-1-4

假设密钥 $K = (7, 3)$, 试用仿射密码体制加密单词 hot, 并对得到的密文进行解密.

明文	h	o	t
编码	7	14	19

Examp-1-1-4

假设密钥 $K = (7, 3)$, 试用仿射密码体制加密单词 hot, 并对得到的密文进行解密.

明文	h	o	t
编码	7	14	19
加密	0	23	6

Examp-1-1-4

假设密钥 $K = (7, 3)$, 试用仿射密码体制加密单词 hot, 并对得到的密文进行解密.

明文	h	o	t
编码	7	14	19
加密	0	23	6
解码	A	X	G

维吉尼亚密码 (Vigenère Cipher)

设 m 是一个正整数. 定义 $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$. 对任意的密钥 $K = (k_1, k_2, \cdots, k_m)$, 定义

$$E_K(x_1, x_2, \cdots, x_m) = (x_1 + k_1, x_2 + k_2, \cdots, x_m + k_m)$$

和

$$D_K(y_1, y_2, \cdots, y_m) = (y_1 - k_1, y_2 - k_2, \cdots, y_m - k_m),$$

以上所有的运算都是在 $\mathbb{Z}_{26}$ 上进行.

维吉尼亚密码 (Vigenère Cipher)

设 m 是一个正整数. 定义 $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$. 对任意的密钥 $K = (k_1, k_2, \cdots, k_m)$, 定义

$$E_K(x_1, x_2, \cdots, x_m) = (x_1 + k_1, x_2 + k_2, \cdots, x_m + k_m)$$

和

$$D_K(y_1, y_2, \cdots, y_m) = (y_1 - k_1, y_2 - k_2, \cdots, y_m - k_m),$$

以上所有的运算都是在 $\mathbb{Z}_{26}$ 上进行.

说明

1. 密钥空间为 26^m, 当 $m = 5$ 时, $26^5 > 1.1 \times 10^7$, 已经超出了使用手算进行密钥空间搜索的能力范围;

维吉尼亚密码 (Vigenère Cipher)

设 m 是一个正整数. 定义 $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$. 对任意的密钥 $K = (k_1, k_2, \cdots, k_m)$, 定义

$$E_K(x_1, x_2, \cdots, x_m) = (x_1 + k_1, x_2 + k_2, \cdots, x_m + k_m)$$

和

$$D_K(y_1, y_2, \cdots, y_m) = (y_1 - k_1, y_2 - k_2, \cdots, y_m - k_m),$$

以上所有的运算都是在 $\mathbb{Z}_{26}$ 上进行.

说明

1. 密钥空间为 26^m, 当 $m = 5$ 时, $26^5 > 1.1 \times 10^7$, 已经超出了使用手算进行密钥空间搜索的能力范围;
2. 在一个密钥字长度为 m 的维吉尼亚密码中, 一个字母最多可以被映射成为 m 个不同的字母, 这样的密码体制称为多表代换密码体制. 它一般被认为比单表密码体制更为安全.

Examp-1-1-5

试用维吉尼亚密码加密明文串:

encode and decode,

这里密钥字为: mykey.

Examp-1-1-5

试用维吉尼亚密码加密明文串:

encode and decode,

这里密钥字为: mykey.

字母序号		e	n	c	o	d	e	a	n	d	d	e	c	o	d	e
明文编码	P =	4	13	2	14	3	4	0	13	3	3	4	2	14	3	4
密钥编码	k =	12	24	10	4	24	12	24	10	4	24	12	24	10	4	24
加密	C =	16	37	12	18	27	16	24	23	7	27	16	26	24	7	28
模运算			11			1					1		0			2
密文	C =	Q	L	M	S	B	Q	Y	X	H	B	Q	A	Y	H	C

1. 设矩阵 $A = (a_{ij})_{l\times m}$, $B = (b_{jk})_{m\times n}$, 它们的乘法定义为 $AB = (c_{ik})_{l\times n}$, 这里

$$c_{ik} = \sum_{j=1}^{m} a_{ij} b_{jk}.$$

补充线性代数知识

1. 设矩阵 $A = (a_{ij})_{l\times m}$, $B = (b_{jk})_{m\times n}$, 它们的乘法定义为 $AB = (c_{ik})_{l\times n}$, 这里

$$c_{ik} = \sum_{j=1}^{m} a_{ij} b_{jk}.$$

2. m 阶单位矩阵 (记为 I_m) 定义为: 主对角线元素的值为 1, 其余元素全为 0. 比如 $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

补充线性代数知识

1. 设矩阵 $A = (a_{ij})_{l\times m}$, $B = (b_{jk})_{m\times n}$, 它们的乘法定义为 $AB = (c_{ik})_{l\times n}$, 这里

$$c_{ik} = \sum_{j=1}^{m} a_{ij} b_{jk}.$$

2. m 阶单位矩阵 (记为 I_m) 定义为: 主对角线元素的值为 1, 其余元素全为 0. 比如 $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

3. 逆矩阵: 如果存在 m 阶方阵 B, 使得 $AB = BA = I_m$, 则称矩阵 A 可逆, 并称矩阵 B 为矩阵 A 的逆矩阵, 记为 $A^{-1} = B$.

可逆矩阵

1. 求逆矩阵的常用方法: 初等行变换方法.

可逆矩阵

1. 求逆矩阵的常用方法: 初等行变换方法.
2. A 可逆条件: $\det A \neq 0$.

可逆矩阵

1. 求逆矩阵的常用方法: 初等行变换方法.
2. A 可逆条件: $\det A \neq 0$.
3. 方阵 $A = (a_{ij})_{m\times m}$ 的行列式为: $\det A = \sum_{j=1}^{m} (-1)^{i+j} a_{ij} \det A_{ij}$, 熟记 $2, 3$ 阶行列式的计算公式.

可逆矩阵

1. 求逆矩阵的常用方法: 初等行变换方法.
2. A 可逆条件: $\det A \neq 0$.
3. 方阵 $A = (a_{ij})_{m\times m}$ 的行列式为: $\det A = \sum_{j=1}^{m} (-1)^{i+j} a_{ij} \det A_{ij}$, 熟记 $2, 3$ 阶行列式的计算公式.
4. 在模 26 的情形下, A 可逆条件是 $\gcd(\det A, 26) = 1$.

可逆矩阵

1. 求逆矩阵的常用方法: 初等行变换方法.
2. A 可逆条件: $\det A \neq 0$.
3. 方阵 $A = (a_{ij})_{m\times m}$ 的行列式为: $\det A = \sum_{j=1}^{m} (-1)^{i+j} a_{ij} \det A_{ij}$, 熟记 $2, 3$ 阶行列式的计算公式.
4. 在模 26 的情形下, A 可逆条件是 $\gcd(\det A, 26) = 1$.
5. 二阶矩阵 $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ 的逆矩阵为

$$A^{-1} = (\det A)^{-1} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}.$$

希尔密码 (Hill Cipher)

设 $m \geq 2$ 为正整数, $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$, 且

$$\mathcal{K} = \{\text{定义在 } \mathbb{Z}_{26} \text{ 上的 } m \times m \text{ 阶可逆方阵}\}.$$

对任意的密钥 K, 定义

$$E_K(x) = xK$$

和

$$D_K(y) = yK^{-1}.$$

Examp-1-1-6

试用希尔密码加密明文串: $x = mor$, 这里密钥为 3 阶方阵

$$K = \begin{pmatrix} 17 & 21 & 2 \\ 17 & 18 & 2 \\ 5 & 21 & 19 \end{pmatrix}.$$

Examp-1-1-6

试用希尔密码加密明文串: $x = mor$, 这里密钥为 3 阶方阵

$$K = \begin{pmatrix} 17 & 21 & 2 \\ 17 & 18 & 2 \\ 5 & 21 & 19 \end{pmatrix}.$$

加密

$$y = E_K(x) = xK = (12, 14, 17) \begin{pmatrix} 17 & 21 & 2 \\ 17 & 18 & 2 \\ 5 & 21 & 19 \end{pmatrix} \bmod 26 =$$

$(527, 861, 375) \bmod 26 = (7, 3, 11) \longleftrightarrow HDL.$

Examp-1-1-6

试用希尔密码加密明文串: $x = mor$, 这里密钥为 3 阶方阵

$$K = \begin{pmatrix} 17 & 21 & 2 \\ 17 & 18 & 2 \\ 5 & 21 & 19 \end{pmatrix}.$$

加密

$$y = E_K(x) = xK = (12, 14, 17) \begin{pmatrix} 17 & 21 & 2 \\ 17 & 18 & 2 \\ 5 & 21 & 19 \end{pmatrix} \bmod 26 =$$

$(527, 861, 375) \bmod 26 = (7, 3, 11) \longleftrightarrow HDL.$

解密

$$x = D_K(y) = yK^{-1} = (7, 3, 11) \begin{pmatrix} 4 & 15 & 24 \\ 9 & 17 & 0 \\ 15 & 6 & 17 \end{pmatrix} \bmod 26 =$$

$(220, 222, 355) \bmod 26 = (12, 14, 17) \longleftrightarrow mor.$

作业 1:

1. 使用穷尽密钥搜索法破译如下利用移位密码加密的密文:

ESPESTCOPIPCNTDPYPPODACZRCLXXTYR.

