ОБ АСИММЕТРИЧНО ВЫПОЛНИМЫХ СИММЕТРИЧНЫХ КРИПТОСИСТЕМАХ (ШИФРАХ)

- Варфоломеев Александр Алексеевич,
- канд. физ.-мат. н., доцент, МГТУ, МИФИ, РУДН, г. Москва, a.varfolomeev@mail.ru

Асимметрия в криптографии. Некоторые примеры.

- 1. Однонаправленные функции.
  - A: O(p(n)). Zl: экспоненциальная или субэкспоненциальная сложность.
- 2. Асимметричные шифры (Однонаправленные функции с секретом).
  - A - отправитель: O(p(n)),
  - B – получатель: O(p(n)),
  - Zl - злоумышленник: экспоненциальная или субэкспоненциальная сложность.
- 3. Протоколы открытого распределения ключей.
  - Шарады Меркля. «Secure communication over insecure channels». 1978г.
  - A - отправитель: O(2^d),
  - B – получатель: O(2^d),
  - Zl - злоумышленник: O(2^2d) .

Асимметрично выполнимые криптосистемы(шифры)

- A - отправитель: O(p(n)),
- B – получатель: O(p(n) *2^d),
- Zl - злоумышленник: O(2^(n+d)).

- d – параметр асимметрии.
- Пример. ГОСТ 28147- 89.
- Разовый ключ k - двоичный вектор длины 256 бит:
- k = (**k1, …, k56**, k57, …, k(56+d), **k(56+d+1), …, k256**).
- Последние 256 – 56-d бит положим фиксированными, например, нулями.
- Значимыми ключевыми битами, известными обоим законным участникам, будем считать первые 56 бит.

Различные определения понятия «ключ»

- **ГОСТ Р 34.12-2015. Блочные шифры.**
- **ИСО/МЭК 18033-1.**
- «Ключ(key) – изменяемый параметр в виде последовательности символов, **ОПРЕДЕЛЯЮЩИЙ** криптографическое преобразование».
- Однозначно определяющий?

- **«Словарь криптографических терминов». 2006.**
- «Ключ (криптосистемы) [key (of a cryptosystem)] — изменяемый элемент (параметр), каждому значению которого **ОДНОЗНАЧНО** соответствует одно из отображений, реализуемых криптосистемой.

Мотивация

- Постановления Правительства РФ от 16.04.2012 N 313 «Об утверждении **Положения о лицензировании** деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, …».

- Положение НЕ распространяется на деятельность с использованием:
- б) шифровальных (криптографических) средств, а также товаров, содержащих шифровальные (криптографические) средства, реализующих либо симметричный криптографический алгоритм, использующий криптографический ключ длиной, не превышающей 56 бит, либо асиметричный (так в ПП) криптографический алгоритм, основанный либо на методе разложения на множители целых чисел, размер которых не превышает 512 бит, либо на методе вычисления дискретных логарифмов в мультипликативной группе конечного поля размера, не превышающего 512 бит, либо на методе вычисления дискретных логарифмов в иной группе размера, не превышающего 112 бит;

Случай однозначного определения (1)

- Предложение Ривеста: преобразование AONT (All-Or-Nothing Transform).
- Преобразование f, отображающее последовательность знаков (блоков) открытого текста m_1, …, m_s в последовательность знаков (блоков) псевдотектса m`_1, …, m`_s`, называется **AON преобразованием (All-Or-Nothing Transform),** если
- (1) преобразование f обратимо;
- (2) преобразование f и его обратное преобразование f^(-1) эффективно вычисляемы, то есть имеют полиномиальную сложность;
- (3) вычислительно невозможно найти какие-нибудь знаки (блоки) открытого текста, если не известны все знаки (блоки) псевдотекста.
- Далее псевдотекст шифруется одним из режимов симметричного (блочного) шифрования.

Случай однозначного определения (2). Пример AONT.

- Для внесения случайности преобразования использовался случайный вектор K`, который вычислительно невозможно опробовать. Первые s значений псевдотекста получались по правилу:
- m`_i = m_i XOR E1(K`,i) для i=1,…,s.
- E1(K`,i) – преобразование зашифрования текста i на ключе K`.
- Значение m`_(s+1) = K` XOR h_1 XOR h_2 … XOR h_s,
- где h_i = E2(K_0, m`_i XOR i) для i= 1, …,s,
- а K_0 – известный всем двоичный вектор, играющий роль ключа в преобразовании E2 зашифрования.
- Все числа здесь представляются двоичными векторами соответствующих размеров.
- В оригинальной статье Ривеста рассматривался случай, когда E1 = E2 = E.

