1.5.1 欧拉函数

- 欧拉函数的通式:

$$\boldsymbol{\Phi}(n)=n\times\left(1-\frac{1}{p_1}\right)\times\left(1-\frac{1}{p_2}\right)\times\ldots\times(1-\frac{1}{p_n})$$

其中$p_1,p_2,\ldots,p_n$是n的所有质因子(也就是通过因式分解可以得到$n=\prod_{i=1}^{s}{p_i}^{k_i}$), n是不为0的整数.

- 备注: 证明略.

1.5.1 欧拉函数

- （两个不同素数的积的欧拉函数值）欧拉函数中假设$n = pq$, 其中p和q是两个不相等的素数, 那么存在以下性质:

$$\Phi(pq) = (p - 1)(q - 1).$$

- RSA将会用到该性质.

1.5.1 欧拉定理

- 【**欧拉定理**】：如果n和a为正整数，且n和a互素(即$\gcd(n,a)=1$)，则存在

$$a^{\Phi(n)} \equiv 1 \ (mod\ n).$$

- 例：假设$n = 12$. 前面例子已经知道$\Phi(12) = 4$，则a是{1, 5, 7, 11}中的任意一个元素都满足上式.
  - $1^{\Phi(12)} \equiv 1 \ (mod\ 12)$.
  - $5^{\Phi(12)} = (24+1)^2 \equiv 1 \ (mod\ 12)$.
  - $7^{\Phi(12)} = (12-5)^4 \equiv 5^4 (mod\ 12) \equiv 1 \ (mod\ 12)$.
  - $11 \equiv -1 \ (mod\ 12)$, 所以$11^{\Phi(12)} = (-1)^4 \equiv 1 (mod\ 12)$.

1.5.1 欧拉定理

- 如果$n = pq$, p和q是两个不相等的素数. 由于$\Phi(n) = (p-1)(q-1)$，那么欧拉定理改写为

$$m^{(p-1)(q-1)} \equiv 1 (mod\ pq)，\text{其中} gcd(m, pq) = 1.$$

- 备注: RSA将会用到.

1.5.1 欧拉定理

- 例:3^{455}的个位数是多少?
- 解:
  - 设3^{455}的个位数为x, 则$3^{455} \equiv x(mod\ 10)$.
  - 由$\Phi(10)=4$. $3^4 \equiv 1(mod\ 10)$, 有 $3^{455} = 3^{4*113+3} \equiv 3^3 \equiv 7(mod\ 10)$.
  - 故3^{455}的个位数是7.

1.5.1 费马小定理

- 【**费马小定理**】：如果p为素数，a是一个不能被p整除的整数，则$a^{p-1} \equiv 1\ (mod\ p)$. 或者$a^{p} \equiv a\ (mod\ p)$.
- 回顾：欧拉定理：$a^{\Phi(n)} \equiv 1\ (mod\ n)$，其中$gcd(a,n) = 1$
- 实际上费马小定理是欧拉定理的一个推论. 费马小定理也将在RSA中具有重要的作用.

- 【**费马大定理**】：对任何正整数a, b, c和n，当n>2时，$a^n + b^n \neq c^n$.

1.5.2 凯撒加密

- 已知的最早使用密码学的人，尤利乌斯.凯撒. 他通过把字母表中的每个字母正向移动三位以加密信息，其中字母表的最后三个字母移到最开始的三个字母. 例如字母A移动变为D，字母X移动变为A. 这就是加密的一个例子，**加密**是对信息进行保密处理的过程.

- **凯撒加密**过程:
  - 首先，将每个字母替换为Z_{26}中的元素，即等于其在字母表中位置减1的0-25之间的一个整数.
  - 加密方法表示为一个函数f，为每个非负整数p，$p<26$，指派集合{0,1,2,...,25}中的一个整数$f(p)$，使得$f(p) = (p + 3) \bmod 26$.
  - 因此，p所代表的原始字母信息用$(p + 3) \bmod 26$所代表的字母替换.

1.5.2 凯撒加密

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

1.5.2 凯撒加密

- 例: 用凯撒加密消息“MEET YOU IN THE PARK”.
- 解:
  - 首先用整数替换消息中的字母:12 4 4 19　24 14 20　8 13　19 7 4　15 0 17 10.
  - 每个整数p替换成$f(p) = (p + 3)$ $\boldsymbol{mod}$ 26, 可得15 7 7 22　1 17 23　11 16 22 10 7　18 3 20 13.
  - 翻译回字母, 则加密后的消息“PHHW BRX LQ WKH SDUN.”

