Информационная безопасность

Симметричное шифрование

(презентация к лекции 1)

Амелин Р. В. Информационная безопасность. Конспект лекций // Амелин Р.В. Лаборатория преподавателя [Электронный ресурс]. URL: rv-lab.ru (2017).

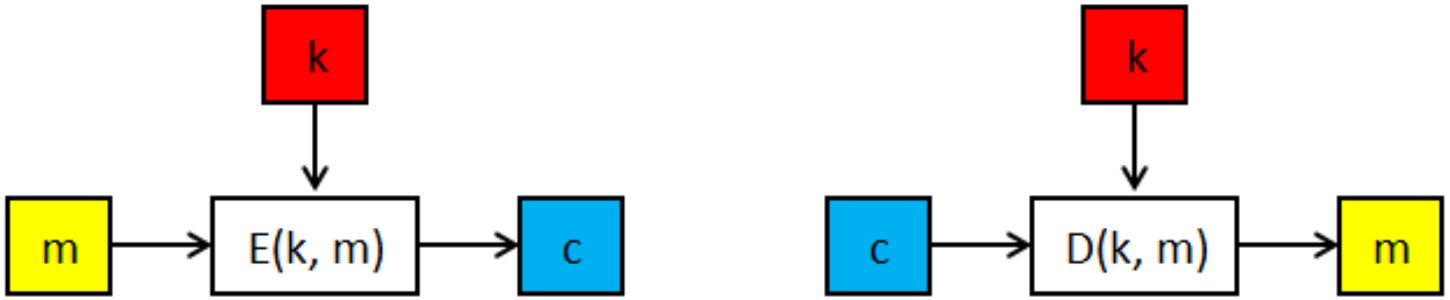
Базовая схема криптологии

Пассивный перехват: противник только наблюдает сообщения в канале связи;
Активный перехват: противник может изменять, удалять и добавлять поддельные сообщения

Симметричное шифрование

Симметричный шифр – это пара функций (E, D), таких что:

$c = E(k, m), m = D(k, c)$



E – функция шифрования (encrypt)

D – функция дешифрования (decrypt)

k – секретный ключ, известный отправителю и получателю сообщения (один и тот же ключ используется и для шифрования и для дешифрования)

m – сообщение или открытый текст

c – зашифрованный текст или шифртекст

Примеры классических шифров

Шифр Цезаря

M = криптография

M’ = нултхсёугчлв +3

K = ?

Принцип Керкгоффса

Надежность схемы шифрования
должна зависеть только
от секретности ключа и не зависеть
от секретности алгоритмов
шифрования и дешифрования

Примеры классических шифров

Модифицированный шифр Цезаря

$$M = \text{криптография}$$
$$M' = \text{нултхсёугчлв} \quad + K$$
$$K = 3$$

Атака на основе шифртекста – метод криптоанализа, при котором криптоаналитик располагает только зашифрованным сообщением или несколькими сообщениями, зашифрованными с использованием одного ключа. Целью является восстановление открытых текстов и/или восстановление ключа.

Эта атака *наиболее легко реализуема*, поскольку для ее осуществления необходим только перехват зашифрованного текста. В то же время это *наиболее слабый и неудобный вид атаки*.

Метод грубой силы или **полный перебор возможных ключей** – позволяет оценить криптостойкость алгоритма сверху.

Примеры классических шифров

Шифр простой замены

```
      абвгдеёжзийклмнопрстуфхцчшщъыьэюя
K =   йцукенгшщзхъэждлорпавыфячсмитьбюё
      а=й
      б=ц
      в=у
      . . .

M =   криптография
M′ =  ързоалкрйызё
```

Размер пространства ключей |K| = 33!

Устойчив к полному перебору

Атака на основе шифртекста: использование таблицы частот

pr(о) = 0.089; pr(е) = 0.072; pr(а) = 0.062; …; pr(ф) = 0.02

Примеры классических шифров

Шифр Гронсфельда

M = информатика
1231231231 2
M′ = йпчптпбфллв

K = 123

Криптоанализ только с зашифрованным текстом:

Каждая буква шифртекста отстоит от буквы открытого текста не более чем на 9 позиций

M = информатика
васявасявас
M′ = ложнунтсллт

K = вася

Криптоанализ только с зашифрованным текстом:

Если есть 2 сообщения, зашифрованных с одним ключом (или известна длина ключа), можно получить зависимость между ними (фрагментами одного сообщения)

Криптоанализ с известным открытым текстом:

Позволяет сразу восстановить исходное сообщение

Примеры классических шифров

Шифр Плейфейера

MONAR
CHYBD
EFGIK
LPQST
UVWXZ

K = MONARCHY

INFORMATION → GAPHMORSFAAW

Шифр Хилла

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}$$

Криптоанализ с избранным открытым текстом:

Зашифровать текст «БАА» (1 0 0)