

Защита информации

Павел Юдаев

МГТУ им. Баумана, Кафедра ИУ-9

Москва, 2014

Раздел 4 - Одноразовый ключ и многоразовый ключ

Лемма о переключении

Одноразовый ключ

Многоразовый ключ

Псевдослучайная функция и псевдослучайная перестановка

Опр.

$\text{Perms}(X)$ - множество всех обратимых функций (перестановок)
 $X \rightarrow X$

Опр.

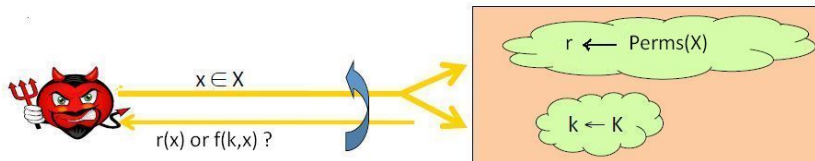
Функция $f : K \times X \rightarrow X$ - это *псевдослучайная перестановка*, если

$\forall k \ f(k, \cdot) \in \text{Perms}(X), f \in \text{PT}, f^{-1}(k, \cdot) \in \text{PT},$

\forall оракула $A \in \text{PPT}$ при $k \xleftarrow{R} K, r \xleftarrow{R} \text{Perms}(X)$

величина

$\text{Adv}(A, F) = |P[A(f(k, \cdot)) = 1] - P[A(r(\cdot)) = 1]| < \varepsilon(n),$



ПСП всегда “эффективно” обратима, ПСФ - не обязательно обратима.

Для маленького множества X ПСФ просто отличить от ПСП, пример:

$$X \rightarrow X, X = \{0, 1\}.$$

Если множество X большое, нельзя эффективно отличить ПСП от ПСФ.

Лемма (О переключении)

Пусть f - ПСП на $K \times X \rightarrow X$. Тогда

\forall алгоритма $A \in \text{PPT}$, который вычисляет функцию в q точках, верно

$$|\text{Adv}_{\text{PRF}}(A, f) - \text{Adv}_{\text{PRP}}(A, f)| < q^2 / (2|X|)$$

Док-во: рассказать по [1]. (Чуть проще, чем там.)

$$q = \text{poly}(n), |X| = 2^n = \text{exp}(n).$$

Зачем это все нужно?

Если блочный шифр - ПСП,
тогда можно формально обосновать криптостойкость блочного шифра.

Если шифр - ПСП, по лемме он - ПСФ.

На основе ПСФ можно строить криптостойкий ГПСЧ. (Один из способов.)

Раздел 4 - Одноразовый ключ и многоразовый ключ

Лемма о переключении

Одноразовый ключ

Многоразовый ключ

До сих пор шифровали один блок длины n бит. Перейдем к сообщению произвольной длины.

Модель:

- одноразовый ключ
- сообщение длиной более одного блока
- злоум-к может: видит только шифротекст
- цель злоум-ка: по шифротексту получить информацию о сообщении

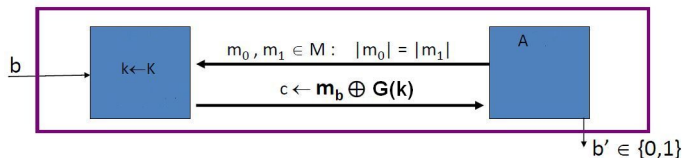
Режим электронной кодовой книги - ECB

Опр.

Режим работы блочного шифра, когда к каждому блоку применяется одна и та же детерминированная перестановка $E(k, \cdot)$, называется Электронная кодовая книга - Electronic codebook, ECB.

Эксперимент SS для одноразового ключа (повтор):

1. Система выбирает случайное значение бита $b \xleftarrow{R} \{0, 1\}$. Оно секретное.
2. Злоумышленник выбирает длину n и отправляет два сообщения $m_0 \neq m_1$ длины n .
3. Система вычисляет $c = E(k, m_b)$ и отправляет его злоум-ку.
4. Злоум-к $A \in \text{PPT}$ анализирует c и выдает результат - бит b' .
5. Если $b' = b$, A достиг успеха.



Один запрос, ответ.

Опр.

Шифр наз. *семантически стойким для одноразового ключа*, если в этом эксперименте вероятность успеха A не более $\frac{1}{2} + \varepsilon(n)$, где $\varepsilon(n)$ - пренебр. малая, вероятность вычисляется по случайным выборам: k , b , алгоритма A и шифрования E .

Эквивалентно:

$$\text{Adv}_{SS}(A, E_{OTK}) = |P(b' = 1|b = 1) - P(b' = 1|b = 0)| < \varepsilon(n).$$

Задача

Доказать, что режим ECB не семантически стойкий.
Использовать сообщение длиной два блока, эти блоки - одинаковые.

Режим счетчика без сцепления блоков - DetCTR

Deterministic counter mode.

Опр.