1.5.2 凯撒解密

- 从加密消息中确定原始消息的过程称为**解密**.
- 凯撒解密: 要从凯撒密码加密的消息恢复原消息, 需要用到函数f的逆函数f^{-1}, 逆函数把Z_{26}中的整数p变换为$f^{-1} = (p-3) \bmod 26$. 即要找到原始消息, 每个字母在字母表中反向移到三位, 而字母表的前三位移动到最后三位.

1.5.3 移位密码

- 凯撒密码是**移位密码**中的一种特例. 移位密码通过把每个字母对应的数移动k位, 于是加密函数为$f = (p + k) \bmod 26$, 对应的解密函数为$f^{-1} = (p - k) \bmod 26$. 这里整数$k$称为**密钥**.

- 例: 用密钥k =11的移位密码加密明文消息“STOP GLOBAL WARMING”.
- 解:
  - 首先,将字母翻译成Z_{26}中对应的元素: 18 19 14 15 6 11 14 1 0 11 22 0 17 12 8 13 6.
  - 用加密函数$f(p) = (p + 11) \bmod 26$替换以上每个元素, 得到3 4 25 0 17 22 25 12 11 22 7 11 2 23 19 24 17.
  - 将以上结果翻译回字母, 得到密文“DEZA RWZMLW HLCXTYR.”

1.5.3 移位密码

- 例:解密用密钥$k = 7$的移位密码加密后的消息“LEWLYPLUJL PZ H NYLHA ALHJOLY”.
- 解:
  - 首先, 将加密后的消息翻译成Z_{26}中的元素, 得到 11 4 22 11 24 15 11 20 9 11 15 25 7 13 24 11 7 0 0 11 7 9 14 11 24.
  - 对以上数字移动$-k = -7$ 模26 位, 得到4 23 15 4 17 8 4 13 2 4 8 18 0 6 17 4 0 19 19 4 0 2 7 4 17.
  - 将以上数字翻译回字母得到原始明文“EXPERIENCE IS A GREAT TEACHER.”

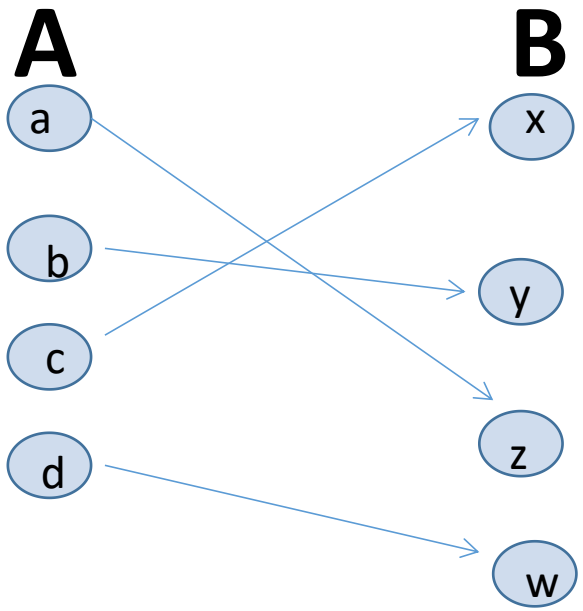
1.5.4 仿射密码

- 移位密码是**仿射密码**中的一种特例. 仿射密码的加密函数表示为 $f(p) = (ap + b) \bmod 26$, 其中a和b是整数, 其选择需保证f是一个双射函数. $f(p)$是一个双射函数, 当且仅当 $gcd(a, 26) = 1$.
- 备注：双射函数, 如果一个函数既是一对一的, 又是映上的.

- 例: 当用$f(p) = (7p + 3) \bmod 26$ 的仿射密码进行加密时, 字母K用什么字母替换?
- 解:K在Z_{26}中对应整数10, $f(10) = (7 \cdot 10 + 3) \bmod 26 = 21$, 那么21对应的字母为$V$, 所以在加密消息时用字母$V$替换字母$K$.