2. 试用维吉尼亚密码加密明文串:

we are discovered, save yourself,

这里密钥字为: friday.

3. 计算定义在 $\mathbb{Z}_{26}$ 上矩阵 $K = \begin{pmatrix} 1 & 11 & 12 \\ 4 & 23 & 2 \\ 17 & 15 & 9 \end{pmatrix}$ 的逆 K^{-1}, 并用 K 作为希尔密码体制的密钥完成对明文串:

looking forward to our national day

的加密和相应密文串的解密.

置换密码 (Permutation Cipher)

设 $m \in \mathbb{Z}_{>0}$, $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$, $\mathcal{K}$ 为集合 $\{1, 2, \cdots, m\}$ 上的所有置换构成的集合. 对任意密钥 $\pi \in \mathcal{K}$, 定义:

$$E_\pi(x_1, x_2, \cdots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \cdots, x_{\pi(m)})$$

和

$$D_\pi(y_1, y_2, \cdots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \cdots, y_{\pi^{-1}(m)}).$$

Examp-1-1-7

设 $m = 6$, 置换 $\pi = (3, 5, 1, 6, 4, 2)$. 试用 π 作为置换密码的密钥加密明文序列:

she sells seashells by the seashore,

并对得到的密文用置换 π 进行解密.

Examp-1-1-7

设 $m = 6$, 置换 $\pi = (3, 5, 1, 6, 4, 2)$. 试用 π 作为置换密码的密钥加密明文序列:

she sells seashells by the seashore,

并对得到的密文用置换 π 进行解密.

密文: EESL SHSA LSES LSHB LEHS YEET HRAE OS

分组密码与流密码

1. 分组密码 (Block cipher): 连续的明文元素用同一个密钥进行加密, 即

$$y_1 y_2 y_3 \cdots = E_K(x_1) E_K(x_2) E_K(x_3) \cdots .$$

分组密码与流密码

1. 分组密码 (Block cipher): 连续的明文元素用同一个密钥进行加密, 即

$$y_1 y_2 y_3 \cdots = E_K(x_1) E_K(x_2) E_K(x_3) \cdots .$$

2. 流密码 (Stream cipher): 连续的明文元素用不同的密钥进行加密, 即

$$y_1 y_2 y_3 \cdots = E_{z_1}(x_1) E_{z_2}(x_2) E_{z_3}(x_3) \cdots .$$

分组密码与流密码

1. 分组密码 (Block cipher): 连续的明文元素用同一个密钥进行加密, 即

$$y_1 y_2 y_3 \cdots = E_K(x_1) E_K(x_2) E_K(x_3) \cdots .$$

2. 流密码 (Stream cipher): 连续的明文元素用不同的密钥进行加密, 即

$$y_1 y_2 y_3 \cdots = E_{z_1}(x_1) E_{z_2}(x_2) E_{z_3}(x_3) \cdots .$$

3. 如何产生密钥流 $z = z_1 z_2 \cdots$ 是流密码的一个很重要方面.

流密码的一些定义

1. 同步流密码中的密钥流直接由初始密钥经过某种特定算法变换得来 (即 $z_i = f(K)$), 所得密钥流与明文串是相互独立的.

流密码的一些定义

1. 同步流密码中的密钥流直接由初始密钥经过某种特定算法变换得来 (即 $z_i = f(K)$), 所得密钥流与明文串是相互独立的.
2. 异步流密码的密钥流不但与初始密钥相关, 而且还与前面的明文串 (即 $z_i = f(K, x_1, x_2, \cdots, x_{i-1})$) 或者密文串 (即 $z_i = f(K, y_1, y_2, \cdots, y_{i-1})$) 相关.

流密码的一些定义

1. 同步流密码中的密钥流直接由初始密钥经过某种特定算法变换得来 (即 $z_i = f(K)$), 所得密钥流与明文串是相互独立的.
2. 异步流密码的密钥流不但与初始密钥相关, 而且还与前面的明文串 (即 $z_i = f(K, x_1, x_2, \cdots, x_{i-1})$) 或者密文串 (即 $z_i = f(K, y_1, y_2, \cdots, y_{i-1})$) 相关.
3. 如果对所有的整数 $i \geq 1$, 有 $z_{i+d} = z_i$, 则称该流密码为具有周期 d 的周期流密码. 例如, 维吉尼亚密码可以看成周期为 m 的流密码.

流密码的一些定义

1. 同步流密码中的密钥流直接由初始密钥经过某种特定算法变换得来 (即 $z_i = f(K)$), 所得密钥流与明文串是相互独立的.
2. 异步流密码的密钥流不但与初始密钥相关, 而且还与前面的明文串 (即 $z_i = f(K, x_1, x_2, \cdots, x_{i-1})$) 或者密文串 (即 $z_i = f(K, y_1, y_2, \cdots, y_{i-1})$) 相关.
3. 如果对所有的整数 $i \geq 1$, 有 $z_{i+d} = z_i$, 则称该流密码为具有周期 d 的周期流密码. 例如, 维吉尼亚密码可以看成周期为 m 的流密码.
4. 流密码通常以二元字符表示, 即 $\mathcal{P} = \mathcal{C} = \mathcal{L} = \mathbb{Z}_2$, 此时加密解密刚好都可以看作模 2 的加法, 它对应于异或运算, 所以都可以用硬件方式有效地实现.

同步流密码

同步流密码是一个六元组 $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{E}, \mathcal{D})$ 和一个函数 g, 满足

1. $\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}$ 意义如前;
2. $\mathcal{L}$ 是一个称之为密钥流字母表的有限集;
3. g 是一个密钥流生成器, 它使用密钥 $K \in \mathcal{K}$ 作为输入, 产生无限长的密钥流

$$z = z_1 z_2 z_3 \cdots,$$

这里 $z_i \in \mathcal{L}$.

4. 对任意的 $z \in \mathcal{L}$, 都有一个加密规则 $E_z \in \mathcal{E} : \mathcal{P} \to \mathcal{C}$ 和相应的解密规则 $D_z \in \mathcal{D} : \mathcal{C} \to \mathcal{P}$, 使得对任意的 $x \in \mathcal{P}$, 有

$$D_z(E_z(x)) = x.$$

同步密钥流产生的线性方法

假设 $m \in \mathbb{Z}_{>0}$, 密钥 $K = (k_1, k_2, \cdots, k_m, c_0, c_1, \cdots, c_{m-1})$.

令 $z_i = k_i$, $1 \leq i \leq m$, 则

$$z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \bmod 2, \quad i \geq 1.$$

这里向量 $(k_1, k_2, \cdots, k_m)$ 也称为初始向量, 上式可产生最大周期为 $2^m - 1$ 的密钥流.

Examp-1-1-8

设 $m = 4$, 初始向量为 $(1, 0, 0, 0)$. 密钥流按如下线性递归关系产生:

$$z_{i+4} = (z_i + z_{i+1}) \bmod 2, \quad i \geq 1,$$

则可得密钥流

$$\underline{1\,0\,0\,0}\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,\underline{1\,0\,0\,0}\cdots,$$

周期为 15.

