応用数学６ 2010 年 10 月 14 日

第 1 回小テスト

講師: 安永憲司

定義 1 (Ceasar 暗号) 長さ n の Ceasar 暗号は次の $(\mathcal{M}, \mathcal{K}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ で定義される．

$$\begin{aligned}
\mathcal{M} &= \{A, B, \ldots, Z\}^n \\
\mathcal{K} &= \{0, 1, 2, \ldots, 25\} \\
\mathsf{Gen} &= k;\ \text{ただし } k \xleftarrow{R} \mathcal{K} \\
\mathsf{Enc}_k(m_1 m_2 \ldots m_n) &= c_1 c_2 \ldots c_n;\ \text{ただし } c_i = m_i + k \bmod 26 \\
\mathsf{Dec}_k(c_1 c_2 \ldots c_n) &= m_1 m_2 \ldots m_n;\ \text{ただし } m_i = c_i - k \bmod 26
\end{aligned}$$

ただし，アルファベット $\{A, B, \ldots, Z\}$ は，整数 $\{0, 1, \ldots, 25\}$ に，それぞれ対応していると考える．

問題 1.

$n = 1$ のとき，Ceasar 暗号は完全秘匿であることを証明せよ．

問題 2.

$n \geq 2$ のとき，Ceasar 暗号は完全秘匿でないことを証明せよ．

問題 3.

使い捨て鍵暗号の使い方に関して，以下の状況を考える．

恋人同士である Alice と Bob は毎日秘匿通信を行いたいが，Alice の母親である Eve に通信内容がすべて盗聴されている．そこで，特に知られたくない内容をやり取りする場合は，完全秘匿性をもつ使い捨て鍵暗号 $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ を使って暗号化して通信することにした．しかし，使い捨て鍵暗号は鍵 1 つに対して 1 回しか通信することができない．

ここで Bob はあるアイディアを思いついた．Alice と Bob は毎日直接会っているので，そのときに鍵 $k \leftarrow \mathsf{Gen}$ を共有する．そして，1 日に 10 回秘匿通信を行いたい場合，Bob は鍵 10 個 $k_1, k_2, \ldots, k_{10} \leftarrow \mathsf{Gen}$ を生成し，それを鍵 k を用いて暗号化し，Alice に送る．つまり，$\mathsf{Enc}_k(k_1), \mathsf{Enc}_k(k_2), \ldots, \mathsf{Enc}_k(k_{10})$ を送る．Alice は鍵 k をもっているので，$k_1, \ldots, k_{10}$ を手に入れることができる．そして，秘匿通信したい 10 回分のメッセージ $m_1, m_2, \ldots, m_{10}$ は，$\mathsf{Enc}_{k_1}(m_1), \mathsf{Enc}_{k_2}(m_2), \ldots, \mathsf{Enc}_{k_{10}}(m_{10})$ と暗号化して送る．

この方法では，同じ鍵 k を使って 10 回も暗号化しているため，安全でないように見える．しかし，Bob は次のように主張する．「使い捨て鍵暗号なので，$\mathsf{Enc}_k(k_1) = k_1 \oplus k = \mathsf{Enc}_{k_1}(k)$ である．鍵 k_1 はランダムに生成されているので，鍵 k は安全なままである．なので，k を使って k_2 を暗号化しても安全なままである．後は同じ議論で，10 回繰り返しても鍵 k は安全なままである.」

Bob の主張に反し，この方法は安全でないことを示せ．特に，暗号文 $\mathsf{Enc}_k(k_1), \ldots, \mathsf{Enc}_k(k_{10})$, $\mathsf{Enc}_{k_1}(m_1), \ldots, \mathsf{Enc}_{k_{10}}(m_{10})$ から，メッセージ $m_1, \ldots, m_{10}$ に関する有用な情報をどのように得ることができるかを説明せよ．