Расстояние единственности шифра

Пусть все ключи из множества $\mathcal{K}$ равновероятны.

Рассмотрим $c \in \mathcal{C}$ и попытаемся расшифровать его, перебирая все ключи из $\mathcal{K}$.

Тогда мы получим $|\mathcal{K}|$ кандидатов на открытый текст.

Типичная (осмысленная) последовательность — это такая, вероятность которой соответствует типичной информации источника.

Доля типичных последовательностей:

$$\frac{2^{nH_L}}{|\Sigma|^n}$$

Тогда вероятность того, что случайно выбранный кандидат окажется осмысленным:

$$2^{n(H_L - \log_2 |\Sigma|)}$$

Ожидаемое количество осмысленных текстов:

$$|\mathcal{K}| \cdot 2^{n(H_L - \log_2 |\Sigma|)}$$

Определение: Расстояние единственности шифра

Если

$$|\mathcal{K}| \cdot 2^{n(H_L - \log_2 |\Sigma|)} \leq 1,$$

то n называется **расстоянием единственности шифра**.

Это такое число N_0, что:

$$\forall n > N_0 \quad |\mathcal{K}| \cdot 2^{n(H_L - \log_2 |\Sigma|)} \leq 1$$

Преобразуем неравенство:

$$\log_2 |\mathcal{K}| + nH_L - n \log_2 |\Sigma| \leq 0$$

$$n(H_L - \log_2 |\Sigma|) \leq -\log_2 |\mathcal{K}|$$

Заметим: $H_L - \log_2 |\Sigma| < 0$, так как:

- $H_L = \lim\limits_{n \to \infty} H_n(x)$,
- $H_0 = \log_2 |\Sigma|$,
- по теореме для стационарного источника $H_n(x)$ убывает при увеличении n.

Также:

$$H_L = (1 - R_L) \cdot \log_2 |\Sigma|$$

Итоговая формула для расстояния единственности:

$$n \geq \frac{-\log_2 |\mathcal{K}|}{H_L - \log_2 |\Sigma|} = \frac{\log_2 |\mathcal{K}|}{\log_2 |\Sigma| - H_L} = \frac{\log_2 |\mathcal{K}|}{R_L \cdot \log_2 |\Sigma|}$$