一些古典密码密码体制

杜育松

中山大学计算机学院

内容提要

1. 密码体制的数学定义
2. 移位密码
3. 代换密码
4. 仿射密码
5. 维吉尼亚密码
6. 希尔密码
7. 置换密码

内容提要

1. 密码体制的数学定义
2. 移位密码
3. 代换密码
4. 仿射密码
5. 维吉尼亚密码
6. 希尔密码
7. 置换密码

密码体制的数学定义

定义1

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. $\mathcal{P}$表示所有可能的明文组成的有限集合，被称为“明文空间”
2. $\mathcal{C}$表示所有可能的密文组成的有限集合，被称为“密文空间”
3. $\mathcal{K}$表示所有可能的密钥组成的有限集合，被称为“密钥空间”
4. 对于每一个密钥$K \in \mathcal{K}$，都存在一个加密规则$e_K \in \mathcal{E}$和相对应的解密规则$d_K \in \mathcal{D}$，并且对每一对$e_K \in \mathcal{E}$和$d_K \in \mathcal{D}$，以及每一个明文$x \in \mathcal{P}$，都有$d_K(e_K(x)) = x$.

密码体制的数学定义

定义1

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. $\mathcal{P}$表示所有可能的明文组成的有限集合，被称为“明文空间”
2. $\mathcal{C}$表示所有可能的密文组成的有限集合，被称为“密文空间”
3. $\mathcal{K}$表示所有可能的密钥组成的有限集合，被称为“密钥空间”
4. 对于每一个密钥$K \in \mathcal{K}$，都存在一个加密规则$e_K \in \mathcal{E}$和相对应的解密规则$d_K \in \mathcal{D}$，并且对每一对$e_K \in \mathcal{E}$和$d_K \in \mathcal{D}$，以及每一个明文$x \in \mathcal{P}$，都有$d_K(e_K(x)) = x$.

- 定义中性质(4)最重要。它确保如果使用加密规则e_K对明文x进行加密，则可以使用对应的解密规则d_K对密文解密，得到明文x。

密码体制的数学定义

定义1

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. $\mathcal{P}$表示所有可能的明文组成的有限集合，被称为“明文空间”
2. $\mathcal{C}$表示所有可能的密文组成的有限集合，被称为“密文空间”
3. $\mathcal{K}$表示所有可能的密钥组成的有限集合，被称为“密钥空间”
4. 对于每一个密钥$K \in \mathcal{K}$，都存在一个加密规则$e_K \in \mathcal{E}$和相对应的解密规则$d_K \in \mathcal{D}$，并且对每一对$e_K \in \mathcal{E}$和$d_K \in \mathcal{D}$，以及每一个明文$x \in \mathcal{P}$，都有$d_K(e_K(x)) = x$.

- 定义中性质(4)最重要。它确保如果使用加密规则e_K对明文x进行加密，则可以使用对应的解密规则d_K对密文解密，得到明文x。
- 实际上，需要加密的明文通常不是明文空间$\mathcal{P}$中的一个元素，而是由同属明文空间$\mathcal{P}$的多个元素组成的元素串，习惯上称之为“消息串”。例如消息串$\mathbf{x} = x_1, x_2, \cdots, x_n$，其中$x_i \in \mathcal{P}$。

加密与解密

1. Alice和Bob随机选择一个密钥$K \in \mathcal{K}$。这一步必须在安全的环境下进行，不能被敌手Oscar知道，例如两人在同一地点当面协商密钥，或者使用安全信道传送密钥。

加密与解密

1. Alice和Bob随机选择一个密钥$K \in \mathcal{K}$。这一步必须在安全的环境下进行，不能被敌手Oscar知道，例如两人在同一地点当面协商密钥，或者使用安全信道传送密钥。
2. Alice想通过不安全的信道发送消息串（或称为明文串）

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

给Bob，这里n 为正整数，$x_i \in \mathcal{P}$且$i = 1, 2, \cdots, n$。Alice使用加密规则$e_K \in \mathcal{E}$对消息串$\mathbf{x}$加密，K是上面协商好的密钥。对于$i = 1, 2, \cdots, n$，Alice计算$y_i = e_K(x_i)$，然后将密文串

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

发给Bob。

加密与解密

1. Alice和Bob随机选择一个密钥$K \in \mathcal{K}$。这一步必须在安全的环境下进行，不能被敌手Oscar知道，例如两人在同一地点当面协商密钥，或者使用安全信道传送密钥。
2. Alice想通过不安全的信道发送消息串（或称为明文串）

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

给Bob，这里n 为正整数，$x_i \in \mathcal{P}$且$i = 1, 2, \cdots, n$。Alice使用加密规则$e_K \in \mathcal{E}$对消息串$\mathbf{x}$加密，K是上面协商好的密钥。对于$i = 1, 2, \cdots, n$，Alice计算$y_i = e_K(x_i)$，然后将密文串

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

发给Bob。

3. Bob收到Alice发送的密文串$\mathbf{y} = y_1, y_2, \cdots, y_n$后，Bob使用加密规则$d_K \in \mathcal{E}$和协商好的密钥$K$对消息串$\mathbf{y}$解密，即计算$x_i = d_K(y_i)$，就可以得到$\mathbf{x} = x_1, x_2, \cdots, x_n$。

内容提要

1 密码体制的数学定义

2 移位密码

3 代换密码

4 仿射密码

5 维吉尼亚密码

6 希尔密码

7 置换密码

模运算

定义2 (模运算)

