应用密码学第三次作业解答

1. 考虑一个密码体制 $M=\{a,b,c\}$，$K=\{k_1,k_2,k_3\}$和 $C=\{1,2,3,4\}$。假设加密矩阵为

	a	b	c
k_1	2	3	4
k_2	3	4	1
k_3	1	2	3

已知密钥概率分布为：$p(k_1)=1/2$，$p(k_2)=p(k_3)=1/4$，且明文概率分布为 $p(a)=1/3$，$p(b)=8/15$，$p(c)=2/15$，计算 $H(M)$，$H(K)$，$H(C)$，$H(M|C)$，$H(K|C)$.

解： 计算密文的概率分布、明密文的联合分布、密钥密文的联合分布，利用熵的定义和条件熵的性质计算。

$$H(M)\approx 1.4;\ H(K)=1.5;\ H(C)\approx 1.88;\ H(M|C)\approx 1.02;\ H(K|C)\approx 1.02$$

提醒：注意条件熵的定义，不要想当然

2. 考虑一个密码系统(P,C,K,E,D)。

a) 说明为什么 $H(P,K)=H(C,P,K)=H(P)+H(K)$。

b) 假设这个系统具有完全保密。证明 $H(C,P)=H(C)+H(P)$和 $H(C)=H(K)-H(K|C,P)$。

c) 假设这个系统有完全保密，并且对每一个明文密文对，最多只有一个相应的密钥能够加密。证明 $H(C)=H(K)$。

(1) 在密码系统中，我们通常假设明文与密钥的概率分布是相互独立的，并且明文、密钥确定了密文，因此有此关系式；

(2) **证明：** 对完善保密系统，明文和密文的概率分布是相互独立的，因此有$H(C,P)=H(C)+H(P)$。另一方面，由于

$$\begin{aligned} H(K,C,P) &= H(K|C,P)+H(C,P)=H(K|C,P)+H(C)+H(P) \\ &= H(C|K,P)+H(K,P)=H(K)+H(P) \\ & \quad (\text{this is because } \ H(C|K,P)=0) \end{aligned}$$

由此即得要证明的关系式。

(3) **证明：** 对完善保密系统，每一个明文密文对最多只有一个相应的密钥能够加密，说明明密文给定的情况下密钥是确定的，因此$H(K|C,P)=0$。根据上题的等式即得结论。□

3. 假设 S_1 是移位密码（密钥等概率），S_2 是密钥满足概率分布 P_k（不必是等概率的）的移位密码。证明 $S_1*S_2=S_1$ (这里用等号不一定准确，请思考什么叫相等或等价，给出你的定义并证明之)。

分析： 这里*是指乘积密码，显然“=”的定义不是指两个加密变换完全一样，因为对给定的明文m，用S_1*S_2和S_1使用同样的密钥加密得到的密文是不一定相同的。但是，S_1*S_2和S_1都仍然是移位密码，我们可以考察两个加密变换的效果：只要对同样的明文概率分布，两种加密方式所得密文的概率分布也相同，并且都是完善保密的，我们便可以说他们是一样的或等价的。所以可以从这个角度去证明。

对S_1，我们知道其密文是均匀分布的，并且它是完善保密的。

对$S_1 * S_2$，考虑明密文分别为x, y，我们有

$$\begin{aligned} p(y) &= \sum_{k_1,k_2} p(k_2)p(k_1)p(x = y - k_1 - k_2) \\ &= \frac{1}{26}\sum_{k_2} p(k_2)\sum_{k_1} p(x = y - k_1 - k_2) \\ &= \frac{1}{26}. \\ & \quad (\text{this is because } \sum_{k_1} p(x = y - k_1 - k_2) = 1, \sum_{k_2} p(k_2) = 1) \end{aligned}$$

另一方面，

$$\begin{aligned} p(y|x) &= \sum_{k_1,k_2} p(k_2 + k_1 = y - x) = \sum_{k_2} p(k_2)p(k_1 = y - x - k_2) \\ &= \frac{1}{26}\sum_{k_2} p(k_2) = \frac{1}{26}. \end{aligned}$$

根据贝叶斯公式可得$p(x|y) = p(x)$。从而$S_1 * S_2$也是完善保密的。□

本题没有标准答案，主要想让大家思考从信息论的角度怎样理解密码系统。作业中大部分同学直接证明$S_2 * S_1$的密钥概率分布也是均匀分布，这样论述并不是太完整，因为$S_2 * S_1$、S_1都是密码系统，两个密码系统的等价关系应该综合明文、密文、密钥的概率分布来定义。