Exercise 5 in Cryptography
- Proposed Solution -

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo
2015-05-21

Solution of Problem 11

Prove Theorem 4.13 '⇒' (sufficient solution):

Recall that each element of these sets has a positive probability:

$$\mathcal{M}_+ := \{M \in \mathcal{M} \mid P(\hat{M} = M) > 0\},$$
$$\mathcal{C}_+ := \{C \in \mathcal{C} \mid P(\hat{C} = C) > 0\}.$$

Lemma 4.12 provides conditions of perfect secrecy on $\mathcal{M}_+$, $\mathcal{K}_+$, $\mathcal{C}_+$.
With Lemma 4.12 a), we obtain:

$$|\mathcal{M}_+| \leq |\mathcal{C}_+| \overset{(I)}{\leq} |\mathcal{C}| \overset{(II)}{=} |\mathcal{M}| \overset{(III)}{=} |\mathcal{M}_+|.$$

(I): With $P(\hat{C} = C) > 0 \Rightarrow \mathcal{C}_+ \subseteq \mathcal{C}$.
(II): Given by assumption $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$.
(III): Given by assumption $P(\hat{M} = M) > 0,\ \forall M \in \mathcal{M}$.

By the 'sandwich theorem', i.e., the upper and lower bounds are both equal to $|\mathcal{M}_+|$:

$$\Rightarrow |\mathcal{C}_+| = |\mathcal{C}| \Rightarrow \mathcal{C}_+ = \mathcal{C},$$
$$\Rightarrow P(\hat{C} = C) > 0,\ \forall C \in \mathcal{C}.$$

Let $M \in \mathcal{M}$, $C \in \mathcal{C}$:

$$\begin{aligned} 0 < P(\hat{C} = C) &\overset{(IV)}{=} P(\hat{C} = C \mid \hat{M} = M) = P(e(\hat{M}, \hat{K}) = C \mid \hat{M} = M) \\ &\overset{(V)}{=} P(e(M, \hat{K}) = C) = \sum\nolimits_{K \in \mathcal{K}:\, e(M,K)=C} P(\hat{K} = K) \neq 0 \qquad (1) \\ \Rightarrow &\ \forall M \in \mathcal{M},\ C \in \mathcal{C}\ \exists K \in \mathcal{K} : e(M, K) = C. \end{aligned}$$

(IV): With perfect secrecy as given by Corollary 4.11.
(V): Given by the assumption that $\hat{M}, \hat{K}$ are stochastically independent.

However, (1) is not shown to be unique yet!

(i) Fix $M \in \mathcal{M}$:

$$|\mathcal{C}_+| = |\mathcal{C}| = |\{e(M, K) \mid K \in \mathcal{K}_+ = \mathcal{K}\}| \leq |\mathcal{K}| \overset{(II)}{=} |\mathcal{C}|$$
$$\Rightarrow K \text{ is unique with } K = K(M, C) \text{ by the 'sandwich theorem'.}$$

(II) Given by assumption $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$.
Let $M \in \mathcal{M}$, $C \in \mathcal{C}$:

$$\Rightarrow P(\hat{C} = C) \overset{(1)}{=} P(\hat{K} = K(M, C)),$$

because of perfect secrecy this expression is independent of M.

(ii) Fix $C_0 \in \mathcal{C}$:

$$\Rightarrow \{K(M, C_0) \mid M \in \mathcal{M}\} = \mathcal{K},$$

because of injectivity of $e(\cdot, K)$, i.e., $e(M, K) = C_0$, and by the assumption $|\mathcal{M}| = |\mathcal{C}|$.

$$\Rightarrow P(\hat{C} = C) = P(\hat{K} = K) \ \forall C \in \mathcal{C}, K \in \mathcal{K}$$
$$\Rightarrow P(\hat{K} = K) = \tfrac{1}{|\mathcal{K}|} \ \forall K \in \mathcal{K}. \quad \square$$

Solution of Problem 12

For an affine cipher in $\mathbb{Z}_{26}$: $e(i, (a, b)) = a \cdot i + b \mod 26$

$$\mathbb{Z}_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} = \{a|\gcd(a, 26) = 1\}$$

$$\Rightarrow |\mathcal{K}| = |\mathbb{Z}_{26}^* \times \mathbb{Z}_{26}| = 12 \cdot 26$$