假设a为整数，m是一个正整数。用m除以a，得到商q和余数r，并确保余数r在0到$m-1$之间，即$a = q \cdot m + r$，其中$0 \leq r \leq m-1$。这一运算可以表示为$a \bmod m = r$，读作“a模m等于r”。特别地，当$r = 0$ 时，我们说“m整除a”。

模运算

定义2 (模运算)

假设a为整数，m是一个正整数。用m除以a，得到商q和余数r，并确保余数r在0到$m-1$之间，即$a = q \cdot m + r$，其中$0 \leq r \leq m-1$。这一运算可以表示为$a \bmod m = r$，读作“a模m等于r”。特别地，当$r = 0$ 时，我们说“m整除a”。

- 例如，计算$101 \bmod 7$，用7除以101得到$101 = 14 \times 7 + 3$。因为$0 \leq 3 \leq 6$，所以$101 \bmod 7 = 3$。

模运算

定义2 (模运算)

假设a为整数，m是一个正整数。用m除以a，得到商q和余数r，并确保余数r在0到$m-1$之间，即$a = q \cdot m + r$，其中$0 \leq r \leq m-1$。这一运算可以表示为$a \bmod m = r$，读作“a模m等于r”。特别地，当$r = 0$ 时，我们说“m整除a”。

- 例如，计算$101 \bmod 7$，用7除以101得到$101 = 14 \times 7 + 3$。因为$0 \leq 3 \leq 6$，所以$101 \bmod 7 = 3$。
- 又例如，计算$(-101) \bmod 7$，可以得到$-101 = (-15) \times 7 + 4$。尽管这并不自然，但是确保了$0 \leq 4 \leq 6$，所以$(-101) \bmod 7 = 4$。

模运算

定义2 (模运算)

假设a为整数，m是一个正整数。用m除以a，得到商q和余数r，并确保余数r在0到$m-1$之间，即$a = q \cdot m + r$，其中$0 \leq r \leq m-1$。这一运算可以表示为$a \bmod m = r$，读作“a模m等于r”。特别地，当$r = 0$ 时，我们说“m整除a”。

- 例如，计算$101 \bmod 7$，用7除以101得到$101 = 14 \times 7 + 3$。因为$0 \leq 3 \leq 6$，所以$101 \bmod 7 = 3$。
- 又例如，计算$(-101) \bmod 7$，可以得到$-101 = (-15) \times 7 + 4$。尽管这并不自然，但是确保了$0 \leq 4 \leq 6$，所以$(-101) \bmod 7 = 4$。
- 一种比较自然的处理方法是，先得到

$$-101 = -(14 \times 7 + 3) = (-14) \times 7 - 3,$$

然后有$(-101) \bmod 7 = (-3) \bmod 7 = (-3) + 7 = 4$。

同余

定义3 (模m同余)

假设a和b均为整数，m是一个正整数。如果$a \bmod m = b \bmod m$，则可以将其表示为

$$a \equiv b \,(\mathrm{mod} m),$$

并读作“a与b模m同余”，即余数相同的意思。

同余

定义3 (模m同余)

假设a和b均为整数，m是一个正整数。如果$a \bmod m = b \bmod m$，则可以将其表示为

$$a \equiv b \,(\mathrm{mod} m),$$

并读作“a与b模m同余”，即余数相同的意思。

一般地，我们用m分别除以a和b，得到相应的商和余数，并且可以确保余数是在0到$m-1$之间的。这样，我们可以把a和b分别表示为

$$a = q_1 m + r_1 \quad 0 \le r_1 \le m-1$$

和

$$b = q_2 m + r_2 \quad 0 \le r_2 \le m-1.$$

显然，$a \equiv b \,(\mathrm{mod} m)$当且仅当$m$整除$b-a$.

集合$\mathbb{Z}_m$

定义4 (集合$\mathbb{Z}_m$)

设m是一个正整数。$\mathbb{Z}_m$定义为整数集合

$$\{0, 1, 2, \cdots, m-1\}.$$

在$\mathbb{Z}_m$中定义两个数学运算，加法$+$和乘法$\times$。它们与普通加法和乘法类似，不同之处只是所得的值总是取除m之后的余数，即模m运算。通常称$\mathbb{Z}_m$为模m的剩余类。

集合$\mathbb{Z}_m$

定义4 (集合$\mathbb{Z}_m$)

设m是一个正整数。$\mathbb{Z}_m$定义为整数集合

$$\{0, 1, 2, \cdots, m-1\}.$$

在$\mathbb{Z}_m$中定义两个数学运算，加法$+$和乘法$\times$。它们与普通加法和乘法类似，不同之处只是所得的值总是取除m之后的余数，即模m运算。通常称$\mathbb{Z}_m$为模m的剩余类。

- 集合$\mathbb{Z}_m$中的加法和乘法满足我们所熟知的许多运算法则，用数学语言说$\mathbb{Z}_m$构成了一个环。

集合$\mathbb{Z}_m$

定义4 (集合$\mathbb{Z}_m$)

设m是一个正整数。$\mathbb{Z}_m$定义为整数集合

$$\{0, 1, 2, \cdots, m-1\}.$$

在$\mathbb{Z}_m$中定义两个数学运算，加法$+$和乘法$\times$。它们与普通加法和乘法类似，不同之处只是所得的值总是取除m之后的余数，即模m运算。通常称$\mathbb{Z}_m$为模m的剩余类。

- 集合$\mathbb{Z}_m$中的加法和乘法满足我们所熟知的许多运算法则，用数学语言说$\mathbb{Z}_m$构成了一个环。
- $\mathbb{Z}_2 = \{0, 1\}$，$\mathbb{Z}_{26} = \{0, 1, 2, \cdots, 25\}$和$\mathbb{Z}_{256} = \{0, 1, 2, \cdots, 255\}$。