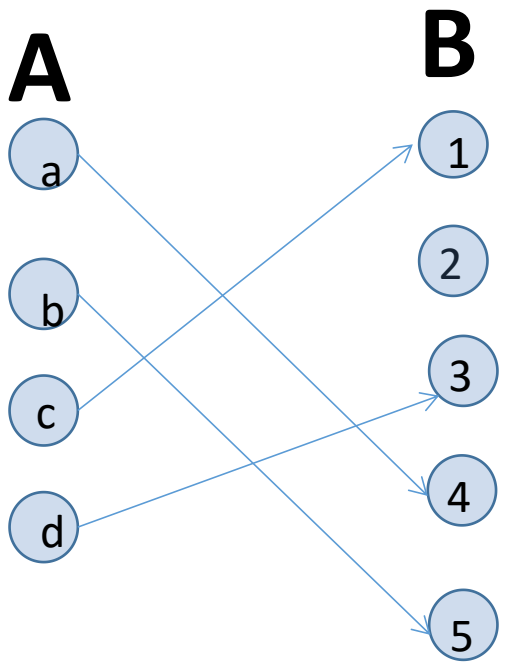
双射(回顾)

- 定义: 函数f是**一一对应**或**双射**函数，如果它既是一对一的，又是映上的. 这样的函数称为双射的.



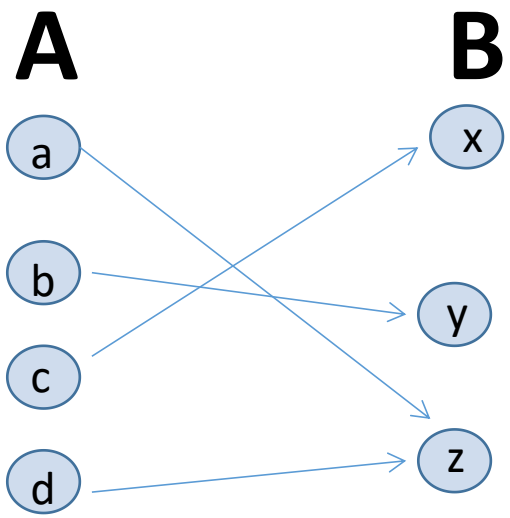
一对一函数(回顾)

- 定义: 函数f称为**单射**函数或**一对一**函数或**内射**函数，当且仅当对于f的定义域中的所有a和b有$f(a)=f(b)$蕴含$a=b$. 一个函数如果是一对一，就称为单射.



映上(回顾)

- 定义: 一个从A到B的函数f称为**映上**或**满射**函数，当且仅当对于每个 $b \in B$有元素 $a \in A$使得 $f(a) = b$



1.5.4 仿射密码

仿射密码的解密:

- 假设$c = (ap + b)\ \boldsymbol{mod}\ 26$, 且满足$gcd(a, 26) = 1$. 为了解密仿射密码, 我们需要知道如何用$c$来表示$p$, 因此采用加密同余方程$c \equiv ap + b\ (mod\ 26)$, 然后求解获得$p$.
  - 为此, 首先两边减去b, 得到$c - b \equiv ap(mod\ 26)$.
  - 因为$\gcd(a, 26) = 1$, 所以一定存在a模26的逆$\bar{a}$存在. 在等式两边乘以$\bar{a}$, 可得$\bar{a}\ (c - b) \equiv \bar{a}ap(mod\ 26)$
  - 因为$\bar{a}a \equiv 1(mod\ 26)$, 说明$\bar{a}\ (c - b) \equiv p(mod\ 26)$
  - 因此$p \equiv \bar{a}\ (c - b)\ (mod\ 26)$. 因为$p$属于$Z_{26}$, 所以就可以确定$p$.

1.5.4 仿射密码

- 例: 解密用$f(p) = (7p + 3) \boldsymbol{mod} 26$的仿射密码进行加密的密文字母$V$.
- 解:明文字母$p \equiv \bar{a}(c - b) (mod\ 26)$. 其中$\bar{a}$表示7模26的逆，所以$\bar{a}$≡15$(mod\ 26)$. 字母$V$对应数字21. 则$c$=21. b为3. 所以p ≡15(21-3) =10$(mod\ 26)$. 翻译回字母以得到明文, 所以我们得到对应的字母为K.