Let $M \in \mathcal{M}$, $C \in \mathcal{C}$

$$\begin{aligned} P(\hat{C} = C|\hat{M} = M) &= P(e(\hat{M}, \hat{K}) = C \mid \hat{M} = M) \\ &\overset{(\hat{K}, M \text{ stoch. ind.})}{=} P(e(M, \hat{K}) = C \\ &\overset{(\hat{K} \text{ unif. distr.})}{=} \frac{1}{|\mathcal{K}|} |\{K \in \mathcal{K} \mid e(M, K) = C\}| \\ &\overset{(*)}{=} \frac{12}{12 \cdot 26} = \frac{1}{26} \end{aligned}$$

$$(*) : e(M, (a, b)) = C \Leftrightarrow a \cdot M + b = C \mod 26 \Leftrightarrow b = C - aM \mod 26$$
$$\Rightarrow \text{ all keys } (a, C - aM),\ a \in \mathbb{Z}_{26}^* \text{ satisfy this equation}$$
$$\Rightarrow \ P(\hat{C} = C|\hat{M} = M) = \frac{1}{26} \forall M \in \mathcal{M}_+$$
$$\Rightarrow \ P(\hat{C} = C) = \frac{1}{26} = P(\hat{C} = C|\hat{M} = M)$$

With Corollary 4.11, the cryptosystem has perfect secrecy, i.e., $\hat{C}$ and $\hat{M}$ are stochastically independent.

Solution of Problem 13

Recall: $H(X) = -\sum_i p_i \log(p_i)$.

a) $H(\hat{M}) = -\frac{1}{4}\log_2(\frac{1}{4}) - \frac{3}{4}\log_2(\frac{3}{4}) = \frac{1}{2} + \frac{3}{2} - \frac{3}{4}\log_2(3) \approx 0.811$
$H(\hat{K}) = -\frac{1}{2}\log_2(\frac{1}{2}) - 2\frac{1}{4}\log_2(\frac{1}{4}) = \frac{1}{2} + 1 = 1.5$

c	K_1	K_2	K_3	
a	1	2	3	$\frac{1}{4}$
b	2	3	4	$\frac{3}{4}$
	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	1

$$
\begin{aligned}
&P(\hat{C} = 1) = P(\hat{M} = a) \cdot P(\hat{K} = K_1) = \tfrac{1}{4} \cdot \tfrac{1}{2} = \tfrac{1}{8} \\
&P(\hat{C} = 2) = P(\hat{M} = a) \cdot P(\hat{K} = K_2) + P(\hat{M} = b) \cdot P(\hat{K} = K_1) = \tfrac{1}{4} \cdot \tfrac{1}{4} + \tfrac{3}{4} \cdot \tfrac{1}{2} = \tfrac{7}{16} \\
&P(\hat{C} = 4) = P(\hat{M} = b) \cdot P(\hat{K} = K_3) = \tfrac{3}{4} \cdot \tfrac{1}{4} = \tfrac{3}{16} \\
\Rightarrow &P(\hat{C} = 3) = 1 - P(\hat{C} = 1) - P(\hat{C} = 2) - P(\hat{C} = 4) = 1 - \tfrac{2}{16} - \tfrac{7}{16} - \tfrac{3}{16} = \tfrac{4}{16} \\
\Rightarrow &H(\hat{C}) = -\tfrac{1}{8}\log_2(\tfrac{1}{8}) - \tfrac{7}{16}\log_2(\tfrac{7}{16}) - \tfrac{3}{16}\log_2(\tfrac{3}{16}) - \tfrac{1}{4}\log_2(\tfrac{1}{4}) \approx 1.850 \\
\Rightarrow &H(\hat{K} \mid \hat{C}) \overset{\text{Thm. 4.7}}{=} H(\hat{M}) + H(\hat{K}) - H(\hat{C}) \approx 0.811 + 1.5 - 1.850 = 0.461
\end{aligned}
$$

b) Lem. 4.12 b) demands $|\mathcal{C}_+| \leq |\mathcal{K}_+|$ for perfect secrecy.
But in this case, we get $4 = |\mathcal{C}_+| > |\mathcal{K}_+| = 3$ ↯