移位密码

- 西方的古典密码大多数都是建立在对字母进行操作的基础上。例如，凯撒密码通过按特定顺序移动字母来加密和解密。

移位密码

- 西方的古典密码大多数都是建立在对字母进行操作的基础上。例如，凯撒密码通过按特定顺序移动字母来加密和解密。
- 以英语26个字母为例，从数学角度来看，可以在26个字母和$\mathbb{Z}_{26}$之间建立一一对应。例如，a对0，b对1，c对2，$\cdots$，y对24，z对25。这样一个被称为移位密码的广义凯撒密码就建立了起来。

移位密码

- 西方的古典密码大多数都是建立在对字母进行操作的基础上。例如，凯撒密码通过按特定顺序移动字母来加密和解密。
- 以英语26个字母为例，从数学角度来看，可以在26个字母和$\mathbb{Z}_{26}$之间建立一一对应。例如，a对0，b对1，c对2，$\cdots$，y对24，z对25。这样一个被称为移位密码的广义凯撒密码就建立了起来。

密码体制1 (移位密码)

设$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$。对于$0 \leq K \leq 25$和任意的$x, y \in \mathbb{Z}_{26}$，加密规则定义为

$$e_K(x) = (x + K) \bmod 26.$$

解密规则定义为

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

特别地，如果$K = 3$，则此密码体制通常被称为凯撒密码。

现代计算机中可用的移位密码

- 移位密码只能加密由26个英文字母组成的消息。可否修改移位密码，使之可以用来加密存储在计算机中的任何数字文件？

现代计算机中可用的移位密码

- 移位密码只能加密由26个英文字母组成的消息。可否修改移位密码，使之可以用来加密存储在计算机中的任何数字文件？

密码体制2 (移位密码)

设$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{256}$。对于$0 \leq K \leq 255$和任意的$x, y \in \mathbb{Z}_{256}$，加密规则定义为

$$e_K(x) = (x + K) \bmod 256.$$

解密规则定义为

$$d_K(y) = (y - K) \bmod 256.$$

现代计算机中可用的移位密码

- 移位密码只能加密由26个英文字母组成的消息。可否修改移位密码，使之可以用来加密存储在计算机中的任何数字文件？

密码体制2 (移位密码)

设$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{256}$。对于$0 \leq K \leq 255$和任意的$x, y \in \mathbb{Z}_{256}$，加密规则定义为

$$e_K(x) = (x + K) \bmod 256.$$

解密规则定义为

$$d_K(y) = (y - K) \bmod 256.$$

- 移位密码显然是不安全的，可以用密钥穷尽搜索方法来破译。因为密钥空间太小，只有26或256种可能。敌手穷举所有可能的密钥，如果发现了有意义的明文，那么极有可能是破译成功了。

内容提要

1 密码体制的数学定义

2 移位密码

3 代换密码

4 仿射密码

5 维吉尼亚密码

6 希尔密码

7 置换密码

置换与代换

定义5 (置换与逆置换)

设正整数$m > 2$，集合$\mathcal{S} = \{1, 2, 3, \cdots, m-1, m\}$。$\mathcal{S}$的置换$\pi$定义为

x	1	2	3	$\cdots$	$m-1$	m
$\pi(x)$	i_1	i_2	i_3	$\cdots$	i_{m-1}	i_m

也即$\pi(x) = i_x$，$\pi^{-1}(i_x) = x$，其中，$1 \leq i_1, i_2, \cdots, i_m \leq m$且对于任意两个整数$1 \leq j < k \leq m$ 有$i_j \neq i_k$。关于$\mathcal{S}$的置换π的逆置换π^{-1}可以定义为

x	i_1	i_2	i_3	$\cdots$	i_{m-1}	i_m
$\pi(x)$	1	2	3	$\cdots$	$m-1$	m

其中$i_1, i_2, \cdots, i_m$通常还会按照从小到大的顺序重新排例。

置换与逆置换举例

例1

设集合$\mathcal{S}=\{1,2,3,\cdots,7,8\}$。$\mathcal{S}$的置换$\pi$定义为

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

置换与逆置换举例

例1

设集合$\mathcal{S}=\{1,2,3,\cdots,7,8\}$。$\mathcal{S}$的置换$\pi$定义为

x	1	2	3	4	5	6	7	8
$\pi(x)$	4	1	6	2	7	3	8	5

例2

设集合$\mathcal{S}=\{1,2,3,\cdots,7,8\}$。关于$\mathcal{S}$的置换$\pi$的逆置换$\pi^{-1}$定义为

x	1	2	3	4	5	6	7	8
$\pi(x)$	2	4	6	1	8	3	5	7

对26个字母的置换

例3

设集合$\mathcal{S}=\{a,b,c,\cdots,x,y,z\}$。$\mathcal{S}$的置换$\pi$定义为

x	a	b	c	d	e	f	g	h	i	j	k	l	m
$\pi(x)$	X	N	Y	A	H	P	O	G	Z	Q	W	B	T
x	n	o	p	q	r	s	t	u	v	w	x	y	z
$\pi(x)$	S	F	L	R	C	V	M	U	E	K	J	D	I

这里用大写字母是为了更好地与小写字母区分开来。

代换密码

密码体制3 (代换密码)

