Совершенная криптосистема и эндоморфный шифр

Определение (Эндоморфный шифр)

Шифр эндоморфный, если $|\mathcal{M}| = |\mathcal{C}|$

Теорема (Главная теорема билета)

Пусть $|\mathcal{K}| = |\mathcal{M}| \Rightarrow |\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$.

Тогда криптосистема $(\mathcal{K}, \mathcal{C}, \mathcal{K}, E, D)$ — **совершенная**

$$\Leftrightarrow \text{ выполняются условия:}$$

1. $\forall m, c \ \exists! k : E(m, k) = c$
2. $\forall k \in \mathcal{K} : P(K = k) = \frac{1}{|\mathcal{K}|}$

Доказательство $\Rightarrow$ пункт 1

По лемме: $|E(m, \mathcal{K})| = |\mathcal{C}| = |\mathcal{K}|$.

Рассматриваем $E(m, \cdot) : \mathcal{K} \to \mathcal{C}$ — сюръекция на множества одинаковой мощности. Следовательно, $E(m, \cdot)$ — **биекция**, и потому для каждого c найдётся единственный k, такой что $E(m, k) = c$.

$$\Rightarrow \forall m, c \ \exists! k : E(m, k) = c \qquad \blacksquare$$

Доказательство $\Rightarrow$ пункт 2

Зафиксируем $c \in \mathcal{C}$, и обозначим k_i — такой ключ, что $E(m_i, k_i) = c$.

Рассмотрим:

$$P(M = m_i \mid C = c) = \frac{P(C = c \mid M = m_i) \cdot P(M = m_i)}{P(C = c)}$$

Так как по условию $E(m_i, k_i) = c$, то $P(C = c \mid M = m_i) = P(K = k_i)$.

$$P(M = m_i \mid C = c) = \frac{P(K = k_i) \cdot P(M = m_i)}{P(C = c)}$$

Но в совершенной системе $P(M = m_i \mid C = c) = P(M = m_i)$, тогда:

$$P(M = m_i) = \frac{P(K = k_i) \cdot P(M = m_i)}{P(C = c)} \Rightarrow P(K = k_i) = P(C = c)$$

Так как $P(C = c)$ одинаково для всех k_i, получаем, что $P(K = k_i)$ одинаковы для всех i:

$$\Rightarrow P(K = k_i) = \frac{1}{|\mathcal{K}|} \qquad \blacksquare$$

Доказательство $\Leftarrow$

Пусть выполняются условия 1) и 2). Покажем, что M и C независимы, т.е. $P(M = m_i \mid C = c) = P(M = m_i)$.

Рассмотрим вероятность $P(C = c)$:

$$P(C = c) = \sum_{m_i \in \mathcal{M}} P(C = c \mid M = m_i) \cdot P(M = m_i)$$

По условию 1), для каждого m_i существует единственный $k_i \in \mathcal{K}$ такой, что $E(m_i, k_i) = c$. Тогда:

$$P(C = c \mid M = m_i) = P(K = k_i)$$

А по условию 2):

$$P(K = k_i) = \frac{1}{|\mathcal{K}|}$$

Тогда:

$$P(C = c) = \sum_{m_i \in \mathcal{M}} \frac{1}{|\mathcal{K}|} \cdot P(M = m_i) = \frac{1}{|\mathcal{K}|} \sum_{m_i \in \mathcal{M}} P(M = m_i) = \frac{1}{|\mathcal{K}|}$$

Теперь вычислим $P(M = m_i \mid C = c)$ по формуле Байеса:

$$P(M = m_i \mid C = c) = \frac{P(C = c \mid M = m_i) \cdot P(M = m_i)}{P(C = c)}$$

Подставим:

$$= \frac{P(K = k_i) \cdot P(M = m_i)}{\frac{1}{|\mathcal{K}|}} = \frac{\frac{1}{|\mathcal{K}|} \cdot P(M = m_i)}{\frac{1}{|\mathcal{K}|}} = P(M = m_i)$$

Следовательно: Условная пероятность равна безусловной, а значит случайные величины M и