密码学二级

分级通关系列教程

古典密码

- 单表代换密码

加密：

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

解密：

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

古典密码

- 维吉利亚密码（多表代换）

英文中a~z，由0~25表示。

假设串长为m，明文为P，密文为C，密钥为K则

$$C = (P_1 + K_1, P_2 + K_2, \ldots, P_m + K_m) mod 26$$

$$P = (C_1 - K_1, C_2 - K_2, \ldots, C_m - K_m) mod 26$$

例如，假设明文为：$ILOVEMIMAXUE$，密钥为：$AWSL$

则密文为：$IHGGEIAXATMP$。

（密钥若长度不够可以继续重复，例如 $AWSLAWSLAWSL$）

古典密码

- Hill密码

- $$(c1, c2, c3) = (x1, x2, x3)\begin{pmatrix} k11 & k12 & k13 \\ k21 & k22 & k23 \\ k31 & k32 & k33 \end{pmatrix}(mod\ 26)$$

自然语言判断

http://practicalcryptography.com/cryptanalysis/text-characterisation/quadgrams/

- 基本思想

  If the text looks very similar to English (or another language), we consider the key to be a good one.

- 四字母词

  - *ATTACK* ⇒*ATTA*, *TTAC*, and *TACK*

- 统计词频/训练

$$p(\mathrm{ATTA}) = \frac{\mathrm{count}(\mathrm{ATTA})}{N}$$

Quadgram	Count	Log Probability
AAAA	1	-6.40018764963
QKPC	0	-9.40018764963
YOUR	1132	-3.34634122278
TION	4694	-2.72864456437
ATTA	359	-3.84509320105

- 计算一段文字概率

$$p(\mathrm{ATTACK}) = p(\mathrm{ATTA}) \times p(\mathrm{TTAC}) \times p(\mathrm{TACK})$$

$$\log\left(p(\mathrm{ATTACK})\right) = \log\left(p(\mathrm{ATTA})\right) + \log\left(p(\mathrm{TTAC})\right) + \log\left(p(\mathrm{TACK})\right)$$

- 原理
  - 在长度相同的情况下，概率对数越大（绝对值越小），与自然语言越接近

背包加密

- 背包加密算法（根据文档自学）
- 求解问题(0，1背包)

已知一背包加密的公钥为
{615436700291,415460700271,15508700231,846430100773,677471501215,139578302079,179168604148,789306608798,563224517265,364498233536,229056467022,670323428329,115934481316,44989786476,518624653302,149955258190,728568829281,796899516776,546782575075,178164449829,356328899658,712657799316,569303048254,223205396187,446410792374,892821584748,524144817108,132888933895,611875519857,877653387647,839906074973,357743530 74}，密文为 6020587936087，试求明文二进制表示。

求公钥中，哪些整数相加的和恰好等于密文6020587936087

格和LLL算法

首先介绍格(Lattice)的概念，设 $B=\{\beta_0,\beta_1,\cdots,\beta_{m-1}\}$ 是实向量空间 $\mathbb{R}^{n+1}$ 的一组线性无关的向量，那么由 B 形成的格定义为 $L(B)=\{\sum_{i=0}^{m-1}v_i\beta_i \mid v_i\in\mathbb{Z}\}$。设向量 $\beta=(r_0,r_1,\cdots,r_n)$，其长度用欧氏范数 $\|\beta\|=\sqrt{\sum_{i=0}^{n}r_i^2}$ 来表示，LLL 算法输入向量组 B，可以在多项式时间内，在 $L(B)$ 中找到一组长度“最短“，接近正交的另外一组 m 个线性无关的向量组 B'。

格和LLL算法

设背包加密的公钥为 $pk=(b_0,b_1,\cdots,b_{n-1})$，密文为 $c=\sum_{i=0}^{n-1}b_iv_i$，下面求向量 v。

构造矩阵 $A=\begin{pmatrix}1&0&\cdots&0&0\\0&1&\cdots&0&0\\\cdots&\cdots&\cdots&\cdots&\cdots\\0&0&\cdots&1&0\\b_0&b_1&\cdots&b_{n-1}&-c\end{pmatrix}$，那么 $A\begin{pmatrix}v_0\\v_1\\\cdots\\v_{n-1}\\1\end{pmatrix}=\begin{pmatrix}v_0\\v_1\\\cdots\\v_{n-1}\\0\end{pmatrix}$，

设矩阵 A 的列向量为 $\beta_0,\beta_1,\cdots,\beta_n$，如果 $c\neq 0$，那么它们是 $n+1$ 个线性无关的向量，可以看成是实向量空间 $\mathbb{R}^{n+1}$ 的一组基底，$(v_0,v_1,\cdots,v_{n-1},0)^T=v_0\beta_0+v_1\beta_1+\cdots+v_{n-1}\beta_{n-1}+\beta_n$，

所以 $(v_0,v_1,\cdots,v_{n-1},0)^T\in L(A)$。又因为 $(v_0,v_1,\cdots,v_{n-1},0)^T$ 的每一项为 0 或者 1，所以其长度较小，通过在 $\beta_0,\beta_1,\cdots,\beta_n$ 上运用 LLL 算法，会生成一组新的“最短”的基底，可能在新的基底中出现 $(v_0,v_1,\cdots,v_{n-1},0)^T$，从而得到背包问题的解 v。