异步流密码的例子: 自动密钥密码

设 $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathcal{L} = \mathbb{Z}_{26}$, $z_1 = K \in \mathcal{K}$, 定义 $z_i = x_{i-1}$, $i \geq 2$. 对任意的 $0 \leq z \leq 25$, $x, y \in \mathbb{Z}_{26}$, 定义

$$E_z(x) = (x + z) \bmod 26$$

和

$$D_z(y) = (y - z) \bmod 26.$$

Examp-1-1-9

试用自动密钥密码加密下列明文串

rendezvous,

这里假设密钥 $K = 8$.

Examp-1-1-9

试用自动密钥密码加密下列明文串

rendezvous,

这里假设密钥 $K = 8$.

密文为: ZVRQ HDUJ IM

§1.2　密码分析

Kerckhoff 假设

密码体制的安全性不是基于对密码算法的保密, 而是基于对密钥的保密.

Kerckhoff 假设

密码体制的安全性不是基于对密码算法的保密, 而是基于对密钥的保密.

Kerckhoff 假设思想

让攻击者知道密码算法没有关系，所有的秘密都隐藏在密钥中。对密码算法保密是不明智的，因为密码算法的设计很困难，一旦算法原理泄露了，必须得花费大量精力重新设计, 但密钥可以随时更换。

攻击者模型

1. 唯密文攻击: 敌手只拥有密文串 y.

攻击者模型

1. 唯密文攻击: 敌手只拥有密文串 y.
2. 已知明文攻击: 敌手拥有明文串 x 及其对应的密文串 y.

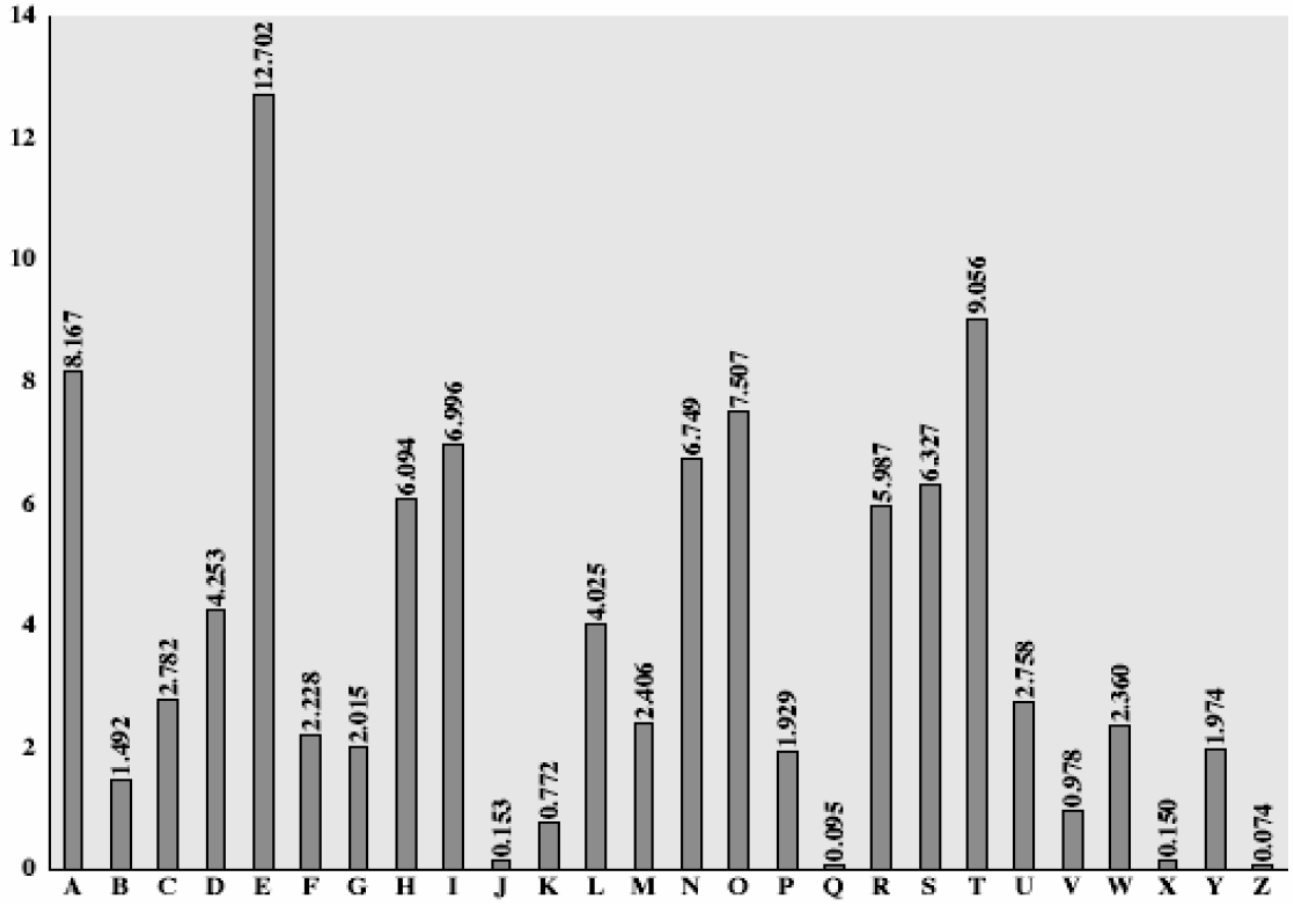
攻击者模型

1. 唯密文攻击: 敌手只拥有密文串 y.
2. 已知明文攻击: 敌手拥有明文串 x 及其对应的密文串 y.
3. 选择明文攻击: 敌手可以获得对加密机的临时访问权限, 这样他就能选择一个明文串 x, 并可以获得相应的密文串 y.

攻击者模型

1. 唯密文攻击: 敌手只拥有密文串 y.
2. 已知明文攻击: 敌手拥有明文串 x 及其对应的密文串 y.
3. 选择明文攻击: 敌手可以获得对加密机的临时访问权限, 这样他就能选择一个明文串 x, 并可以获得相应的密文串 y.
4. 选择密文攻击: 敌手可以获得对解密机的临时访问权限, 这样他就能选择一个密文串 y, 并可以获得相应的明文串 x.

英文字母使用频率


14
12
10
8
6
4
2
0
8.167
1.492
2.782
4.253
12.702
2.228
2.015
6.094
6.996
0.153
0.772
4.025
2.406
6.749
7.507
1.929
0.095
5.987
6.327
9.056
2.758
0.978
2.360
0.150
1.974
0.074
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

1. 单字母概率统计:
    1. E 的概率大约为 0.12;
    2. T, A, O, I, N, S, H, R 的概率在 0.06 至 0.09 之间;
    3. D, L 的概率大约为 0.04;
    4. C, U, M, W, F, G, Y, P, B 的概率在 0.015 至 0.028 之间;
    5. V, K, J, X, Q, Z 的概率小于 0.01;

1. 单字母概率统计:
    1. E 的概率大约为 0.12;
    2. T, A, O, I, N, S, H, R 的概率在 0.06 至 0.09 之间;
    3. D, L 的概率大约为 0.04;
    4. C, U, M, W, F, G, Y, P, B 的概率在 0.015 至 0.028 之间;
    5. V, K, J, X, Q, Z 的概率小于 0.01;
2. 最常见的两字母组: TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF;

1. 单字母概率统计:
    1. E 的概率大约为 0.12;
    2. T, A, O, I, N, S, H, R 的概率在 0.06 至 0.09 之间;
    3. D, L 的概率大约为 0.04;
    4. C, U, M, W, F, G, Y, P, B 的概率在 0.015 至 0.028 之间;
    5. V, K, J, X, Q, Z 的概率小于 0.01;
2. 最常见的两字母组: TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF;
3. 最常见的三字母组: THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH.

