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

Возьмём $c \in \mathcal{C}$ и будем пытаться расшифровывать, используя все ключи

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

“Типичная” последовательность это тоже самое что “осмысленная”

Знаем долю типичных $\frac{2^{nH_L}}{|\Sigma|^n}$

Тогда вероятность, что случайно выбранный кандидат окажется осмысленным, это $2^{n(H_L - log(|\Sigma|))}$

В итоге получаем $|\mathcal{K}| \cdot 2^{n(H_L - log(|\Sigma|))}$ - осмысленных текстов

ОПР(Расстояние единственности шифра)

Если $|\mathcal{K}| \cdot 2^{n(H_L - log(|\Sigma|))} \leq 1$, то n - это **расстояние единственности шифра**

- Это такое число $N_0 : \forall n > N_0 : |\mathcal{K}| \cdot 2^{n(H_L - log(|\Sigma|))} \leq 1$

Его можно посчитать

$log(|\mathcal{K}|) + n \cdot H_L - n \cdot log(|\Sigma|) \leq 0$

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

- число $H_L - log(|\Sigma|) < 0$ Если на него поделить, то мы должны поменять знак неравенства
  - т.к $H_L = \lim\limits_{n \to \infty} H_n(x)$; $H_0 = log(|\Sigma|)$;
  - по теореме для стационарного источника $H_n(x) \searrow$ с ростом n
- $H_L = (1 - R_L) \cdot log(|\Sigma|)$

$n \geq \frac{-log(|\mathcal{K}|)}{(H_L - log(|\Sigma|))} = \frac{log(|\mathcal{K}|)}{(log(|\Sigma|) - H_L)} = \frac{log(\mathcal{K})}{R_L \cdot log(|\Sigma|)} = N_0$

Спроси что ещё можно докинуть в билет