设$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$。密钥空间$\mathcal{K}$是由26个数字$0, 1, 2 \cdots, 25$的所有可能的置换组成。对于置换$\pi \in \mathcal{K}$和任意的$x, y \in \mathbb{Z}_{26}$，定义加密规则为

$$e_\pi(x) = \pi(x).$$

解密规则为

$$d_\pi(y) = \pi^{-1}(y).$$

代换密码

密码体制3 (代换密码)

设$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$。密钥空间$\mathcal{K}$是由26个数字$0, 1, 2 \cdots, 25$的所有可能的置换组成。对于置换$\pi \in \mathcal{K}$和任意的$x, y \in \mathbb{Z}_{26}$，定义加密规则为

$$e_\pi(x) = \pi(x).$$

解密规则为

$$d_\pi(y) = \pi^{-1}(y).$$

- 普通计算机运计算量大于等于2^{80}数量级是难以实现。

代换密码

密码体制3 (代换密码)

设$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$。密钥空间$\mathcal{K}$是由26个数字$0, 1, 2 \cdots, 25$的所有可能的置换组成。对于置换$\pi \in \mathcal{K}$和任意的$x, y \in \mathbb{Z}_{26}$，定义加密规则为

$$e_\pi(x) = \pi(x).$$

解密规则为

$$d_\pi(y) = \pi^{-1}(y).$$

- 普通计算机运计算量大于等于2^{80}数量级是难以实现。穷尽26!个代换密钥至少需要执行

$$26! > 4.0 \times 10^{26} > 4.0 \times (2^{3.3})^{26} = 2^{3.3 \times 26 + 2} = 2^{87.8}$$

次运算。所以，利用穷尽密钥搜索的攻击方法攻击代换密码并不有效，甚至是不可行的。

内容提要

1 密码体制的数学定义

2 移位密码

3 代换密码

4 仿射密码

5 维吉尼亚密码

6 希尔密码

7 置换密码

互素

定义6 (最大公因数)

设a和b均为整数。称整数d是a和b的最大公因数，如果d是a和b的公因数，即d既整除a又整除b，并且如果有d'也是a和b的公因数，则一定满足$d' \leq d$。整数d是a和b的最大公因数表示为$\gcd(a,b) = d$。

互素

定义6 (最大公因数)

设a和b均为整数。称整数d是a和b的最大公因数，如果d是a和b的公因数，即d既整除a又整除b，并且如果有d'也是a和b的公因数，则一定满足$d' \leq d$。整数d是a和b的最大公因数表示为$\gcd(a,b) = d$。

定义7 (互素)

设a和b均为正整数，如果a和b之间的最大公因数为1，则称a和b互素，表示为$\gcd(a,b) = 1$。

互素

定义6 (最大公因数)

设a和b均为整数。称整数d是a和b的最大公因数，如果d是a和b的公因数，即d既整除a又整除b，并且如果有d'也是a和b的公因数，则一定满足$d' \leq d$。整数d是a和b的最大公因数表示为$\gcd(a, b) = d$。

定义7 (互素)

设a和b均为正整数，如果a和b之间的最大公因数为1，则称a和b互素，表示为$\gcd(a, b) = 1$。

- 例如，7与13的最大公因数是1，表示为$\gcd(7, 13) = 1$。

互素

定义6 (最大公因数)

设a和b均为整数。称整数d是a和b的最大公因数，如果d是a和b的公因数，即d既整除a又整除b，并且如果有d'也是a和b的公因数，则一定满足$d' \leq d$。整数d是a和b的最大公因数表示为$\gcd(a,b) = d$。

定义7 (互素)

设a和b均为正整数，如果a和b之间的最大公因数为1，则称a和b互素，表示为$\gcd(a,b) = 1$。

- 例如，7与13的最大公因数是1，表示为$\gcd(7,13) = 1$。
- 又例如，13与26的最大公因数是13，表示为$\gcd(13,26) = 13$。这也表明13与26不互素。

$\mathbb{Z}_m$上的乘法逆

- 集合$\mathbb{Z}_m$中有加法和乘法运算，有没有除法运算呢？例如，在$\mathbb{Z}_{26}$中，1除以3等于多少？1能不能除以13呢？

$\mathbb{Z}_m$上的乘法逆

- 集合$\mathbb{Z}_m$中有加法和乘法运算，有没有除法运算呢？例如，在$\mathbb{Z}_{26}$中，1除以3等于多少？1能不能除以13呢？
- 换一种说法，1除以3等于就是3的逆，即3^{-1}。在$\mathbb{Z}_{26}$中，有3^{-1}吗？等于多少？那么13^{-1}呢？

$\mathbb{Z}_m$上的乘法逆

- 集合$\mathbb{Z}_m$中有加法和乘法运算，有没有除法运算呢？例如，在$\mathbb{Z}_{26}$中，1除以3等于多少？1能不能除以13呢？
- 换一种说法，1除以3等于就是3的逆，即3^{-1}。在$\mathbb{Z}_{26}$中，有3^{-1}吗？等于多少？那么13^{-1}呢？

定义8 ($\mathbb{Z}_m$上的乘法逆)

设$a \in \mathbb{Z}_m$。如果存在$a' \in \mathbb{Z}_m$使得

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

则称a'是a在$\mathbb{Z}_m$上的乘法逆，或者称为a'是a模m的乘法逆，并记为$a^{-1} \bmod m$，有时还简记为a^{-1}。

$\mathbb{Z}_m$上的乘法逆

- 集合$\mathbb{Z}_m$中有加法和乘法运算，有没有除法运算呢？例如，在$\mathbb{Z}_{26}$中，1除以3等于多少？1能不能除以13呢？
- 换一种说法，1除以3等于就是3的逆，即3^{-1}。在$\mathbb{Z}_{26}$中，有3^{-1}吗？等于多少？那么13^{-1}呢？

