应用密码学作业 #2

XXX：202XX80XXXXXXXX

2023 年 4 月 14 日

信息熵的计算

(1)

$$H(M)=\sum_{i=1}^{3}p(m_i)I(m_i)=-(\frac{1}{3}\log_2\frac{1}{3}+\frac{8}{15}\log_2\frac{8}{15}+\frac{2}{15}\log_2\frac{2}{15})=1.40$$

(2)

$$H(K)=\sum_{i=1}^{3}p(k_i)I(k_i)=-(\frac{1}{4}\log_2\frac{1}{4}+\frac{1}{2}\log_2\frac{1}{2}+\frac{1}{4}\log_2\frac{1}{4})=\frac{3}{2}=1.5$$

(3)

$$p(c=1)=p(m=a)p(k=k_3)+p(m=c)p(k=k_2)=\frac{1}{3}\frac{1}{4}+\frac{2}{15}\frac{1}{4}=\frac{7}{60}$$

$$p(c=2)=p(m=a)p(k=k_1)+p(m=b)p(k=k_3)=\frac{1}{3}\frac{1}{2}+\frac{8}{15}\frac{1}{4}=\frac{3}{10}$$

$$p(c=3)=p(m=a)p(k=k_2)+p(m=b)p(k=k_1)+p(m=c)p(k=k_3)=\frac{1}{3}\frac{1}{4}+\frac{8}{15}\frac{1}{2}+\frac{2}{15}\frac{1}{4}=\frac{23}{60}$$

$$p(c=4)=p(m=b)p(k=k_2)+p(m=c)p(k=k_1)=\frac{8}{15}\frac{1}{4}+\frac{2}{15}\frac{1}{2}=\frac{1}{5}$$

$$H(C)=\sum_{i=0}^{4}p(c_i)I(c_i)=-(\frac{7}{60}\log_2\frac{7}{60}+\frac{3}{10}\log_2\frac{3}{10}+\frac{23}{60}\log_2\frac{23}{60}+\frac{1}{5}\log_2\frac{1}{5})=1.877$$

(4) 联合概率、条件概率表如下：

$p(m_i,c_j)$	1	2	3	4
a	$\frac{1}{12}$	$\frac{1}{6}$	$\frac{1}{12}$	0
b	0	$\frac{2}{15}$	$\frac{4}{15}$	$\frac{2}{15}$
c	$\frac{1}{30}$	0	$\frac{1}{30}$	$\frac{1}{15}$

$p(m_i\|c_j)$	1	2	3	4
a	$\frac{5}{7}$	$\frac{5}{9}$	$\frac{5}{23}$	0
b	0	$\frac{4}{9}$	$\frac{16}{23}$	$\frac{2}{3}$
c	$\frac{2}{7}$	0	$\frac{2}{23}$	$\frac{1}{3}$

$$H(M|C)=\sum_{i,j}p(m_i,c_j)I(m_i|c_i)=-(\frac{1}{12}\log_2\frac{5}{7}+\frac{1}{6}\log_2\frac{5}{9}+\frac{1}{12}\log_2\frac{5}{23}+$$

$$\frac{2}{15}\log_2\frac{4}{9}+\frac{4}{15}\log_2\frac{16}{23}+\frac{2}{15}\log_2\frac{2}{3}+\frac{1}{30}\log_2\frac{2}{7}+\frac{1}{30}\log_2\frac{2}{23}+\frac{1}{15}\log_2\frac{1}{3})=1.022$$

(5) 联合概率、条件概率表如下：

$p(k_i, c_j)$	1	2	3	4
k_1	0	$\frac{1}{6}$	$\frac{4}{15}$	$\frac{1}{15}$
k_2	$\frac{1}{30}$	0	$\frac{1}{12}$	$\frac{2}{15}$
k_3	$\frac{1}{12}$	$\frac{2}{15}$	$\frac{1}{30}$	0

$p(k_i \mid c_j)$	1	2	3	4
k_1	0	$\frac{5}{9}$	$\frac{16}{23}$	$\frac{1}{3}$
k_2	$\frac{2}{7}$	0	$\frac{5}{23}$	$\frac{2}{3}$
k_3	$\frac{5}{7}$	$\frac{4}{9}$	$\frac{2}{23}$	0

$$H(K|C) = \sum_{i,j} p(k_i, c_j) I(k_i|c_i) = 1.022$$

第二题

(a)

$$\because H(C, P, K) = H(P, K) + H(C|P, K)$$

其中 $H(C|P, K)$ 表示已知明文和密钥之后，密文还保留的信息量，此时密文还有的信息量为零，故 $H(C|P, K) = 0$

$$\therefore H(C, P, K) = H(P, K)$$

又因为密码系统中明文和密文的分布是独立的,所以 $H(P, K) = H(P) + H(K)$ 故

$$H(P, K) = H(C, P, K) = H(P) + H(K)$$

(b) (1) $\because H(C, P) = H(P|C) + H(C)$, 又 $\because$ 在完善保密系统中，密文不会透露出明文的任何信息，即明文和密文互相独立，则 $H(P|C) = H(P)$。故 $H(C, P) = H(P) + H(C)$

(2)

$$H(C) = H(C, P) - H(P) = H(C, P, K) - H(K|C, P) - H(P)$$

$$= H(P) + H(K) - H(K|C, P) - H(P) = H(K) - H(K|C, P)$$

(c) 因为在完善保密系统中，有 (b) 中结论成立，且明密文对有唯一密钥，故当明密文确定时，密钥也唯一确定，故 $H(K|C, P) = 0$, 则有 $H(C) = H(K) - H(K|C, P) = H(K)$

第三题

设密钥空间为 KEY,

$$S_1(x) = x + k_1,\ k_1 \sim U(KEY)$$

$$S_2(x) = x + k_2,\ k_2 \sim P_k$$

其中 $U(KEY)$ 表示在密钥空间 KEY 上的均匀分布，P_k 为 k_2 的概率分布。则

$$S_1 * S_2(x) = x + k_1 + k_2$$

令 $k = k_1 + k_2$ 任取 $K \in KEY$

$$p(k = K) = \sum_{i=1}^{|k_2|} p(k_2 = K_2) p(k_1 = K - K_2)$$

$$= p(k_1 = K - K_2) \sum_{i=1}^{|k_2|} p(k_2 = K_2) = p(k_1 = K - K_2) = \frac{1}{|KEY|}$$

故可知 $k = k_1+k_2$ 也是服从均匀分布,即 $k \sim U(KEY)$ 故 $S_1*S_2 = S_1$。此处定义的相等为密钥在密钥空间的分布是一致的。

$$f(-1) = \frac{1}{f(-1+2)} = \frac{1}{f(1)} = \frac{1}{\frac{1}{f(1+2)}} = f(1+2) = f(3) = \frac{1}{f(3+2)} = \frac{1}{f(5)} = \frac{1}{\frac{1}{f(5+2)}} = f(7) = 2$$