仿射密码 (Affine Cipher)

令 $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, 且

$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\}.$$

对任意的 $K = (a, b) \in \mathcal{K}$, 定义

$$E_K(x) = (ax + b) \bmod 26$$

和

$$D_K(y) = a^{-1}(y - b) \bmod 26.$$

Examp-1-2-1: 仿射密码的密码分析

试对以下用仿射密码加密得到的密文进行密码分析:

FMXV EDKA PHFE RBND KRXR SREF MORU DSDK DVSH

VUFE DKAP RKDL YEVL RHHR H

分析步骤

1. 频数分析: 57 个密文字母中, 出现次数最多的是: R (8), D (7), E, H, K (5) 和 F, S, V (4);

分析步骤

1. 频数分析: 57 个密文字母中, 出现次数最多的是: R (8), D (7), E, H, K (5) 和 F, S, V (4);
2. 尝试猜测密钥 (如果消息足够长, 则猜测是准确的):
   1. R←e, D←t: $\begin{cases} 4a + b = 17, \\ 19a + b = 3, \end{cases} \Longrightarrow a = 6, b = 19\ (\times)$

分析步骤

1. 频数分析: 57 个密文字母中, 出现次数最多的是: R (8), D (7), E, H, K (5) 和 F, S, V (4);
2. 尝试猜测密钥 (如果消息足够长, 则猜测是准确的):
   1. R←e, D←t: $\begin{cases} 4a+b=17, \\ 19a+b=3, \end{cases} \Longrightarrow a=6, b=19\ (\times)$
   2. R←e, E←t: $\begin{cases} 4a+b=17, \\ 19a+b=4, \end{cases} \Longrightarrow a=13, b=17\ (\times)$

分析步骤

1. 频数分析: 57 个密文字母中, 出现次数最多的是: R (8), D (7), E, H, K (5) 和 F, S, V (4);
2. 尝试猜测密钥 (如果消息足够长, 则猜测是准确的):
   1. R←e, D←t: $\begin{cases} 4a+b=17, \\ 19a+b=3, \end{cases} \Longrightarrow a=6, b=19\ (\times)$
   2. R←e, E←t: $\begin{cases} 4a+b=17, \\ 19a+b=4, \end{cases} \Longrightarrow a=13, b=17\ (\times)$
   3. R←e, H←t: $\begin{cases} 4a+b=17, \\ 19a+b=7, \end{cases} \Longrightarrow a=8, b=11\ (\times)$

分析步骤

1. 频数分析: 57 个密文字母中, 出现次数最多的是: R (8), D (7), E, H, K (5) 和 F, S, V (4);
2. 尝试猜测密钥 (如果消息足够长, 则猜测是准确的):
   1. R←e, D←t: $\begin{cases} 4a+b=17, \\ 19a+b=3, \end{cases} \Longrightarrow a=6, b=19\ (\times)$
   2. R←e, E←t: $\begin{cases} 4a+b=17, \\ 19a+b=4, \end{cases} \Longrightarrow a=13, b=17\ (\times)$
   3. R←e, H←t: $\begin{cases} 4a+b=17, \\ 19a+b=7, \end{cases} \Longrightarrow a=8, b=11\ (\times)$
   4. R←e, K←t: $\begin{cases} 4a+b=17, \\ 19a+b=10, \end{cases} \Longrightarrow a=3, b=5\ (\surd)$

分析步骤

1. 频数分析: 57 个密文字母中, 出现次数最多的是: R (8), D (7), E, H, K (5) 和 F, S, V (4);
2. 尝试猜测密钥 (如果消息足够长, 则猜测是准确的):
   1. R←e, D←t: $\begin{cases} 4a+b=17, \\ 19a+b=3, \end{cases} \Longrightarrow a=6, b=19\ (\times)$
   2. R←e, E←t: $\begin{cases} 4a+b=17, \\ 19a+b=4, \end{cases} \Longrightarrow a=13, b=17\ (\times)$
   3. R←e, H←t: $\begin{cases} 4a+b=17, \\ 19a+b=7, \end{cases} \Longrightarrow a=8, b=11\ (\times)$
   4. R←e, K←t: $\begin{cases} 4a+b=17, \\ 19a+b=10, \end{cases} \Longrightarrow a=3, b=5\ (\surd)$
3. 解密, 看能否得到有意思的明文序列. 如果能, 则表述所猜测的密钥为正确密钥.

分析步骤

1. 频数分析: 57 个密文字母中, 出现次数最多的是: R (8), D (7), E, H, K (5) 和 F, S, V (4);
2. 尝试猜测密钥 (如果消息足够长, 则猜测是准确的):
   1. R←e, D←t: $\begin{cases} 4a+b=17, \\ 19a+b=3, \end{cases} \Longrightarrow a=6, b=19\ (\times)$
   2. R←e, E←t: $\begin{cases} 4a+b=17, \\ 19a+b=4, \end{cases} \Longrightarrow a=13, b=17\ (\times)$
   3. R←e, H←t: $\begin{cases} 4a+b=17, \\ 19a+b=7, \end{cases} \Longrightarrow a=8, b=11\ (\times)$
   4. R←e, K←t: $\begin{cases} 4a+b=17, \\ 19a+b=10, \end{cases} \Longrightarrow a=3, b=5\ (\surd)$
3. 解密, 看能否得到有意思的明文序列. 如果能, 则表述所猜测的密钥为正确密钥.

algorithms are quite general definitions of arithmetic processes

代换密码 (Substitution Cipher)

令 $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$, $\mathcal{K}$ 是由 26 个数字 $0, 1, \cdots, 25$ 上的所有可能的置换组成. 对任意的置换 $\pi \in \mathcal{K}$, 定义

$$E_\pi(x) = \pi(x)$$

和

$$D_\pi(y) = \pi^{-1}(y),$$

这里 π^{-1} 表示置换 π 的逆置换.

Examp-1-2-2: 代换密码的密码分析

试对以下用代换密码加密得到的密文进行密码分析:

YIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTXCDDUMJ
NDIFEFMDZCDMQZKCEYFCJMYRNCWJCSZREXCHZUNMXZ
NZUCDRJXYYSMRTMEYIFZWDYVZVYFZUMRZCRWNZDZJJ
XZWGCHSMRNMDHNCMFQCHZJMXJZWIEJYUCFWDJNZDIR

单字母频数

字母	频数	字母	频数
A	0	*N*	9
B	1	*O*	0
C	15	*P*	1
D	13	*Q*	4
E	7	*R*	10
F	11	*S*	3
G	1	*T*	2
H	4	*U*	5
I	5	*V*	5
J	11	*W*	8
K	1	*X*	6
L	0	*Y*	10
M	16	*Z*	20

分析步骤

1. Z 出现的次数为 20, 远高于其它字母, 所以猜测 $Z \to e$;

分析步骤

1. Z 出现的次数为 20, 远高于其它字母, 所以猜测 $Z \to e$;
2. 出现次数大于 10 的有: C, D, F, J, M, R, Y, 希望它们对应的明文字母属于集合 $\{t, a, o, i, n, s, h, r\}$;

分析步骤

1. Z 出现的次数为 20, 远高于其它字母, 所以猜测 $Z \to e$;
2. 出现次数大于 10 的有: C, D, F, J, M, R, Y, 希望它们对应的明文字母属于集合 $\{t, a, o, i, n, s, h, r\}$;
3. 因为 $Z \to e$, 考察形如 $-Z$ 和 $Z-$ 的二元组, 发现这种类型最多的二元组是 DZ 和 ZW (4), 其次是 NZ 和 ZU (3);

分析步骤

1. Z 出现的次数为 20, 远高于其它字母, 所以猜测 $Z \to e$;
2. 出现次数大于 10 的有: C, D, F, J, M, R, Y, 希望它们对应的明文字母属于集合 $\{t, a, o, i, n, s, h, r\}$;
3. 因为 $Z \to e$, 考察形如 $-Z$ 和 $Z-$ 的二元组, 发现这种类型最多的二元组是 DZ 和 ZW (4), 其次是 NZ 和 ZU (3);
4. 因为 ZW 出现 4 次, 而 WZ 一次也没有出现, 同时 W (8) 出现的次数相对较少, 故猜测 $W \to d$; 又因为 DZ 出现了 4 次, 而 ZD 出现了 2 次, 故猜测 $D \to \{r, s, t\}$;