Пусть $f : K \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ - ПСФ. Тогда i -й блок:

$$E_{\text{DetCtr}}(k, m)[i] = m[i] \oplus f(k, i)$$

$$E_{\text{DETCTR}}(k, m) =$$

| | | | |
|--------|--------|-----|--------|
| $m[0]$ | $m[1]$ | ... | $m[L]$ |
|--------|--------|-----|--------|

\oplus

| | | | |
|-----------|-----------|-----|-----------|
| $F(k, 0)$ | $F(k, 1)$ | ... | $F(k, L)$ |
|-----------|-----------|-----|-----------|

| | | | |
|--------|--------|-----|--------|
| $c[0]$ | $c[1]$ | ... | $c[L]$ |
|--------|--------|-----|--------|

Когда блочный шифр исп. как поточный, это наз. режимом гаммирования.

Утверждение

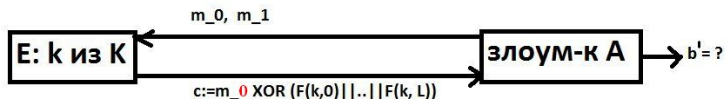
Пусть $f : K \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ - ПСФ. Тогда $\forall L > 0$ при одноразовом ключе E_{DetCtr} - семант. стойкий шифр: $K \times \{0, 1\}^{nL} \rightarrow \{0, 1\}^{nL}$.

В частности, \forall алгоритма $A \in \text{PPT}$, реализ. атаку на E_{DetCtr} , сущ. алгоритм $B \in \text{PPT}$, осущ. атаку на ПСФ F :

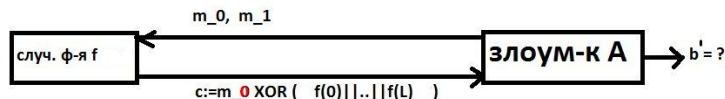
$$\text{Adv}_{SS}[A, E_{DetCtr}] \leq 2 \cdot \text{Adv}_{SS}[B, F]$$

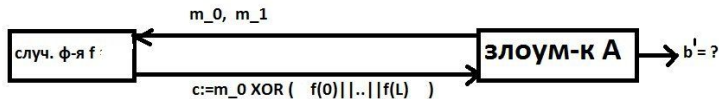
Док-во

Аналогично теореме 2 о семантической стойкости поточного шифра.

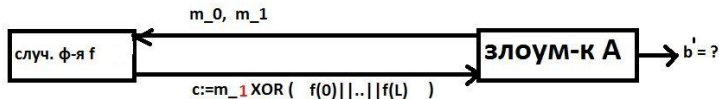


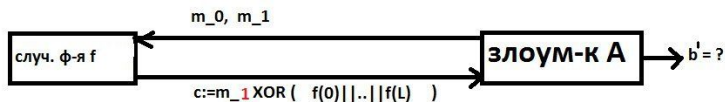
F - стойкая ПСФ, не отличима от случайно выбранной функции f



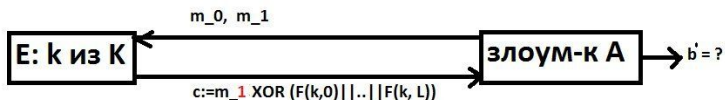


Одноразовый блокнот - абсолютно стойкий шифр





F - стойкая ПСФ, не отличима от случайно выбранной функции f



Для первого перехода вероятность отличить “верх” от “низа”:
 $|P(b' = 1|b = 0, E) - P(b' = 1|b = 0, OTP)| = Adv_{SS}[B, F] < \varepsilon(n)$

Для второго - отличить нельзя.

Для третьего: $|P(b' = 1|b = 1, E) - P(b' = 1|b = 1, OTP)| = Adv_{SS}[B, F] < \varepsilon(n)$

Поэтому $Adv_{SS}[A, E_{DetCtr}] \leq Adv_{SS}[B, F] + 0 + Adv_{SS}[B, F] = 2 \cdot Adv_{SS}[B, F]$.

Ч.т.д.

Раздел 4 - Одноразовый ключ и многоразовый ключ

Лемма о переключении

Одноразовый ключ

Многоразовый ключ

Режимы использования, стойкие при многократном использовании ключа.

Злоум-к видит много шифротекстов, зашифрованных одним ключом.

Модель:

- Возможности злоум-ка: может получать шифротексты для любых сообщений.
Т.е. атака с выбором открытого текста,
chosen plaintext attack.
- Цель злоум-ка: нарушить семантическую стойкость.

Эксперимент “атака с выбором открытого текста” (CPA):

Пусть (E, D) - шифр.

1. Система выбирает ключ k и значение бита b , секр., фикс.

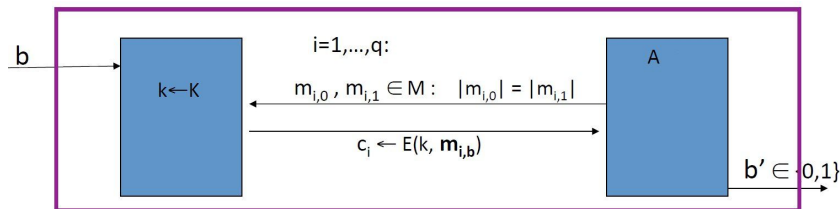
2. $q \in \mathbb{N}$ - число запросов злоумышленника.

