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

- M распределена на $\mathcal{M}$
- C распределена на $\mathcal{C}$
- K распределена на $\mathcal{K}$
- $D : \mathcal{C} \times \mathcal{K} \to \mathcal{M}$
- $\forall c \in \mathcal{C}, k \in \mathcal{K} : P(M = D(c, k)|C = c, K = k) = 1$
- $\forall m \notin D(c, k) : P(M = m, C = c, K = k) = 0$

т.е

$$H(M|C, K) = 0$$

т.к либо множитель равен 0, либо $log(1) = 0$, см опр H(p)

Теорема (Главная часть билета)

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

Д-ВО

$H(K|C) = H(K|C) + H(M|C, K) =$

- применяем цепное правило

$H(M, K|C) =$

- применяем цепное правило
- $H(K|M, C) \geq 0$ по опр $H(p)$

$H(M|C) + H(K|M, C) \geq H(M|C)$

Получаем, что $H(M|C) \leq H(K|C)$

- Применяем к $H(K|C)$ цепное правило прибавим и вычтем $H(K)$

$H(K|C) = H(K|C) - H(C) - H(K) + H(K) =$

- По Т о взаимной информации $H(K|C) - H(C) - H(K) = -I(K \leftrightarrow C)$

$H(K) - I(K \leftrightarrow C) \leq H(K)$

Получаем, что $H(K) \geq H(K|C)$

- По Т о взаимной информации

$I(M \leftrightarrow C) = H(M) + H(C) - H(M, C)=$

- по цепному правилу $H(C) - H(M, C) = -H(M|C)$
- из $H(K) \geq H(K|C)$ и $H(K|C) \geq H(M|C)$ **получаем, что** $H(K) \geq H(M|C)$

Получаем, что:

$H(M) - H(M|C) \geq H(M) - H(K)$

■

Смысл теоремы

- Взаимная информация между октрытым текстом и криптограммой тем больше, чем больше $H(M) - H(K)$
- H(M) - это энтропия открытого текста, с ней ничего поделать нельзя
- H(K) - это энтропия ключа. Можно делать ключи равномернораспределенными, тогда $H(K) \leq log(|\mathcal{K}|)$ по свойствам энтропии
- Получается, что H(K) растёт с ростом кол-ва ключей, т.е с ростом длины
- Тогда чтобы как можно сильнее уменьшить нижнюю границу $I(M \leftrightarrow C)$ нужно увеличивать $H(K)$, т.е ключей должно быть не меньше чем длина открытого текста(если открытые тексты равномерно распределены)

В идеале $I(M \leftrightarrow C) = 0$, т.е M и C будут независимыми

ОПР(Совершенной криптосистемы)

Криптосистема - **совершенная**, если $I(M \leftrightarrow C) = 0 \Leftrightarrow$ случайные величины M и C - независимы

- в совершенной КС $H(K) \geq H(M)$

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

Лемма(Главная часть билета)

В совершенной КС $\forall m \in \mathcal{M} : E(m, \mathcal{K}) = \mathcal{C}$ т.е если мы возьмем любой открытый текст, зашифруем его на всех ключах, то получим все криптограмы

Д-ВО (О/П)

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

Тогда $P(M = m|C = c) = 0 \Rightarrow$ [т.к в совершенной КС, М и С независимы, то условная и безусловная вероятности равны]$\Rightarrow P(M = m) = 0$ $\bigotimes$

■

В частности это значит, что $|\mathcal{K}| \geq |\mathcal{C}| \geq$ [иначе бы не получалось однозначно расшифровывать] $\geq |\mathcal{M}|$