分析步骤

1. Z 出现的次数为 20, 远高于其它字母, 所以猜测 $Z \to e$;
2. 出现次数大于 10 的有: C, D, F, J, M, R, Y, 希望它们对应的明文字母属于集合 $\{t, a, o, i, n, s, h, r\}$;
3. 因为 $Z \to e$, 考察形如 $-Z$ 和 $Z-$ 的二元组, 发现这种类型最多的二元组是 DZ 和 ZW (4), 其次是 NZ 和 ZU (3);
4. 因为 ZW 出现 4 次, 而 WZ 一次也没有出现, 同时 W (8) 出现的次数相对较少, 故猜测 $W \to d$; 又因为 DZ 出现了 4 次, 而 ZD 出现了 2 次, 故猜测 $D \to \{r, s, t\}$;
5. 因已猜测 $Z \to e$, $W \to d$, 并注意到 ZRW 出现在密文的开始部分, 并且 RW 在后面也出现过, 因为 nd 是一个常见的二元组, 故猜测 $R \to n$;

分析步骤 (续)

6. 因为 NZ 出现了 3 次, 而 ZN 不是一个常见的二元组, 所以猜测 $N \to h$; 这样又可以由 $ne - ndhe$ 猜测 $C \to a$;

分析步骤 (续)

6. 因为 NZ 出现了 3 次, 而 ZN 不是一个常见的二元组, 所以猜测 $N \to h$; 这样又可以由 $ne - ndhe$ 猜测 $C \to a$;
7. 现在确定密文字母 M. 因为 RNM 解密成 $nh-$, 这说明 $h-$ 是一个词的开头, 所以 M 很可能是一个元音. 因为已经使用了 a, e, 故猜测 $M \to \{i, o\}$. 因为二元组 ai 出现的次数比 ao 高, 所以猜测 $M \to i$.

分析步骤 (续)

6. 因为 NZ 出现了 3 次, 而 ZN 不是一个常见的二元组, 所以猜测 $N \to h$; 这样又可以由 $ne - ndhe$ 猜测 $C \to a$;
7. 现在确定密文字母 M. 因为 RNM 解密成 $nh-$, 这说明 $h-$ 是一个词的开头, 所以 M 很可能是一个元音. 因为已经使用了 a, e, 故猜测 $M \to \{i, o\}$. 因为二元组 ai 出现的次数比 ao 高, 所以猜测 $M \to i$.
8. 下面确定明文 $o \leftarrow \{D, F, J, Y\}$ 对应的密文: 由于密文中出现 CFM, CDM, CJM, 如果 F, D, 或 $J \to o$ 的话, 将出现长串的元音字母 aoi, 所以猜测 $Y \to o$.

分析步骤 (续)

6. 因为 NZ 出现了 3 次, 而 ZN 不是一个常见的二元组, 所以猜测 $N \to h$; 这样又可以由 $ne - ndhe$ 猜测 $C \to a$;
7. 现在确定密文字母 M. 因为 RNM 解密成 $nh-$, 这说明 $h-$ 是一个词的开头, 所以 M 很可能是一个元音. 因为已经使用了 a, e, 故猜测 $M \to \{i, o\}$. 因为二元组 ai 出现的次数比 ao 高, 所以猜测 $M \to i$.
8. 下面确定明文 $o \leftarrow \{D, F, J, Y\}$ 对应的密文: 由于密文中出现 CFM, CDM, CJM, 如果 F, D, 或 $J \to o$ 的话, 将出现长串的元音字母 aoi, 所以猜测 $Y \to o$.
9. 下面确定剩余的三个出现频率高的密文字母 D, F, J, 猜测它们以某种次序解密成 r, s, t: 三元组 $NMD \to hi-$ 两次出现说明很可能 $D \to s$, 这与前面假设 $D \to \{r, s, t\}$ 是一致的.

10. $HNCMF \to -hai-$ 且 $F \to \{r, t\}$ 说明很可能 $F \to r$, $H \to c$, 同时说明很可能 $J \to t$.

10. $HNCMF \to -hai-$ 且 $F \to \{r, t\}$ 说明很可能 $F \to r$, $H \to c$, 同时说明很可能 $J \to t$.

11. 最后很容易恢复明文串为:

    Our friend from Paris examined his empty glass with surprise, as if evaporation had taken place while he wasn't looking. I poured some more wine and he settled back in his chair, face tilted up towards the sun.

作业 2 (共 2 题)

试从以下密文恢复出相应的明文:

2.1 仿射密码:

AOPC GUDE	YKRO IFKG	BEFM CPIY	CRAR DEPB
AQUF EPGH	KJPK DDCJ	GKPJ IEVC	GEBE BAYC
FAMC XCER	IARE HAFF	ERJG HCRA	OKBB KYAR
RCED KFAI	GHCP CDCK	DFCB KKME	FEMC GKXC
OKRQ KYYE	BKYC ERBH	CCRJ KVEI	BKPS AQKU
FJRK BIDC	EMEG HKFC	ICRB CRQC	ARQK YDER
SERJ GEIQ	KRIA JCPC	JRKB BKKX	PAOH B

2.2 代换密码

FSHF PMGH TFVM AZPP ZYUB MMGZ SOVI NFUM
KCZM ZSOM GZVN FFWK IVAH YZAZ SOGF KTUY
GTIM GHTI MZYI BNIY WOCF USAM FZSY BUAH
YCDL MFOC ILGD ZVIN CFIA VUNQ HYMI SAZM
CHRU ZCHV WSFK BHAO HFPV HEHC IBIC HIVF
PTIM GHTI MZYV ZSYB UAZS OSUT NHCM GHFC
DOCF ULVC ZSOV ISAP ZHBA VBZS HICI BOHN
CILC FNIN ZBZM DISA ZSPF CTIM ZFSM GHFC
DZGI EHMC ZHAS FMMF IVVU THMF FTUY GTIM
GHTI MZYI BNIY WOCF USAI SAMG UVZA HEHB
FLTI MGHT IMZY IBMF FBVI VMGH DICH SHHA
HAPF CMGH TFVM LICM SFMH MGIM ZPDF UPZS
ZVGM GHIN FEHM KFHJ HCYZ VHVL BHIV HZTT
HAZI MHBD VHSA THIS HTIZ BKZM GMGH VFBU
MZFS VZPD FUYI SPFC MUSI MHBD CHYH ZEHI
YFSP ZCTI MZFS HTIZ BKGZ YGZS PFCT VDFU
MGIM DFUI CHMG HPZC VMFS HMFA FMGI MDFU
KZBB NHIK ICAH AIUA ZVWF PPFU CON

维吉尼亚密码

设 m 是一个正整数. 定义 $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$. 对任意的密钥 $K = (k_1, k_2, \cdots, k_m)$, 定义

$$E_K(x_1, x_2, \cdots, x_m) = (x_1 + k_1, x_2 + k_2, \cdots, x_m + k_m)$$

和

$$D_K(y_1, y_2, \cdots, y_m) = (y_1 - k_1, y_2 - k_2, \cdots, y_m - k_m),$$

以上所有的运算都是在 $\mathbb{Z}_{26}$ 上进行.

维吉尼亚密码

设 m 是一个正整数. 定义 $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$. 对任意的密钥 $K = (k_1, k_2, \cdots, k_m)$, 定义

$$E_K(x_1, x_2, \cdots, x_m) = (x_1 + k_1, x_2 + k_2, \cdots, x_m + k_m)$$

和

$$D_K(y_1, y_2, \cdots, y_m) = (y_1 - k_1, y_2 - k_2, \cdots, y_m - k_m),$$

以上所有的运算都是在 $\mathbb{Z}_{26}$ 上进行.

密钥空间

密钥空间大小为 26^m, 当 $m = 5$ 时, $26^5 > 1.1 \times 10^7$, 已经超出了使用手算进行密钥空间搜索的能力范围.

