Криптосистема и её свойства

Криптосистема — это $(\mathcal{M}, \mathcal{C}, \mathcal{K}, E, D)$, где:

- M — случайная величина на (распределена) $\mathcal{M}$ (открытые тексты)
- C — случайная величина на (распределена)$\mathcal{C}$ (криптограммы)
- K — случайная величина на (распределена) $\mathcal{K}$ (ключи)
- $D : \mathcal{C} \times \mathcal{K} \to \mathcal{M}$ — функция дешифрования
- $\forall c \in \mathcal{C},\ \forall k \in \mathcal{K} : \quad P(M = D(c, k) \mid C = c, K = k) = 1$
- $\forall m \notin D(c, k) : \quad P(M = m, C = c, K = k) = 0$

То есть:

$$H(M \mid C, K) = 0$$

Так как либо множитель равен 0, либо $\log(1) = 0$, см. определение энтропии $H(p)$.

Теорема (Главная часть билета)

$$I(M \leftrightarrow C) \geq H(M) - H(K)$$

Доказательство

Рассмотрим:

$$H(K \mid C) = H(K \mid C) +$$
$$+ H(M \mid C, K)$$

Применим цепное правило:

$$H(M, K \mid C) = H(K \mid C) + H(M \mid C, K)$$

Также:

$$H(M, K \mid C) = H(M \mid C) + H(K \mid M, C) \geq H(M \mid C)$$
$$\Rightarrow H(M \mid C) \leq H(K \mid C)$$

Рассмотрим $H(K \mid C)$:

$$H(K \mid C) = H(K, C) - H(C) - H(K)$$
$$+ H(K) = H(K) - I(K \Leftrightarrow C) \leq H(K)$$

Теперь выразим взаимную информацию:

$$I(M \Leftrightarrow C) = H(M) + H(C) - H(M, C) =$$
$$= H(M) - H(M \mid C) \geq H(M) - H(K) \qquad \blacksquare$$

Смысл теоремы

- Взаимная информация $I(M \leftrightarrow C)$ тем больше, чем больше $H(M) - H(K)$.
- $H(M)$ — энтропия открытого текста, задать её мы не можем.
- $H(K)$ — энтропия ключа. Чтобы уменьшить взаимную информацию, нужно увеличить $H(K)$.
- Если ключи равномерно распределены, то $H(K) \leq \log |\mathcal{K}|$.
- Тогда $H(K)$ увеличивается с увеличением числа ключей — т.е. длины ключа.
- Чтобы $I(M \leftrightarrow C)$ было как можно меньше, нужно, чтобы $H(K) \geq H(M)$.
- В идеале хотим: $I(M \leftrightarrow C) = 0$ — M и C независимы.

Определение (Совершенная криптосистема)

Криптосистема называется **совершенной**, если:

$$I(M \leftrightarrow C) = 0 \quad \Leftrightarrow \quad M \text{ не зависит от } C$$

То есть, открытый текст и криптограмма — независимые случайные величины.

В совершенной криптосистеме:

$$H(K) \geq H(M)$$

Предполагается: $\forall m \in \mathcal{M} : P(M = m) > 0$

Лемма (Главная часть билета)

В совершенной криптосистеме:

$$\forall m \in \mathcal{M} : \quad E(m, \mathcal{K}) = \mathcal{C}$$

То есть, если зашифровать любой открытый текст на всех ключах, получится весь набор криптограмм.

Доказательство (от противного)

Пусть:

$$\exists m \in \mathcal{M},\ \exists c \in \mathcal{C} : \quad \forall k \in \mathcal{K} : \quad E(m, k) \neq c$$

Тогда:

$$P(M = m \mid C = c) = 0 \Rightarrow P(M = m) = 0 \quad (\text{в совершенной КС: } M \perp C) \Rightarrow \text{противоречие} \qquad \blacksquare$$

Следствие

Из леммы:

$$|\mathcal{K}| \geq |\mathcal{C}| \geq |\mathcal{M}|$$

Иначе невозможно обеспечить однозначную расшифровку всех сообщений.