Fundamentals Of Information Science **2022 Spring**

Homework9

学生: 华园(202000120027)) *时间: 2022.3.23*

Problem 1.

multiplicative one-time pad
We may also define a "multiplication mod p" variation of the one-time pad. This is a cipher $\mathcal{E} = (E, D)$, defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, where $\mathcal{K} := \mathcal{M} := \mathcal{C} := \{1, \ldots, p-1\}$, where p is a prime. Encryption and decryption are defined as follows:

$$E(k, m) := k \cdot m \bmod p \quad D(k, c) := k^{-1} \cdot c \bmod p.$$

Here, k^{-1} denotes the multiplicative inverse of k modulo p. Verify the correctness/ property for this cipher and prove that it is perfectly secure.

Solution.

(1)为了验证其正确性,我们仅需要验证D(k,E(k,m))=m,因此我们可以获得

$$\begin{aligned} E(k,m) &= k \cdot m \ mod \ p \\ D(k,E(k,m)) &= k^{-1} \cdot (k \cdot m \ mod \ p) mod \ p \\ &= m \end{aligned}$$

因此我们可以验证其正确性。(2)为了证明是否绝对安全,我们需要验证每个不同的信息被加密成同一密文的概率相同,由于mod乘除运算的特殊性,以及k的等概率分布,我们只需要证明针对不同的m,有且仅有1个k使得m被加密为c. 由于k • m mod p=c,则可以表示为

$$k \cdot m = c + np, (n >= 0)$$

之后的讨论我们只针对一位进行讨论,k<p,则我们一定可以获得的是

$$0 <= n <= m - 1$$

,由于k<p,则有

$$m \cdot p > c + np$$

,c+np mod m=k • m mod m=0,那么我们可以证明对于任意一个信息m_i都有一个整数$k = \frac{c+np}{m_i}$,使得m_i被加密为c,且其余满足条件的k值为$k = \frac{c+(n+dm_i)p}{m_i}$,均不在范围内,因此可以证明k的唯一性,由于k的等概率性,从而我们可以证明这种加密方式是绝对安全的。
经过查阅相关材料,获得乘法逆元又称数论倒数。若且a,m互质,则x为a的逆元,记为,若a,m不互质,则不存在逆元。当且仅当m为素数时,a有唯一的乘法逆元。在此题目中,P与k互质,且k^{-1}为k的逆元,因此我们可以确定,针对任意一个m_i均有唯一一个k使得m_i被加密为C,因此我们可以获得

$$Pr[E(k,m) = c] = constant$$

从而可以证明该加密方法是绝对安全的。

Problem 2.

Truncating PRFs
Let F be a PRF whose range is $\mathcal{Y} = \{0,1\}^n$. For some $\ell < n$ consider the PRF F' with a range $\mathcal{Y}' = \{0,1\}^\ell$ defined as: $F'(k,x) = F(k,x)[0 \ldots \ell]$. That is, we truncate the output of $F(k,x)$ to the first ℓ bits. Show that if F is a secure PRF then so is F'.

Solution.

倘若F是安全的PRF，那么可以获得F(k,x)与f（x）无法区分，也就是说从K中随机选取一个k与从所有函数中随机选取一个函数是无法区分的，针对n位无法区分，则针对其前l位，同样无法进行区分，因此F’也是安全的。

Problem 3.

Chain encryption
Let $\mathcal{E} = (E, D)$ be a perfectly secure cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ where $\mathcal{K} = \mathcal{M}$. Let $\mathcal{E}' = (E', D')$ be a cipher where encryption is defined as $E'\left(\left(k_1, k_2\right), m\right) := \left(E\left(k_1, k_2\right), E\left(k_2, m\right)\right)$. Show that $\mathcal{E}'$ is perfectly secure.

Solution.

根据绝对安全的定义，我们可以假设：

$$\forall m_0, m_1 \in M \text{ and } \forall c \in C$$

由于（E,D）是绝对安全的，因此

$$Pr[E(k_2, m_0) = c_1] = Pr[E(k_2, m_1) = c_1]$$

$$Pr[E(k_1, k_2) = c_2] = Pr[E(k_1, k_3) = c_2]$$

也就是说对于$E[k_1, k_2]$ $E[k_2, m]$两者均为安全加密，从而两者的分布确定，因此可知：

$$Pr[E'((k_1, k_2), m_0) = c] = Pr[E'((k_1, k_2), m_1) = c]$$

从而可以判断$E'((k_1, k_2), m)$是绝对安全的。