1.5.5 密码分析

- 在不具有加密方法和密钥的情况下从密文中恢复出明文的过程称为**密码分析**或破译密码. 密码分析通常是一个很困难的过程, 特别是不知道加密方法的时候. 这儿, 我们不做一般性的密码分析, 而限定在如何破译用移位密码加密的消息.
- 对移位密码加密的密文分析的主要工具是利用密文中字母频率的统计. 英语中最常用的9个字母以及其大概的相对概率为E 13%, T 9%, A 8%, O 8%, I 7%, N 7%, S 7%, H 6%, R 6%. 因此破译过程如下:
  - 首先, 找出密文中字母的相对频率, 并按照频率对密文中最常出现的字母排序
  - 假设最常出现的字母由E加密生成. 然后, 根据假设确定移位的值.
  - 确定k值后, 将密文移-k位后查看密文是否有含义.
  - 如果没有含义, 接下来考虑密文中最常出现的字母由T加密生成, 循环以上过程.

1.5.5 密码分析

- 例: 获取到密文“ZNK KGXRE HOXJ MKZY ZNK CUXS”，已知它是用移位密码加密的. 原始的明文消息是什么?
- 解:密文中最常出现的字母是K. 所以假设移位密码将明文字母E移位到了密文字母K. 那么10=4+k $\boldsymbol{mod}$ 26, 可知k=6. 根据K的值, 我们将密文解密可得消息 “THE EARLY BIRD GETS THE WORM.”因为这个消息是有意义的, 所以我们认为k=6的假设是正确的.

1.5.6 分组密码

- 移位密码和仿射密码中都是用字母表中的一个字母来替换另一个字母, 因此这些密码称为字符或**单码密码**.

- 单码密码通过字母频率分析很容易被破译. 因此, 通过用一组字母替换另一组字母的方式(而不是单个字母替换另一个字母)可以强化成功破译密文的难度, 这类密码称为**分组密码**.

1.5.7 换位密码

- 在分组密码中，一种简单的密码叫做**换位密码**(或称置换密码). 用密钥的集合是{1,2,…,m}上的一个置换σ，即从{1,2,…,m}到{1,2,…,m}的一个一对一函数，这里m是正整数.
- 备注: σ国际音标/ ‘sɪgmə/. 换位密码是把明文中各字符的位置次序重新排列来得到密文的一种密码体制.
- 换位密码加密: 首先将消息分为大小为m的分组. 其中，消息中的字母数不能被m整除时，可以在结尾加上一些随机的字母填充来构成最后一个分组. 将分组$p_1p_2…p_m$通过置换σ操作加密为$c_1c_2…c_m$.
- 换位密码解密: 用σ的逆σ^{-1}置换对$c_1c_2…c_m$进行换位.

1.5.7 换位密码

- 例: 利用基于集合{1,2,3,4} 上的置换σ的换位密码, 其中σ(1) = 3, σ(2) = 1, σ(3) = 4, σ(4) = 2,
  - (a)加密明文消息 “PIRATE ATTACK”
  - (b)解密密文消息 “SWUE TRAEOEHS”
- 解:
  - (a)将明文根据m=4, 划分为4个字母为一组PIRA TEAT TACK. 把第一个字母移动到第三位, 第二个字母移动到第一位, 第三个字母移动到第四位, 第四个字母移动到第二位, 得到IAPR ETTA AKTC.
  - (b)σ的逆置换 σ^{-1} : $\sigma^{-1}(1) = 2$, $\sigma^{-1}(2) = 4$, $\sigma^{-1}(3) = 1$, $\sigma^{-1}(4) = 3$. 对每个分组SWUE TRAE OEHS应用$\sigma^{-1}(m)$, 可得明文USEW ATER HOSE, 将这些字母重新分组形成常见词汇, 猜测明文消息是USE WATER HOSE.

1.5.8 维吉利亚密码

- **维吉利亚(Vigenere)密码**(或称维吉尼亚密码, 维热纳尔密码)是一种用一段字母来代替另外一段字母的分组密码. 维吉利亚密码是由一些偏移量不同的凯撒密码组成, 它使用一系列凯撒密码组成密码字母表的加密算法.
- 维吉利亚密码首先将明文分为若干段，每段有n个数字，密钥$k=k_1k_2...k_n$.
  - 加密算法$E(m_1m_2...m_n)=c_1c_2...c_n$, 其中$c_i = (m_i+k_i)$ **mod** 26， m_1= 0, 1, 2, ..., 25. $i = 1, 2, ..., n$.
  - 解密的过程则与加密相反. $m_i = (c_i - k_i)$ **mod** 26

1.5.8 维吉利亚密码

- 例: 维吉尼亚密码加密明文I ‘ve got it. 其中使用密钥为ok. 该例子下加密分为1段, 非字母被忽略. 密钥不足则重复补全.
- 解:
  - 密钥长度需要与明文长度相同，如果少于明文长度，则重复拼接直到相同. 本例中明文长度为8个字母(非字母均被忽略)，密钥会被补全为“okokokok”. 因此$E(m_1m_2...m_8)=c_1c_2...c_8$, 其中$c_i = (m_i+k_i)$ **mod** 26， k_1= 14, k_2= 10, ...
  - 可得最终密文为W'fs qcd wd.