Случай однозначного определения (3). Трудоемкость.

- A: Трудоемкость выросла в 3 раза за счет предварительного преобразования открытого текста.
- B: Трудоемкость выросла в 3 раза за счет предварительного преобразования открытого текста.
- ZL: для опробования каждого варианта ключа необходимо получать не знаки открытого текста на длине работы критерия, а все знаки псевдотекста. И чем он длиннее, тем трудоемкость выше.
- Влияние выбора режима шифрования.

Случай однозначного определения (4). Влияние режимов шифрования.

- **ГОСТ 28147-89**
- Размер блоков – 64 битов.
- **Новый ГОСТ Р 34.13 – 2015 Режимы работы блочных шифров**
- 5.1 Режим простой замены
- 5.2 Режим гаммирования
- 5.3 **Режим гаммирования с обратной связью по выходу (s<n)**
- 5.4 Режим простой замены с зацеплением
- 5.5 **Режим гаммирования с обратной связью по шифртексту (s<n)**
- 5.6 Режим выработки имитовставки

Случай однозначного определения (5). Изменение в AONT

- m`_i = m_i XOR E1(K`,i) для i=1,…,s.
- E1(K`,i) – преобразование зашифрования текста i на ключе K`.
- Значение m`_(s+1) = K`XOR h_1 XOR h_2 … XOR h_s,
- где h_i = E2(K_0, m`_i XOR i) для i= 1, …,s,
- а K_0 – известный всем двоичный вектор, играющий роль ключа в преобразовании E2 зашифрования.

- Размер вектора K` можно увеличить, если использовать вместо шифрования вычисление хеш-функции по ГОСТ Р 34.11-2012, размер хэш-кода которой может быть равен 256 или 512 битам.
- Выбирать при AONT в векторе K_0 часть координат случайно, при их опробовании законным пользователем при расшифровании.
- или
- Не шифровать и не передавать часть координат значения вектора m`_(s+1), при их опробовании законным пользователем при расшифровании.

Случай однозначного определения (6). Практический пример.

- 56 бит ключ симметричного алгоритма шифрования
- 20 бит опробование на PC в течении 1 мин получателем (V= 10^9 оп/сек).
- открытый текст – 370 Кбайт.
- Режим шифрования - Режим гаммирования с обратной связью по шифртексту.
- Трудоемкость метода полного опробования увеличивается с порядка 2^56 до порядка 2^97 операций.

Другие технологии повышения стойкости.

- EKE – Encrypted Key Exchange (Bellovin S., Merritt M.) 1992г.
- Рассматривать парольное слово PW как 56 битовый ключ.
- 1. A: [A, E(PW, PKa)] → B ,
- 2. B: E(PW, E_PKa(k)) → A , k – высокоэнтропийный ключ.
- 3. …
- SESPAKE – Security Evaluated Standardized Password Authenticated Key Exchange (Алексеев Е., Ахметзянова Л., Ошкин И., Смышляев С.) 2016г.
- И др.
- **Система криптографическая** [cryptographic system (cryptosystem), син. *криптосистема]*— система обеспечения безопасности информации криптографическими методами в части *конфиденциальности, целостности, аутентификации, невозможности отказа* и *неотслеживаемости.* В качестве подсистем может включать *системы шифрования, системы идентификации, системы имитозащиты, системы подписи цифровой* и др., а также *систему ключевую,* обеспечивающую работу остальных систем. В основе выбора и построения с. к. лежит условие обеспечения *стойкости криптографической.*

Трудоемкость вскрытия

- **EKE – Encrypted Key Exchange (Bellovin S., Merritt M.) 1992г.**
- Рассматривать парольное слово PW как 56 битовый ключ.
- 1. A: [A, E(PW, PKa)] → B ,
- 2. B: E(PW, E_PKa(k)) → A , k – высокоэнтропийный ключ.
- 3. …

- O(2^56 * L_(1/3)[1,9018, 512])
- Если используется «**асимметричный криптографический алгоритм, основанный либо на методе разложения на множители целых чисел, размер которых не превышает 512 бит, либо на методе вычисления дискретных логарифмов в мультипликативной группе конечного поля размера, не превышающего 512 бит**»

Асимметрично выполнимые асимметричные криптосистемы

- RSA-OAEP (AONT)
- PK: n, e
- ?
- EL Gamal
- PK: g^x (mod p)
- ?

Заключение

- Стойкость криптосистем может быть существенно повышена даже при нормативных ограничениях ПП № 313 на размер ключей.
- «Словарь криптографических терминов» 2006 года – обновить и дополнить.