$q = \text{poly}(\log(|\{m\}|))$.

Каждый раз он отправляет $m_{i,0}, m_{i,1} : \text{len}(m_{i,0}) = \text{len}(m_{i,1})$.

3. Система вычисляет $c_i = E(k, m_{i,b})$, отправляет злоум-ку.

4. После q запросов злоум-к выдает b' - гипотезу о b .



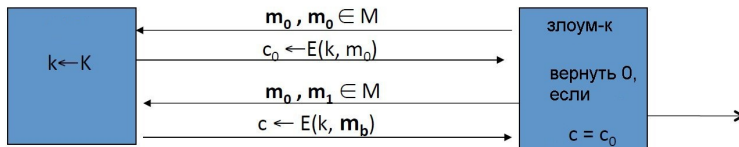
Сообщения могут повторяться.

Опр.

шифр $C = (E, D)$ наз. семантически стойким к атаке с выбранным открытым текстом, если $\forall A \in \text{PPT}$

$$\text{Adv}_{\text{CPA}}(A, C) := |P(b' = 1|b = 0) - P(b' = 1|b = 1)| < \varepsilon(n)$$

Если шифрование детерминированное,
простая атака нарушает сем. стойкость:



Решения:

1. Рандомизированный алгоритм шифрования:

$E_r(k, m) = c_1$, повторно $E_r(k, m) = c_2$, с высокой вероятностью $c_1 \neq c_2$.

D - детерминированный алгоритм!

Длина шифротекста больше длины сообщения.

(Рисунок: $m \rightarrow \{c_1, \dots, c_t\} \rightarrow m$)

Пример реализации:

Пусть $f : K \times R \rightarrow M$ - ПСФ.

R - конечное множество чисел или других параметров.

Пусть $E(k, m) = [r \xleftarrow{R} R, \text{ вернуть } (r, f(k, r) \oplus m)]$

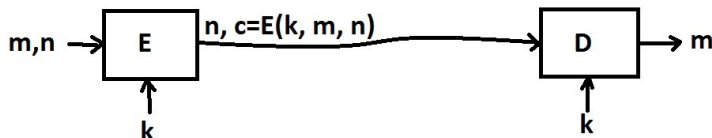
Задача

В каком случае этот шифр семант. стойкий относительно атаки с выбранным открытым текстом?

Подсказка: $f(k, \cdot) \approx$ случайная $g(\cdot)$.

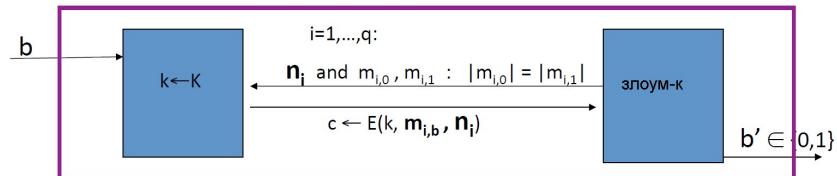
2. Использование nonce

nonce - уникальное значение, "n used once". Пара (n, m) никогда не повторится.



nonce:

- случайное число, выбир. из большого множества, так что оно никогда не повторится с большой вероятностью.
- счетчик (энегрoneзавис. память, можно не передавать nonce)

Эксперимент $n\text{CPA}$:

Все поппе n_i попарно различны, хоть их и выбирает злоум-к.

Опр.

шифр $C = (E, D)$, исп. поппе, семантически стойкий к атаке с выбранным открытым текстом, если $\forall A \in \text{PPT}$

$$\text{Adv}_{n\text{CPA}}[A, C] = |P(b' = 1 | b = 0) - P(b' = 1 | b = 1)| < \varepsilon(n).$$

Пример реализации:

Пусть $f : K \times R \rightarrow M$ - ПСФ.

R - конечное множество чисел.

Пусть $E(k, m) = [+ + r, \text{ вернуть } (r, f(k, r) \oplus m)]$

Задача

В каком случае этот шифр семант. стойкий относительно атаки с выбранным открытым текстом?

Некоторые итоги:

А. Стойкость шифров с одноразовым ключом:

А.1. Абсолютная стойкость к атаке с известным шифротекстом.

А.2. Семант. стойкость к атаке с известным шифротекстом.

В. Стойкость шифров с многоразовым ключом:

В.1. Семант. стойкость к атаке с выбором открытого текста.

С. Шифры:

С.1. Алфавитные.

С.2. Одноразовый блокнот.

С.3. Поточные шифры, ГПСЧ.

С.4. Блочные шифры. Шифр DES и его анализ.

D. Режимы использования блочных шифров:

D.1. ECB.

D.2. DetCTR.

D.3. Начали рассматривать использование многоразового ключа.

Литература к лекции:

1. D.Chang, M.Nandi, *A short proof of the PRP/PRF Switching Lemma*, <https://eprint.iacr.org/2008/078.ps>