1.5.9 密码系统

- 定义: 一个**密码系统**是一个五元组(P, C, K, E, D), 其中P明文串的集合, C是密文串的集合, K是密钥空间(所有可能的密钥的集合), E是加密函数的集合, D是解密函数的集合.
- 我们用E_k表示在E中相对于秘钥k的加密函数, D_k是D中用来解密由E_k加密的密文的解密函数, 即对于所有明文串p有$D_k(E_k(p)) = p$.

1.5.9 密码系统

- 例: 将移位密码系列描述为一个密码系统.
- 解:假设字母串都是Z_{26}中的元素. 密码系统(P, C, K, E, D)中
  - P是Z_{26}中的元素串的集合,
  - C是Z_{26}中的元素串的集合,
  - K是所有可能的移位,所以$K = Z_{26}$,
  - E有所有这样的函数$E_k(p) = (p + k)$ **mod** 26构成
  - D和加密函数一样, 其中$D_k(p) = (p - k)$ **mod** 26.

1.5.10 公钥密码

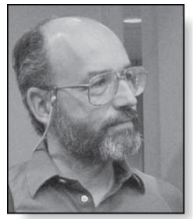
- 所有的古典密码, 包括移位密码和仿射密码都是**私钥密码系统**. 私钥密码系统中一旦知道密钥, 那就能够很快破译. 通信的双方都共享同一密钥, 所以安全通信的双方需要安全地交互该密钥.

- 20世纪70年代, **公钥密码系统**被发明, 发送加密消息的人并不能解密消息, 每个人都可以有一个众所周知的加密密钥(简称加密公钥, 或公钥), 只有解密密钥是保密的(简称私钥), 而且只有消息的接受人能解密消息.

1.5.11 RSA密码系统

- **RSA**是一个非常出名的公钥密码系统,1976年被MIT的三位科学家.

Ronald Rivest
(Born 1948)



Adi Shamir
(Born 1952)

Leonard Adelman
(Born 1945)

- RSA理论基础是费马小定理，其安全性依赖于大整数因数分解的困难性. 三位学者因在密码学和信息安全方面的这一突出工作获2002年图灵奖.
- 实际上,1973年RSA系统在英国政府的秘密研究中已经被Clifford Cocks发现.

Clifford Cocks
(Born 1950)

1.5.11 RSA密码系统

- RSA是一种分组密码, 加密密钥(或称公共密钥)为(n, e), 其中$n = pq$是一个由两个大素数, 比如各有300位数字的p和q的乘积构成的模数, e是与$(p-1)(q-1)$互素的指数.
- 要生成这样的加密密钥, 需要找到两个大素数. 比如$n = pq$大约有600位数字, 目前不可能在合理时间内被因子分解, 因此没有单独的解密密钥不可能迅速解密.

1.5.11 RSA加密

- RSA中, 用公共密钥(n, e)**加密过程**：
  - 首先, 将明文消息M翻译成整数序列. 其中, 每个明文字母翻译成两位数, 如A翻译成00, B翻译成01,....J翻译成09.
  - 然后, 将这些两位数连接起来构成数字串.
  - 将这个数字串分为$2N$位数字等长的分组, 这里$2N$是一个大偶数使得$2N$位数字的整数2525...25不超过n. 其中, 必要时在明文消息最后填充无意义的X使得最后一组的大小和其他分组一样.
    - 【举例: n=2537, 则2525 < 2537 < 252525, 所以划分为4位等长的分组】
  - 到此, 明文消息M翻译成了一个整数序列$m_1, m_2,..., m_k$, 其中k为整数.
  - 然后, 将每个分组m_i转换成密文分组c_i, 其转换由函数$C = M^e \bmod n$实现.
  - 加密以后的消息依然是数的分组形式, 并发送给接受者.