定义8 ($\mathbb{Z}_m$上的乘法逆)

设$a \in \mathbb{Z}_m$。如果存在$a' \in \mathbb{Z}_m$使得

$$aa' \equiv a'a \equiv 1 \,(\mathrm{mod} m),$$

则称a'是a在$\mathbb{Z}_m$上的乘法逆，或者称为a'是a模m的乘法逆，并记为$a^{-1} \,\mathrm{mod} m$，有时还简记为a^{-1}。

- 根据乘法逆的定义，在$\mathbb{Z}_{26}$中，我们来检验，
  $1^{-1} = 1$，$3^{-1} = 9$，$5^{-1} = 21$，$7^{-1} = 15$，$11^{-1} = 19$，
  $17^{-1} = 23$，$25^{-1} = 25$

模$\mathbb{Z}_m$乘法逆的存在性

- 想一想，在$\mathbb{Z}_{26}$中，为什么没有2^{-1}，4^{-1}，6^{-1}，8^{-1} .....?

模$\mathbb{Z}_m$乘法逆的存在性

- 想一想，在$\mathbb{Z}_{26}$中，为什么没有2^{-1}，4^{-1}，6^{-1}，8^{-1} .....?

定理1 (乘法逆的存在性)

$a \in \mathbb{Z}_m$在$\mathbb{Z}_m$上的有乘法逆当且仅当$\gcd(a, m) = 1$。特别地，如果m是素数，则$\mathbb{Z}_m$中的元素除0外都有乘法逆。

- 有了模m乘法逆的概念，就可以考虑$\mathbb{Z}_m$中的除法运算了。例如，设$a, b \in \mathbb{Z}_m$，并且$\gcd(a, m) = 1$。那么在$\mathbb{Z}_m$中，即

$$\frac{b}{a} = b \cdot a^{-1} \bmod m.$$

  需要注意，在$\mathbb{Z}_m$中我们不再用“b除以a”的说法，而习惯上说“b乘以a的逆”。

- 扩展的欧几里得算法可以有效地计算模m的乘法逆。

一次同余方程解的存在性

定理2 (一次方程解的存在性)

设$\mathbb{R}$为全体实数集合。给定$a \in \mathbb{R}$，对于任意的$b \in \mathbb{R}$，一次方程

$$ax = b$$

有唯一解$x \in \mathbb{R}$当且仅当

一次同余方程解的存在性

定理2 (一次方程解的存在性)

设$\mathbb{R}$为全体实数集合。给定$a \in \mathbb{R}$，对于任意的$b \in \mathbb{R}$，一次方程

$$ax = b$$

有唯一解$x \in \mathbb{R}$当且仅当$a \neq 0$，即$x = \frac{b}{a} = b \cdot a^{-1}$。

一次同余方程解的存在性

定理2 (一次方程解的存在性)

设$\mathbb{R}$为全体实数集合。给定$a \in \mathbb{R}$，对于任意的$b \in \mathbb{R}$，一次方程

$$ax = b$$

有唯一解$x \in \mathbb{R}$当且仅当$a \neq 0$，即$x = \frac{b}{a} = b \cdot a^{-1}$。

定理3 (一次同余方程解的存在性)

给定$a \in \mathbb{Z}_m$，对于任意的$b \in \mathbb{Z}_m$，同余方程

$$ax \equiv b \,(\mathrm{mod} m)$$

有唯一解$x \in \mathbb{Z}_m$当且仅当

一次同余方程解的存在性

定理2 (一次方程解的存在性)

设$\mathbb{R}$为全体实数集合。给定$a \in \mathbb{R}$，对于任意的$b \in \mathbb{R}$，一次方程

$$ax = b$$

有唯一解$x \in \mathbb{R}$当且仅当$a \neq 0$，即$x = \frac{b}{a} = b \cdot a^{-1}$。

定理3 (一次同余方程解的存在性)

给定$a \in \mathbb{Z}_m$，对于任意的$b \in \mathbb{Z}_m$，同余方程

$$ax \equiv b \,(\mathrm{mod} m)$$

有唯一解$x \in \mathbb{Z}_m$当且仅当$\gcd(a, m) = 1$，即a和m互素。

仿射密码

密码体制4 (仿射密码)

设$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$。密钥空间$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\}$。对于密钥$K = (a, b) \in \mathcal{K}$和任意的$x, y \in \mathbb{Z}_{26}$，定义加密规则为

$$e_K(x) = (ax + b) \bmod 26,$$

解密规则定义为

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

仿射密码

密码体制4 (仿射密码)

设$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$。密钥空间$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\}$。对于密钥$K = (a, b) \in \mathcal{K}$和任意的$x, y \in \mathbb{Z}_{26}$，定义加密规则为

$$e_K(x) = (ax + b) \bmod 26,$$

解密规则定义为

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

- 仿射密码可以解密成功因为有同余式

仿射密码

密码体制4 (仿射密码)

设$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$。密钥空间$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\}$。对于密钥$K = (a, b) \in \mathcal{K}$和任意的$x, y \in \mathbb{Z}_{26}$，定义加密规则为

$$e_K(x) = (ax + b) \bmod 26,$$

解密规则定义为

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

- 仿射密码可以解密成功因为有同余式

$$d_K(y) \equiv d_K((ax + b)) \equiv a^{-1}(ax + b - b) \equiv a^{-1}ax \equiv x \bmod 26$$