密钥字长度 m 的确定

1. Kasiski 测试法: 两个距离为 δ (假设 $m|\delta$) 的相同明文段将加密成相同的密文段. 反过来, 如果在密文中观察到两个相同密文段 (长度至少为 3), 则它们其实对应了相同的明文段, 而且密钥字长度就是距离的一个因子, 这将给攻击者带来很大方便.

密钥字长度 m 的确定

1. Kasiski 测试法: 两个距离为 δ (假设 $m|\delta$) 的相同明文段将加密成相同的密文段. 反过来, 如果在密文中观察到两个相同密文段 (长度至少为 3), 则它们其实对应了相同的明文段, 而且密钥字长度就是距离的一个因子, 这将给攻击者带来很大方便.

2. 重合指数法: 当用 Kasiski 方法猜测出密钥字长度之后, 可以用重合指数法进一步进行确定.

Kasiski 测试法

搜索长度至少为 3 的相同密文段, 并记下它们与起始点的距离.

假如得到了 k 个距离 $\delta_1, \delta_2, \cdots, \delta_k$, 则可以猜测

$$m = \gcd(\delta_1, \delta_2, \cdots, \delta_k).$$

重合指数法

1. 重合指数: 假设 $\mathbf{x} = x_1 x_2 \cdots x_n$ 是一条长度 n 的字符串, $\mathbf{x}$ 的重合指数 ($\mathbf{I}_c(\mathbf{x})$) 定义为: $\mathbf{x}$ 中两个随机元素相同的概率.

重合指数法

1. 重合指数: 假设 $\mathbf{x} = x_1 x_2 \cdots x_n$ 是一条长度 n 的字符串, $\mathbf{x}$ 的重合指数 ($\mathbf{I}_c(\mathbf{x})$) 定义为: $\mathbf{x}$ 中两个随机元素相同的概率.
2. $\mathbf{I}_c(\mathbf{x})$ 的计算: 假设 $f_0, f_1, f_2, \cdots, f_{25}$ 分别表示字母 $A, B, C, \cdots, Z$ 在 $\mathbf{x}$ 中出现的次 (频) 数, 则

$$\mathbf{I}_c(\mathbf{x}) = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)}. \tag{1}$$

重合指数法

1. 重合指数: 假设 $\mathbf{x} = x_1 x_2 \cdots x_n$ 是一条长度 n 的字符串, $\mathbf{x}$ 的重合指数 ($\mathbf{I}_c(\mathbf{x})$) 定义为: $\mathbf{x}$ 中两个随机元素相同的概率.
2. $\mathbf{I}_c(\mathbf{x})$ 的计算: 假设 $f_0, f_1, f_2, \cdots, f_{25}$ 分别表示字母 $A, B, C, \cdots, Z$ 在 $\mathbf{x}$ 中出现的次 (频) 数, 则

$$\mathbf{I}_c(\mathbf{x}) = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)}. \tag{1}$$

   1. 从 $\mathbf{x}$ 中任意选择两个元素的选法个数有: $C_n^2 = \frac{n(n-1)}{2}$;
   2. 对每一个 i, $0 \le i \le 25$, 共有 $C_{f_i}^2 = \frac{f_i(f_i-1)}{2}$ 种方法使得所选两个元素皆为 i;
   3. 故 (1) 式成立.

英语文本串的重合指数

假设 **x** 是一个英文文本串, 字母 $a, b, c, \cdots, z$ 出现的期望概率为 $p_0, p_1, p_2, \cdots, p_{25}$ (参见书本中表 1.1), 则 **x** 的重合指数为

$$\mathbf{I}_c(\mathbf{x}) = \frac{\sum_{i=0}^{25} f_i(f_i-1)}{n(n-1)} = \sum_{i=0}^{25} \frac{f_i}{n} \cdot \frac{f_i-1}{n-1} \approx \sum_{i=0}^{25} p_i^2 = 0.065.$$

英语文本串的重合指数

假设 **x** 是一个英文文本串, 字母 $a, b, c, \cdots, z$ 出现的期望概率为 $p_0, p_1, p_2, \cdots, p_{25}$ (参见书本中表 1.1), 则 **x** 的重合指数为

$$\mathbf{I}_c(\mathbf{x}) = \frac{\sum_{i=0}^{25} f_i(f_i-1)}{n(n-1)} = \sum_{i=0}^{25} \frac{f_i}{n} \cdot \frac{f_i-1}{n-1} \approx \sum_{i=0}^{25} p_i^2 = 0.065.$$

注意:

1. 如果密文串 **x** 是通过单表代换而来, 此时尽管各个字母的概率将被置换, 但总量 $\sum_{i=0}^{25} p_i^2 = 0.065$ 不变.

英语文本串的重合指数

假设 **x** 是一个英文文本串, 字母 $a, b, c, \cdots, z$ 出现的期望概率为 $p_0, p_1, p_2, \cdots, p_{25}$ (参见书本中表 1.1), 则 **x** 的重合指数为

$$\mathbf{I}_c(\mathbf{x}) = \frac{\sum_{i=0}^{25} f_i(f_i-1)}{n(n-1)} = \sum_{i=0}^{25} \frac{f_i}{n} \cdot \frac{f_i-1}{n-1} \approx \sum_{i=0}^{25} p_i^2 = 0.065.$$

注意:

1. 如果密文串 **x** 是通过单表代换而来, 此时尽管各个字母的概率将被置换, 但总量 $\sum_{i=0}^{25} p_i^2 = 0.065$ 不变.
2. 如果密文串 **x** 是随机字母串的话, 则期望其重合指数为

$$\mathbf{I}_c(\mathbf{x}) = \sum_{i=0}^{25} (\frac{1}{26})^2 = 26(\frac{1}{26})^2 = \frac{1}{26} = 0.038.$$

Examp-1-2-3: 重合指数的计算

计算密文串 $\mathbf{X}=$

FSHF PMGH	TFVM AZPP	ZYUB MMGZ	SOVI NFUM
KCZM ZSOM	GZVN FFWK	IVAH YZAZ	SOGF KTUY
GTIM GHTI	MZYI BNIY	WOCF USAM	FZSY BUAH
YCDL MFOC	ILGD ZVIN	CFIA VUNQ	HYMI SAZM
CHRU ZCHV	WSFK BHAO	HFPV HEHC	IBIC HIVF
PTIM GHTI	MZYV ZSYB	UAZS OSUT	NHCM GHFC
DOCF ULVC	ZSOV ISAP	ZHBA VBZS	HICI BOHN
CILC FNIN	ZBZM DISA	ZSPF CTIM	ZFSM GHFC

的重合指数 $\mathbf{I}_c(\mathbf{X})$.

1. 字母出现次数:

Z	I	F	H	M	C	S	V	A	O	G	U	Y
23	22	20	20	19	18	17	13	12	10	10	10	10

B	N	T	P	K	L	D	W	Q	R	E	X	J
10	9	8	7	4	4	4	3	1	1	1	0	0

1. 字母出现次数:

Z	I	F	H	M	C	S	V	A	O	G	U	Y
23	22	20	20	19	18	17	13	12	10	10	10	10

B	N	T	P	K	L	D	W	Q	R	E	X	J
10	9	8	7	4	4	4	3	1	1	1	0	0

2. $\sum_{i=0}^{25} f_i(f_i-1) = 23\cdot(23-1)+22\cdot(22-1)+\cdots+0\cdot(0-1) = 3598;$

1. 字母出现次数:

Z	I	F	H	M	C	S	V	A	O	G	U	Y
23	22	20	20	19	18	17	13	12	10	10	10	10

B	N	T	P	K	L	D	W	Q	R	E	X	J
10	9	8	7	4	4	4	3	1	1	1	0	0

2. $\sum_{i=0}^{25} f_i(f_i-1) = 23\cdot(23-1)+22\cdot(22-1)+\cdots+0\cdot(0-1) = 3598;$
3. $n \cdot (n-1) = 256 \cdot 255 = 65280;$

1. 字母出现次数:

Z	I	F	H	M	C	S	V	A	O	G	U	Y
23	22	20	20	19	18	17	13	12	10	10	10	10

B	N	T	P	K	L	D	W	Q	R	E	X	J
10	9	8	7	4	4	4	3	1	1	1	0	0

2. $\sum_{i=0}^{25} f_i(f_i-1) = 23\cdot(23-1)+22\cdot(22-1)+\cdots+0\cdot(0-1) = 3598;$
3. $n\cdot(n-1) = 256\cdot 255 = 65280;$
4. $\mathbf{I}_c(\mathbf{X}) = \frac{\sum_{i=0}^{25} f_i(f_i-1)}{n(n-1)} = \frac{3598}{62580} \approx 0.055.$

确定密钥字长度的方法

假设密文串为 $\mathbf{y} = y_1 y_2 y_3 \cdots y_n$, m 是其一个猜测的密钥字长度 (比如通过前面介绍的 Kasiski 方法而获得), 则可通过以下方法对 m 的值进行确定:

确定密钥字长度的方法

假设密文串为 $\mathbf{y} = y_1 y_2 y_3 \cdots y_n$, m 是其一个猜测的密钥字长度 (比如通过前面介绍的 Kasiski 方法而获得), 则可通过以下方法对 m 的值进行确定:

1. 将 $\mathbf{y}$ 按列分为 m 个长度相等的子串 $\mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_m$:

$$\begin{aligned} \mathbf{y}_1 &= y_1 y_{m+1} y_{2m+1} \cdots \\ \mathbf{y}_2 &= y_2 y_{m+2} y_{2m+2} \cdots \\ &\vdots \\ \mathbf{y}_m &= y_m y_{2m} y_{3m} \cdots \end{aligned}$$

确定密钥字长度的方法

假设密文串为 $\mathbf{y} = y_1 y_2 y_3 \cdots y_n$, m 是其一个猜测的密钥字长度 (比如通过前面介绍的 Kasiski 方法而获得), 则可通过以下方法对 m 的值进行确定:

1. 将 $\mathbf{y}$ 按列分为 m 个长度相等的子串 $\mathbf{y}_1, \mathbf{y}_2, \cdots, \mathbf{y}_m$:

$$\begin{aligned} \mathbf{y}_1 &= y_1 y_{m+1} y_{2m+1} \cdots \\ \mathbf{y}_2 &= y_2 y_{m+2} y_{2m+2} \cdots \\ &\vdots \\ \mathbf{y}_m &= y_m y_{2m} y_{3m} \cdots \end{aligned}$$

2. 对 $\forall\, 1 \le i \le m$, 计算重合指数 $\mathbf{I}_c(\mathbf{y}_i)$. 如果它们的值都约等于 0.065, 则确定 m 就是密钥字长度; 否则, $\mathbf{I}_c(\mathbf{y}_i)$ 的值应该约等于 0.038, m 不是密钥字长度.

Examp-1-2-4: 两种技术的综合应用

试确定用于下列维吉尼亚密码密文的密钥字长度:

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBW
RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK
LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX
VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR
ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI
PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP
WQAIIWXNRMGWOIIFKEE

解答:

1. 首先用 Kasiski 测试法: 在密文中, 密文串 CHR 共出现在 5 个位置, 起始位置分别为: 1, 166, 236, 276, 286, 其距离分别为: 155, 235, 275, 285. 这四个整数的最大公约数为 5, 故猜测密钥字长度为 5.

解答:

1. 首先用 Kasiski 测试法: 在密文中, 密文串 CHR 共出现在 5 个位置, 起始位置分别为: 1, 166, 236, 276, 286, 其距离分别为: 155, 235, 275, 285. 这四个整数的最大公约数为 5, 故猜测密钥字长度为 5.
2. 再用重合指数法确认这一猜测:

解答:

1. 首先用 Kasiski 测试法: 在密文中, 密文串 CHR 共出现在 5 个位置, 起始位置分别为: 1, 166, 236, 276, 286, 其距离分别为: 155, 235, 275, 285. 这四个整数的最大公约数为 5, 故猜测密钥字长度为 5.
2. 再用重合指数法确认这一猜测:
    1. $m = 1$: 重合指数为 .045;

解答:

1. 首先用 Kasiski 测试法: 在密文中, 密文串 CHR 共出现在 5 个位置, 起始位置分别为: 1, 166, 236, 276, 286, 其距离分别为: 155, 235, 275, 285. 这四个整数的最大公约数为 5, 故猜测密钥字长度为 5.
2. 再用重合指数法确认这一猜测:
    1. $m = 1$: 重合指数为 .045;
    2. $m = 2$: 两个重合指数分别为 .046 和 .041;

解答:

1. 首先用 Kasiski 测试法: 在密文中, 密文串 CHR 共出现在 5 个位置, 起始位置分别为: 1, 166, 236, 276, 286, 其距离分别为: 155, 235, 275, 285. 这四个整数的最大公约数为 5, 故猜测密钥字长度为 5.
2. 再用重合指数法确认这一猜测:
    1. $m = 1$: 重合指数为 .045;
    2. $m = 2$: 两个重合指数分别为 .046 和 .041;
    3. $m = 3$: 三个重合指数分别为 .043, .050, .047;

解答:

1. 首先用 Kasiski 测试法: 在密文中, 密文串 CHR 共出现在 5 个位置, 起始位置分别为: 1, 166, 236, 276, 286, 其距离分别为: 155, 235, 275, 285. 这四个整数的最大公约数为 5, 故猜测密钥字长度为 5.
2. 再用重合指数法确认这一猜测:
    1. $m = 1$: 重合指数为 .045;
    2. $m = 2$: 两个重合指数分别为 .046 和 .041;
    3. $m = 3$: 三个重合指数分别为 .043, .050, .047;
    4. $m = 4$: 四个重合指数分别为 .042, .039, .045, .040;

解答:

1. 首先用 Kasiski 测试法: 在密文中, 密文串 CHR 共出现在 5 个位置, 起始位置分别为: 1, 166, 236, 276, 286, 其距离分别为: 155, 235, 275, 285. 这四个整数的最大公约数为 5, 故猜测密钥字长度为 5.
2. 再用重合指数法确认这一猜测:
   1. $m = 1$: 重合指数为 .045;
   2. $m = 2$: 两个重合指数分别为 .046 和 .041;
   3. $m = 3$: 三个重合指数分别为 .043, .050, .047;
   4. $m = 4$: 四个重合指数分别为 .042, .039, .045, .040;
   5. $m = 5$: 五个重合指数分别为 .063, .068, .069, .061, .072;

解答:

1. 首先用 Kasiski 测试法: 在密文中, 密文串 CHR 共出现在 5 个位置, 起始位置分别为: 1, 166, 236, 276, 286, 其距离分别为: 155, 235, 275, 285. 这四个整数的最大公约数为 5, 故猜测密钥字长度为 5.
2. 再用重合指数法确认这一猜测:
   1. $m = 1$: 重合指数为 .045;
   2. $m = 2$: 两个重合指数分别为 .046 和 .041;
   3. $m = 3$: 三个重合指数分别为 .043, .050, .047;
   4. $m = 4$: 四个重合指数分别为 .042, .039, .045, .040;
   5. $m = 5$: 五个重合指数分别为 .063, .068, .069, .061, .072;
3. 上述值为密钥字长度为 5 提供了强有力的证据.

