现代密码学 第二章

2.3. (a) 证明仿射密码具有完善保密性. 如果每个密钥的概率都是 $1/312$

$y = ax + b \quad k = (a, b)$

证明:

~~$\Pr(Y=y) = \sum_{\{k:\, y \in (k)\}} \Pr(k=k)\Pr(X = d_k(y))$~~

~~$X = a^{-1}$~~

~~$= \frac{1}{312} \sum_{k} \Pr(X = d_k(y))$~~

$$\Pr(Y=y) = \sum_{(a,b)} \Pr(k=(a,b))\ \Pr(X = d_k(y))$$

$$= \frac{1}{312} \sum_{(a,b)\in Z_{26}^2} \Pr(X = a^{-1}(y-b))$$

$y - b \in Z_{26}$. $X = a^{-1}(y-b)$ 可求出 $X = a^{-1}y$, 对于 $\forall a^{-1}$.

~~对于每个 y. 所有 (a,b) 组合会使 x 在所有值域出现~~

~~(一定不等于)~~

~~假设 x 的每种情况都在 Z_{26}.~~

$a^{-1}y$ 均为 Z_{26} 上的置换. 即 $\forall \Pr(X \in Z_{26}) = 1$

$$= \frac{1}{312} \cdot 12 = \frac{1}{26}$$

$$\Pr(y|x) = \Pr(y = ax + b) = \frac{12}{312 \cdot 26} = \frac{1}{26}$$ (在 312 种 a,b 中找出使 ~~$x = x$ 且 $y = y$~~ 的 (a,b))

令程 $y = ax + b$ 的解 $\begin{cases} a = 1 + t \\ b = y + xt - x \end{cases}$ $t \in Z$.)

使用贝叶斯公式: $\Pr(x|y) = \frac{P(x)P(y|x)}{P(y)} = \frac{\frac{1}{26} \cdot P(x)}{\frac{1}{26}} = \Pr(x)$.

(b). 假设在 $\{a \in Z_{26} : \gcd(a, 26) = 1\}$ 给定一概率分布. 假设仿射密码的每个密钥 (a,b) 的概率为 $P(a)/26$; 证明当这个概率分布定义在密钥空间上时. 仿射密码具有完善保密性.

证明:

$$\Pr(Y=y) = \sum_{(a,b)\in Z_{26}^2} P(k=(a,b))\ P(X = d_k(y))$$

$$= \sum_{(a,b)\in Z_{26}^2} \frac{P(a)}{26} \cdot P(X = a^{-1}(y-b))$$

$$= \sum_{a \in Z_{26}^{*}} \left(\sum_{b \in Z_{26}} \frac{P(a)}{26} \cdot P(X = a^{-1}(y-b)) \right)$$

$$= \sum_{a \in Z_{26}^{*}} \frac{P(a)}{26} \left(\sum_{b \in Z_{26}} P(X = a^{-1}(y-b)) \right)$$

$$= \sum_{a \in Z_{26}^{*}} \frac{P(a)}{26} \cdot 1$$

$$= \frac{1}{26} \sum_{a \in Z_{26}^{*}} P(a) = \frac{1}{26}$$

$$\Pr(Y=y | X=x) = P(y = ax + b).$$

$y = ax + b \quad (x, y \in Z_{26})$

$a_0 = 1. \quad b_0 = y - x$

$$\therefore \begin{cases} a = 1 + t \\ b = y - x + xt \end{cases}, \quad t \in Z$$

$\because a$ 共有 12 个

$\therefore$ 这样 (a,b) 也对应有 12 组

$$P(y|x) = \sum_{a \in Z_{26}^{*}} P(a) \cdot \frac{1}{26} = \frac{1}{26}$$

~~Z_{26} 都要~~

$$\therefore P(x|y) = \frac{P(x)P(y|x)}{P(y)} = \frac{\frac{1}{26}P(x)}{\frac{1}{26}} = P(x)$$

$\therefore$ 得证