成立。

- 仿射密码所有能的密钥一共有多少个呢？

仿射密码

密码体制4 (仿射密码)

设$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$。密钥空间$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1\}$。对于密钥$K = (a, b) \in \mathcal{K}$和任意的$x, y \in \mathbb{Z}_{26}$，定义加密规则为

$$e_K(x) = (ax + b) \bmod 26,$$

解密规则定义为

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

- 仿射密码可以解密成功因为有同余式

$$d_K(y) \equiv d_K((ax + b)) \equiv a^{-1}(ax + b - b) \equiv a^{-1}ax \equiv x \bmod 26$$

成立。

- 仿射密码所有能的密钥一共有多少个呢？答案是$26 \times 12 = 312$。

Euler函数$\phi(n)$:集合$\mathbb{Z}_n$中所有与n互素的数的个数

Euler函数$\phi(n)$:集合$\mathbb{Z}_n$中所有与n互素的数的个数

定义9 (Euler函数$\phi(n)$)

集合$\mathbb{Z}_n$中所有与n互素的数组成的集合记为$\mathbb{Z}_n^*$。*Euler*函数$\phi(n)$定义为集合$\mathbb{Z}_n$中所有与n互素的数的个数，即$|\mathbb{Z}_n^*| = \phi(n)$。特别地，如果$p$是素数，则$\phi(p) = p - 1$，也即$\mathbb{Z}_p^* = \{1, 2, 3, \cdots, p-1\}$，$|\mathbb{Z}_p^*| = p - 1$。

Euler函数$\phi(n)$:集合$\mathbb{Z}_n$中所有与n互素的数的个数

定义9 (Euler函数$\phi(n)$)

集合$\mathbb{Z}_n$中所有与n互素的数组成的集合记为$\mathbb{Z}_n^*$。*Euler*函数$\phi(n)$定义为集合$\mathbb{Z}_n$中所有与n互素的数的个数，即$|\mathbb{Z}_n^*| = \phi(n)$。特别地，如果$p$是素数，则$\phi(p) = p - 1$，也即$\mathbb{Z}_p^* = \{1, 2, 3, \cdots, p-1\}$，$|\mathbb{Z}_p^*| = p - 1$。

定理4

设$m = \prod_{i=1}^{n} p_i^{e_i}$，其中$p_i$为素数且互不相同，$e_i > 0$。集合$\mathbb{Z}_m$中所有与$m$互素的数的个数为

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

特别地，$m = p \cdot q$，而p和q为素数，则$\phi(n) = \phi(p) \cdot \phi(q)$。

Euler函数$\phi(n)$:集合$\mathbb{Z}_n$中所有与n互素的数的个数

定义9 (Euler函数$\phi(n)$)

集合$\mathbb{Z}_n$中所有与n互素的数组成的集合记为$\mathbb{Z}_n^*$。*Euler*函数$\phi(n)$定义为集合$\mathbb{Z}_n$中所有与n互素的数的个数，即$|\mathbb{Z}_n^*| = \phi(n)$。特别地，如果$p$是素数，则$\phi(p) = p - 1$，也即$\mathbb{Z}_p^* = \{1, 2, 3, \cdots, p-1\}$，$|\mathbb{Z}_p^*| = p - 1$。

定理4

设$m = \prod_{i=1}^{n} p_i^{e_i}$，其中$p_i$为素数且互不相同，$e_i > 0$。集合$\mathbb{Z}_m$中所有与$m$互素的数的个数为

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

特别地，$m = p \cdot q$，而p和q为素数，则$\phi(n) = \phi(p) \cdot \phi(q)$。

- $\mathbb{Z}_{26}$中与26互素的的数的个数为

$$\phi(26) =$$

Euler函数$\phi(n)$:集合$\mathbb{Z}_n$中所有与n互素的数的个数

定义9 (Euler函数$\phi(n)$)

集合$\mathbb{Z}_n$中所有与n互素的数组成的集合记为$\mathbb{Z}_n^*$。*Euler*函数$\phi(n)$定义为集合$\mathbb{Z}_n$中所有与n互素的数的个数，即$|\mathbb{Z}_n^*| = \phi(n)$。特别地，如果$p$是素数，则$\phi(p) = p - 1$，也即$\mathbb{Z}_p^* = \{1, 2, 3, \cdots, p-1\}$，$|\mathbb{Z}_p^*| = p - 1$。

定理4

设$m = \prod_{i=1}^{n} p_i^{e_i}$，其中$p_i$为素数且互不相同，$e_i > 0$。集合$\mathbb{Z}_m$中所有与$m$互素的数的个数为

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

特别地，$m = p \cdot q$，而p和q为素数，则$\phi(n) = \phi(p) \cdot \phi(q)$。

- $\mathbb{Z}_{26}$中与26互素的的数的个数为

$$\phi(26) = \phi(3) \cdot \phi(13) = (2-1) \cdot (12-1) = 12.$$

素数

定义10 (素数与合数)

设整数$p \neq 0, \pm 1$。如果它除了显然因数± 1，$\pm p$以外没有其它的约数，那么，p就称为是不可约数，或素数。如果$a \neq 0, \pm 1$且a不是素数，则a称为合数。一般地，没有特别说明，素数总是指正的。

素数

定义10 (素数与合数)

设整数$p \neq 0, \pm 1$。如果它除了显然因数± 1，$\pm p$以外没有其它的约数，那么，p就称为是不可约数，或素数。如果$a \neq 0, \pm 1$且a不是素数，则a称为合数。一般地，没有特别说明，素数总是指正的。