确定密钥字 $K = (k_1, k_2, \cdots, k_m)$

假设已经确定了密钥字长度为 m, 将长度为 n 的密文序列 $\mathbf{y}$ 按列分成 m 个子串 $\mathbf{y}_i$, $1 \leq i \leq m$, 每个子串 $\mathbf{y}_i$ 长度为 $n' = n/m$. 为了确定分量 k_i, 可以执行以下步骤:

1. 统计字母 $A, B, \cdots, Z$ 在 $\mathbf{y}_i$ 中出现的次数, 记为 $f_0, f_1, \cdots, f_{25}$, 则其概率分布为

$$\frac{f_0}{n'}, \frac{f_1}{n'}, \cdots, \frac{f_{25}}{n'};$$

确定密钥字 $K = (k_1, k_2, \cdots, k_m)$

假设已经确定了密钥字长度为 m, 将长度为 n 的密文序列 $\mathbf{y}$ 按列分成 m 个子串 $\mathbf{y}_i$, $1 \leq i \leq m$, 每个子串 $\mathbf{y}_i$ 长度为 $n' = n/m$. 为了确定分量 k_i, 可以执行以下步骤:

1. 统计字母 $A, B, \cdots, Z$ 在 $\mathbf{y}_i$ 中出现的次数, 记为 $f_0, f_1, \cdots, f_{25}$, 则其概率分布为

$$\frac{f_0}{n'}, \frac{f_1}{n'}, \cdots, \frac{f_{25}}{n'};$$

2. 对 $\forall\, 0 \leq g \leq 25$, 计算 $M_g \triangleq \sum_{i=0}^{25} p_i \frac{f_{i+g}}{n'}$, 这样可得

$$M_0, M_1, \cdots, M_{25};$$

确定密钥字 $K = (k_1, k_2, \cdots, k_m)$

假设已经确定了密钥字长度为 m, 将长度为 n 的密文序列 $\mathbf{y}$ 按列分成 m 个子串 $\mathbf{y}_i$, $1 \leq i \leq m$, 每个子串 $\mathbf{y}_i$ 长度为 $n' = n/m$. 为了确定分量 k_i, 可以执行以下步骤:

1. 统计字母 $A, B, \cdots, Z$ 在 $\mathbf{y}_i$ 中出现的次数, 记为 $f_0, f_1, \cdots, f_{25}$, 则其概率分布为

$$\frac{f_0}{n'}, \frac{f_1}{n'}, \cdots, \frac{f_{25}}{n'};$$

2. 对 $\forall\, 0 \leq g \leq 25$, 计算 $M_g \triangleq \sum_{i=0}^{25} p_i \frac{f_{i+g}}{n'}$, 这样可得

$$M_0, M_1, \cdots, M_{25};$$

3. $k_i = g$, 这里 $M_g = \max\{M_0, M_1, \cdots, M_{25}\} \approx 0.065$.

Examp-1-2-4 (续)

i	value of $M_g(\mathbf{y}_i)$								
1	.035	.031	.036	.037	.035	.039	.028	.028	.048
	.061	.039	.032	.040	.038	.038	.045	.036	.030
	.042	.043	.036	.033	.049	.043	.042	.036	
2	.069	.044	.032	.035	.044	.034	.036	.033	.029
	.031	.042	.045	.040	.045	.046	.042	.037	.032
	.034	.037	.032	.034	.043	.032	.026	.047	
3	.048	.029	.042	.043	.044	.034	.038	.035	.032
	.049	.035	.031	.035	.066	.035	.038	.036	.045
	.027	.035	.034	.034	.036	.035	.046	.040	
4	.045	.032	.033	.038	.060	.034	.034	.034	.050
	.033	.033	.043	.040	.033	.029	.036	.040	.044
	.037	.050	.034	.034	.039	.044	.038	.035	
5	.034	.031	.035	.044	.047	.037	.043	.038	.042
	.037	.033	.032	.036	.037	.036	.045	.032	.029
	.044	.072	.037	.027	.031	.048	.036	.037	

由上表可知, 密钥很可能就是 $K = (9, 0, 13, 4, 19)$, 对应的密钥字为 JANET, 可以通过解密密文来进行验证.

由上表可知, 密钥很可能就是 $K = (9, 0, 13, 4, 19)$, 对应的密钥字为 JANET, 可以通过解密密文来进行验证.

密文解密后为:

The almond tree was in tentative blossom. The days were longer, often ending with magnificent evenings of corrugated pink skies. The hunting season was over, with hounds and guns put away for six months. The vineyards were busy again as the well-organized farmers treated their vines and the more lackadaisical neighbors hurried to do the pruning they should have done in November.

希尔密码的密码分析

设 $m \geq 2$ 为正整数, $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$, 且

$$\mathcal{K} = \{\text{定义在 } \mathbb{Z}_{26} \text{ 上的 } m \times m \text{ 阶可逆方阵}\}.$$

对任意的密钥 K, 定义

$$y = E_K(x) = xK$$

和

$$D_K(y) = yK^{-1}.$$

希尔密码的密码分析

设 $m \geq 2$ 为正整数, $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$, 且

$$\mathcal{K} = \{\text{定义在 } \mathbb{Z}_{26} \text{ 上的 } m \times m \text{ 阶可逆方阵}\}.$$

对任意的密钥 K, 定义

$$y = E_K(x) = xK$$

和

$$D_K(y) = yK^{-1}.$$

1. 唯密文攻击破译很难;

希尔密码的密码分析

设 $m \geq 2$ 为正整数, $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$, 且

$$\mathcal{K} = \{\text{定义在 } \mathbb{Z}_{26} \text{ 上的 } m \times m \text{ 阶可逆方阵}\}.$$

对任意的密钥 K, 定义

$$y = E_K(x) = xK$$

和

$$D_K(y) = yK^{-1}.$$

1. 唯密文攻击破译很难;
2. 已知明文攻击破译很容易.

希尔密码的已知明文攻击

假设敌手已经知道 m, 并且有不少于 m 个不同的明文-密文对 $(\mathbf{x}_i, \mathbf{y}_i)$, 这里 $\mathbf{y}_i = \mathbf{x}_i K$. 定义两个矩阵 A 和 B 如下:

$$A = \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_m \end{pmatrix}, \quad B = \begin{pmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_m \end{pmatrix}$$

则有式子: $B = AK$.

1. 如果矩阵 A 可逆, 则显然有 $K = A^{-1}B$, 从而得到 K.

希尔密码的已知明文攻击

假设敌手已经知道 m, 并且有不少于 m 个不同的明文-密文对 $(\mathbf{x}_i, \mathbf{y}_i)$, 这里 $\mathbf{y}_i = \mathbf{x}_i K$. 定义两个矩阵 A 和 B 如下:

$$A = \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_m \end{pmatrix}, \quad B = \begin{pmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_m \end{pmatrix}$$

则有式子: $B = AK$.

1. 如果矩阵 A 可逆, 则显然有 $K = A^{-1}B$, 从而得到 K.
2. 如果矩阵 A 不可逆, 则需重新选择 m 个明文-密文对, 然后构造矩阵 A 和 B. 如果有必要, 这个过程一直下去, 直到构造的 A 可逆为止.

Examp-1-2-5: 希尔密码的密码分析

假设明文

friday

利用 $m = 2$ 的希尔密码加密, 得到的密文为

VYUZSM.

试确定密钥 K.

Examp-1-2-5: 希尔密码的密码分析

假设明文

friday

利用 $m = 2$ 的希尔密码加密, 得到的密文为

VYUZSM.

试确定密钥 K.

密钥等式: $\begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix} K = \begin{pmatrix} 21 & 24 \\ 20 & 25 \end{pmatrix}$

Examp-1-2-5: 希尔密码的密码分析

假设明文

friday

利用 $m = 2$ 的希尔密码加密, 得到的密文为

VYUZSM.

试确定密钥 K.

密钥等式: $\begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix} K = \begin{pmatrix} 21 & 24 \\ 20 & 25 \end{pmatrix} \Rightarrow K = \begin{pmatrix} 1 & 7 \\ 4 & 7 \end{pmatrix}$

希尔密码的密码分析: 如何确定 m

1. 可以通过简单的尝试 $m = 2, 3, \cdots,$ 直到找到正确的密钥. 密钥是否正确可以通过其余的明文-密文对来验证;

希尔密码的密码分析: 如何确定 m

1. 可以通过简单的尝试 $m = 2, 3, \cdots,$ 直到找到正确的密钥. 密钥是否正确可以通过其余的明文-密文对来验证;
2. 前面介绍的 Kasiski 测试法.

作业 3 (共 2 题)

3.1 (书上习题 1.21 (b)) 破译下列用维吉尼亚密码加密的密文:

KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUD
DKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYC
QKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRL
SVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMV
GKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAFS
PEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHI
FFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIY
CWHJVLNHIQIBTKHJVNPIST

3.2 (书上习题 1.23) 假设明文

breathtaking

使用希尔密码被加密为

RUPOTENTOSUP.

试确定加密密钥矩阵 (矩阵维数 m 未知).