Лекция №1

Часть 3. Абсолютная криптографическая стойкость. Одноразовый блокнот.

Елена Киршанова

Курс “Основы криптографии”

Шифр Шеннона (Shannon's cipher)

Положим $\mathcal{K}, \mathcal{M}, \mathcal{C}$ – множества ключей, открытых текстов, шифр-текстов

Шифр Шеннона –

это тройка функций KeyGen, Enc, Dec:

$$\mathsf{Enc} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$$
$$\mathsf{Enc}(k, m) = c$$

$$\mathsf{Dec} : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$$
$$\mathsf{Dec}(k, c) = m,$$

для которых выполняется

$$\mathsf{Dec}(k, \mathsf{Enc}(k, m)) == m \qquad \forall k \leftarrow \mathsf{KeyGen}, m \in \mathcal{M}$$

Абсолютная криптографическая стойкость (perfect secrecy)

- На каждом из этих множеств зададим распределение: $\Pr[M = m]$ – вероятность выбора $m \in \mathcal{M}$.
- Аналогично для $K \in \mathcal{K}, C \in \mathcal{C}$.

Абсолютная криптографическая стойкость

Шифр-схема $\Pi = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ обладает *абсолютной криптографической стойкостью*, если для любого распределения над $\mathcal{M}$

$$\Pr\left[M = m | C = c\right] = \Pr\left[M = m\right] \quad \forall m \in \mathcal{M}, c \in \mathcal{C}.$$

Интуиция: шифр-текст c не содержит никакой информации об открытом тексте m.

Шифр-текст не зависит от открытого текста

Шифр-схема $\Pi = (\mathsf{Enc}, \mathsf{Dec})$, определённая над $\mathcal{K}, \mathcal{M}, \mathcal{C}$, абсолютно стойка тогда и только тогда, когда

$$\Pr[C = c \mid M = m] = \Pr[C = c] \qquad \forall m \in \mathcal{M}, c \in \mathcal{C}.$$

Шифр-текст не отличимы друг от друга

Шифр-схема $\Pi = (\mathsf{Enc}, \mathsf{Dec})$, определённая над $\mathcal{K}, \mathcal{M}, \mathcal{C}$, абсолютно стойка тогда и только тогда, когда для любых $m_0, m_1 \in \mathcal{M}$ выполняется

$$\Pr[C = c \mid M = m_0] = \Pr[C = C \mid M = m_1]$$

Одноразовый блокнот (One-time pad) или шифр Вернама

Одноразовый блокнот

Положим $\mathcal{M}, \mathcal{K}, \mathcal{C} = \{0,1\}^n$.

- $\mathsf{KeyGen}(1^\lambda) : k \leftarrow \{0,1\}^n$
- $\mathsf{Enc}(k, m \in \{0,1\}^n) : c = k \oplus m$
- $\mathsf{Dec}(k, c \in \{0,1\}^n) : m = k \oplus c$

Теорема. Одноразовый блокнот является абсолютно стойким.

Недостаток абсолютной стойкости

Теорема. Положим $\Pi = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ – абсолютно стойкая шифр-схема. Тогда $|\mathcal{K}| \geq |\mathcal{M}|$

Интуиция: Абсолютно стойкие схемы неэффективны.

Теорема Шэннона (1949)

Положим $\Pi = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ – шифр-схема с $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$.
Тогда Π – абсолютно стойкая тогда и только тогда, когда

1. KeyGen выбирает $k \in \mathcal{K}$ с вероятностью $\frac{1}{|\mathcal{K}|}$ для всех k
2. $\forall m \in \mathcal{M}, c \in \mathcal{C}$ существует единственный $k \in \mathcal{K} : c = \mathsf{Enc}(k, m)$.

Одноразовый блокнот на практике

- Правительственная «горячая линия» между Вашингтоном и Москвой в 60-х
  https://en.wikipedia.org/wiki/Moscow%E2%80%93Washington_hotline
- Вьетнамские войны
  https://eprint.iacr.org/2016/1136.pdf