- 例如，$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$都是素数。

素数

定义10 (素数与合数)

设整数$p \neq 0, \pm 1$。如果它除了显然因数± 1，$\pm p$以外没有其它的约数，那么，p就称为是不可约数，或素数。如果$a \neq 0, \pm 1$且a不是素数，则a称为合数。一般地，没有特别说明，素数总是指正的。

- 例如，$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$都是素数。

定理5 (合数必有素因子)

$a > 1$是合数的充要条件是$a = de$，其中$1 < d < a$且$1 < e < a$。如果a是合数，则必有素数p整除a。

素数

定义10 (素数与合数)

设整数$p \neq 0, \pm 1$。如果它除了显然因数± 1，$\pm p$以外没有其它的约数，那么，p就称为是不可约数，或素数。如果$a \neq 0, \pm 1$且a不是素数，则a称为合数。一般地，没有特别说明，素数总是指正的。

- 例如，$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$都是素数。

定理5 (合数必有素因子)

$a > 1$是合数的充要条件是$a = de$，其中$1 < d < a$且$1 < e < a$。如果a是合数，则必有素数p整除a。

定理6 (素数的个数)

素数有无穷多个。

内容提要

1 密码体制的数学定义

2 移位密码

3 代换密码

4 仿射密码

5 维吉尼亚密码

6 希尔密码

7 置换密码

维吉尼亚密码

密码体制5 (维吉尼亚密码)

设$\mathcal{P}=\mathcal{C}=\mathcal{K}=(\mathbb{Z}_{26})^m$。对于密钥$K=(k_1,k_2,\cdots,k_m)$和任意的

$$x=(x_1,x_2,\cdots,x_m)\in(\mathbb{Z}_{26})^m, y=(y_1,y_2,\cdots,y_m)\in(\mathbb{Z}_{26})^m,$$

定义加密规则为

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

解密规则定义为

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

并且以上运算都在$\mathbb{Z}_{26}$上进行。

维吉尼亚密码

密码体制5 (维吉尼亚密码)

设$\mathcal{P}=\mathcal{C}=\mathcal{K}=(\mathbb{Z}_{26})^m$。对于密钥$K=(k_1,k_2,\cdots,k_m)$和任意的

$$x=(x_1,x_2,\cdots,x_m)\in(\mathbb{Z}_{26})^m, y=(y_1,y_2,\cdots,y_m)\in(\mathbb{Z}_{26})^m,$$

定义加密规则为

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

解密规则定义为

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

并且以上运算都在$\mathbb{Z}_{26}$上进行。

- 维吉尼亚密码是m维向量形式的移位密码。

从单表代换到多表代换

定义11 (单表代换)

一旦密钥被选定，每个字母都被加密规则变换成唯一的密文字母，就好像有唯一的一张事先确定好了的表一样。例如，移位密码、代换密码和仿射密码都是单表代换的密码体制。

定义12 (多表代换)

密钥被选定后，相同字母仍有可能被加密规则变换成不同的密文字母，就好像有多张表一样不断地变换使用。维吉尼亚密码是多表代换的密码体制，一个字母可以被映射为m个字母中的某一个，即有m 种可能。

维吉尼亚密码字母矩阵

Table 3 A Vigenère square.

Plain	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

内容提要

1 密码体制的数学定义

2 移位密码

3 代换密码

4 仿射密码

5 维吉尼亚密码

6 希尔密码

7 置换密码

$\mathbb{Z}_{26}$上向量和矩阵运算

设$\mathbf{x}$是m维的向量，而$\mathbf{K}$是$m \times m$的矩阵。对于任意的

$$\mathbf{x} = (x_1, x_2, \cdots, x_m) \in (\mathbb{Z}_{26})^m,$$

向量$\mathbf{x}$乘以矩阵$\mathbf{K}$得到另一个向量$\mathbf{y} = (y_1, y_2, \cdots, y_m) \in (\mathbb{Z}_{26})^m$，即

$$(y_1, y_2, \cdots, y_m) = (x_1, x_2, \cdots, x_m) \begin{pmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ k_{m1} & k_{m2} & \cdots & k_{mm} \end{pmatrix},$$

并且以上运算都在$\mathbb{Z}_{26}$上进行，可以简单记为

$$\mathbf{y} = \mathbf{x} \cdot \mathbf{K} \bmod 26.$$

逆矩阵

如果先有向量

$$\mathbf{y} = (y_1, y_2, \cdots, y_m) \in (\mathbb{Z}_{26})^m,$$

那么向量$\mathbf{x} = (x_1, x_2, \cdots, x_m) \in (\mathbb{Z}_{26})^m$可以通过向量$\mathbf{y}$乘以矩阵$\mathbf{K}$的逆矩阵$\mathbf{K}^{-1}$的方式得到，即

$$\mathbf{y} \cdot \mathbf{K}^{-1} = \mathbf{x} \cdot \mathbf{K} \cdot \mathbf{K}^{-1} = \mathbf{x} \cdot (\mathbf{K} \cdot \mathbf{K}^{-1}) = \mathbf{x} \cdot \mathbf{I}_m = \mathbf{x} \bmod 26.$$

