ОПР(Эндоморфный шифр)

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

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

Лемма

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, M и C 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] $\geq |\mathcal{M}|$

Теорема (Главная теорема билета)

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

Тогда КС $(\mathcal{K}, \mathcal{C}, \mathcal{K}, E, D)$ - совершенная $\Leftrightarrow$ выполняется 1) и 2)

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

Д-ВО $\Rightarrow$ пункт 1

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

$\measuredangle \forall m \in \mathcal{M} \; : E(m, \_) : \mathcal{K} \to \mathcal{C}$

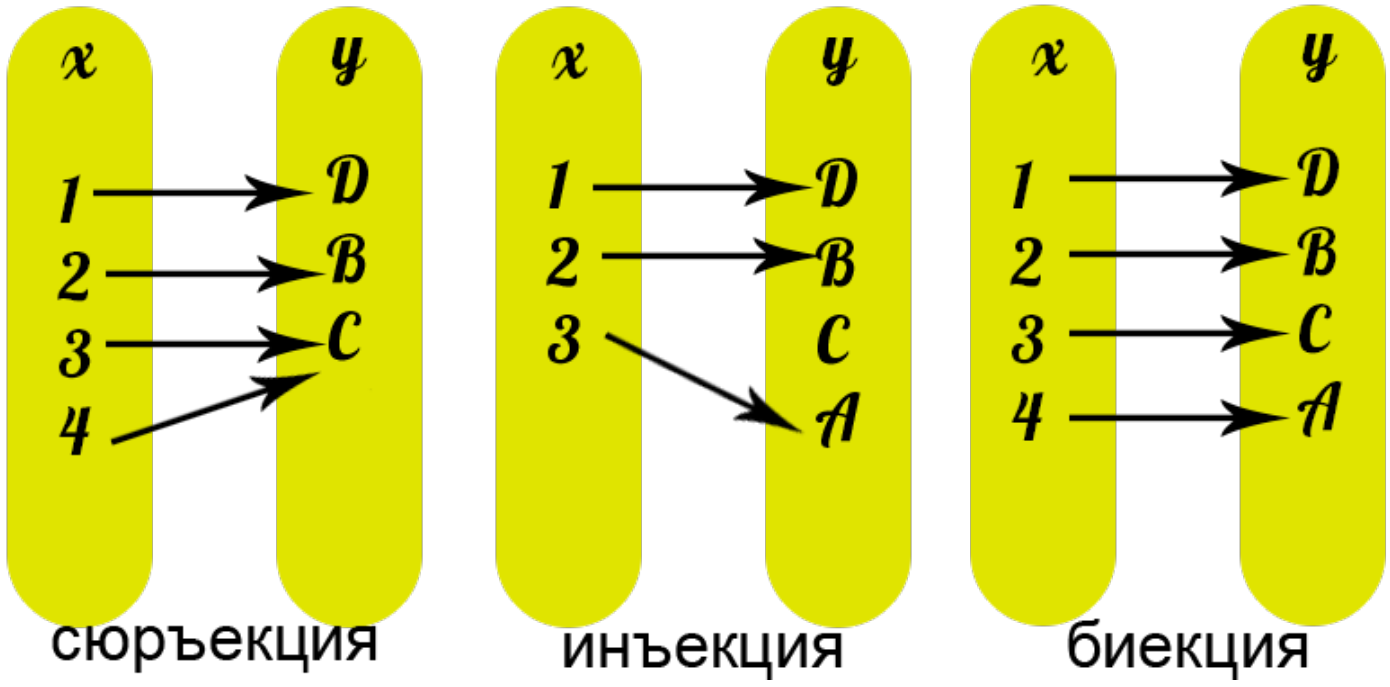

Рис. 1: воспоминания о свойствах функций

- Это сюръективная функция на множествах одинакового размера $\Rightarrow$ эта $E(m, \_)$ - биекция
  - Функция это всюдуопределенное однозначное б.и

■

Д-ВО $\Rightarrow$ пункт 2

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

Тогда

$P(M = m_i) = P(M = m_i|C = c)=$

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

- $P(C = c|M = m_i)$ - такая же как $P(K = k_i)$

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

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

$\forall i \ : P(K = k_i) = P(C = c)$

т.к C зафиксировано, то $\forall\ i\ P(K = k_i)$ получаем одинаковую вероятность, т.е k_i - распределены равномерно $\Rightarrow$ $\forall\ i\ P(K = k_i) = \frac{1}{|\mathcal{K}|}$

■

Д-ВО $\Leftarrow$

берём $c \in \mathcal{C}$ и $\measuredangle P(C = c)$

$P(C = c) =$

- По формуле полной вероятности

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

- по 1)

$\sum_{m_i \in \mathcal{M}}(P(K = k_i) \cdot P(M = m_i))=$

- по 2)

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

Получили, что $P(C = c) = \frac{1}{|\mathcal{K}|}$

$P(M = m_i|C = c_i)=$

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

- по 2)

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

Получили, что условная вероятность равна безусловной,т.е случайные величины M и C - независимы

■

Шифр вернама - совершенный шифр