其中$\mathbf{I}_m$是m阶的单位矩阵。

逆矩阵

如果先有向量

$$\mathbf{y} = (y_1, y_2, \cdots, y_m) \in (\mathbb{Z}_{26})^m,$$

那么向量$\mathbf{x} = (x_1, x_2, \cdots, x_m) \in (\mathbb{Z}_{26})^m$可以通过向量$\mathbf{y}$乘以矩阵$\mathbf{K}$的逆矩阵$\mathbf{K}^{-1}$的方式得到，即

$$\mathbf{y} \cdot \mathbf{K}^{-1} = \mathbf{x} \cdot \mathbf{K} \cdot \mathbf{K}^{-1} = \mathbf{x} \cdot (\mathbf{K} \cdot \mathbf{K}^{-1}) = \mathbf{x} \cdot \mathbf{I}_m = \mathbf{x} \bmod 26.$$

其中$\mathbf{I}_m$是m阶的单位矩阵。

定理7 ($\mathbb{Z}_n$上逆矩阵的存在性)

K是$\mathbb{Z}_n$上的$m \times m$矩阵。存在K的逆矩阵K^{-1}使得$K \cdot K^{-1} = \mathbf{I}_m \bmod n$当且仅当

$$\gcd(\det(K), n) = 1,$$

这里$\det(K)$是矩阵K的行列式。

希尔密码

密码体制6 (希尔密码)

设$\mathcal{P}=\mathcal{C}=(Z_{26})^m$。密钥空间$\mathcal{K}$是定义在$\mathbb{Z}_{26}$上的所有$m\times m$可逆矩阵。对于密钥$\mathbf{K}\in\mathcal{K}$和任意的

$$\mathbf{x}=(x_1,x_2,\cdots,x_m)\in(\mathbb{Z}_{26})^m$$

和

$$\mathbf{y}=(y_1,y_2,\cdots,y_m)\in(\mathbb{Z}_{26})^m,$$

定义加密规则为

$$e_K(\mathbf{x})=\mathbf{x}\cdot\mathbf{K}\,\mathrm{mod}26,$$

解密规则为

$$d_K(\mathbf{y})=\mathbf{y}\cdot\mathbf{K}^{-1}\,\mathrm{mod}26.$$

内容提要

1. 密码体制的数学定义
2. 移位密码
3. 代换密码
4. 仿射密码
5. 维吉尼亚密码
6. 希尔密码
7. 置换密码

置换密码

密码体制7 (置换密码)

设$\mathcal{P}=\mathcal{C}=(Z_{26})^m$，密钥空间$\mathcal{K}$是由$m$个数字$1,2\cdots,m$的所有可能的置换组成。对于置换$\pi\in\mathcal{K}$和任意的$\mathbf{x}=(x_1,x_2,\cdots,x_m)\in(\mathbb{Z}_{26})^m$和$\mathbf{y}=(y_1,y_2,\cdots,y_m)\in(\mathbb{Z}_{26})^m$，定义加密规则为

$$e_\pi(\mathbf{x})=(x_{\pi(1)},x_{\pi(2)},\cdots,x_{\pi(m)}),$$

解密规则为

$$d_\pi(\mathbf{y})=(y_{\pi^{-1}(1)},y_{\pi^{-1}(2)},\cdots,y_{\pi^{-1}(m)}).$$

这里，π^{-1}是π的逆置换。

置换密码

密码体制7 (置换密码)

设$\mathcal{P}=\mathcal{C}=(Z_{26})^m$，密钥空间$\mathcal{K}$是由$m$个数字$1,2\cdots,m$的所有可能的置换组成。对于置换$\pi\in\mathcal{K}$和任意的$\mathbf{x}=(x_1,x_2,\cdots,x_m)\in(\mathbb{Z}_{26})^m$和$\mathbf{y}=(y_1,y_2,\cdots,y_m)\in(\mathbb{Z}_{26})^m$，定义加密规则为

$$e_\pi(\mathbf{x})=(x_{\pi(1)},x_{\pi(2)},\cdots,x_{\pi(m)}),$$

解密规则为

$$d_\pi(\mathbf{y})=(y_{\pi^{-1}(1)},y_{\pi^{-1}(2)},\cdots,y_{\pi^{-1}(m)}).$$

这里，π^{-1}是π的逆置换。

- 代换密码利用置换的结果加密，而置换密码利用置换的方式加密。

置换密码是特殊的希尔密码

例4

考虑课本例*1.7*的置换密码。设集合$\mathcal{S}=\{1,2,3,\cdots,6\}$。其置换$\pi$定义为

x	1	2	3	4	5	6
$\pi(x)$	3	5	1	6	4	2

- 对于此置换π和任意的$\mathbf{x}=(x_1,x_2,x_3,x_4,x_5,x_6)^m$，我们有密文

$$\pi(x)=\mathbf{y}=(y_1,y_2,y_3,y_4,y_5,y_6)=(x_3,x_5,x_1,x_6,x_4,x_2)\in(\mathbb{Z}_{26})^m$$

置换密码是特殊的希尔密码(续)

- 把此置换密码看成是一个希尔密码，那么明文看成是6维向量 $\mathbf{x} = (x_1, x_2, \cdots, x_6) \in (\mathbb{Z}_{26})^m$，而密钥$\pi \in \mathcal{K}$等价于$m \times m$矩阵，

$$
\begin{aligned}
(y_1, y_2, \cdots, y_6) &= (x_1, x_2, \cdots, x_6) \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}. \\
&= (x_3, x_5, x_1, x_6, x_4, x_2)
\end{aligned}
$$

内容提要

1. 密码体制的数学定义
2. 移位密码
3. 代换密码
4. 仿射密码
5. 维吉尼亚密码
6. 希尔密码
7. 置换密码

谢谢！

杜育松
东校园北学院楼三楼(国家保密学院)A304室
15918768869
duyuong@mail.sysu.edu.cn