Лекция 12. Симметричные криптосистемы

1. Современные алгоритмы симметричного шифрования. Абсолютно стойкий шифр.
2. Криптосистемы DES и ГОСТ 28147-89.
3. Использование симметричных криптосистем. Генерация, хранение и распространение сеансовых ключей.

Современные симметричные криптоалгоритмы

- Потоковые (результат шифрования каждого бита открытого текста зависит от ключа шифрования и значения этого бита).
- Блочные (результат шифрования каждого бита открытого текста зависит от ключа шифрования и значений всех битов шифруемого блока и, возможно, предыдущего блока).

Потоковые шифры

- В основе лежит гаммирование. Криптостойкость полностью определяется структурой используемого генератора псевдослучайной последовательности (чем меньше период псевдослучайной последовательности, тем ниже криптостойкость потокового шифра).
- Основным преимуществом является высокая производительность. Эти шифры наиболее пригодны для шифрования непрерывных потоков открытых данных (например, в сетях передачи данных или связи).

Потоковые шифры

К наиболее известным относятся:

- RC4 (Rivest Cipher 4), разработанный Р. Ривестом (R.Rivest); в шифре RC4 может использоваться ключ переменной длины;
- SEAL (Software Encryption ALgorithm) – приспособленный для программной реализации потоковый шифр, использующий ключ длиной 160 бит;
- WAKE (Word Auto Key Encryption).

Блочные шифры

К наиболее распространенным способам построения блочных шифров относится *сеть Фейстела*, при использовании которой каждый блок открытого текста представляется сцеплением двух полублоков одинакового размера $L_0||R_0$. Затем для каждой итерации (раунда) i выполняется следующее:

1. $L_i=R_{i-1}$;
2. $R_i=L_{i-1} \oplus f(R_{i-1}, k_i)$, где

- f – функция шифрования;
- k_i – *внутренний ключ*, используемый на i-м раунде шифрования (k_i определяется исходным ключом шифрования открытого текста и номером раунда).

Название шифра	Длина блока	Раундов	Длина ключа
DES (Data Encryption Standard)	64	16	64 (8 контрольных)
3-DES (Triple-DES)	64	48	168
DESX (DES eXtended)	64	16	184
ГОСТ 28147-89 (ГОСТ Р 34.12-2015, «Магма»)	64	32	256
ГОСТ Р 34.12-2015, «Кузнечик»	128	10	256
IDEA (International Data Encryption Algorithm)	64	8	128
AES (Advanced Encryption Standard)	128	14	128, 192, 256
RC2 (Rivest Cipher 2)	64	Переменное	Переменная
RC5 (Rivest Cipher 5)	32, 64, 128	Переменное	Переменная
RC6 (Rivest Cipher 6)	Переменная	Переменное	Переменная
CAST (C.Adams, S.Tavares)	64	16	128
Blowfish	64	16	Переменная
SAFER+	128	8, 12, 16	128, 192, 256
Skipjack	64	32	80

Совершенный шифр

- ∀ X, Y p(X|Y)=p(X), где
  - p(X) – вероятность выбора для шифрования открытого текста X,
  - p(X|Y) – вероятность передачи открытого текста X при условии перехвата шифротекста Y.

Условия построения идеального (абсолютно стойкого) шифра

Определены К.Шенноном:

- ключ шифрования вырабатывается совершенно случайным образом;
- один и тот же ключ должен применяться для шифрования только одного открытого текста;
- длина шифруемого открытого текста не должна превышать длину ключа шифрования.

Условия К.Шеннона

К сожалению, в большинстве случаев выполнение этих условий обеспечить практически невозможно, хотя короткие и наиболее важные сообщения следует шифровать именно так. Для открытых текстов большой длины главной проблемой симметричной криптографии является генерация, хранение и распространение ключа шифрования достаточной длины.

Алгоритм DES

K – ключ шифрования (длина 64 бита, из которых 8 битов контрольных), IP – начальная перестановка битов в блоке открытого текста P длиной 64 бита, IP^{-1} – обратная к IP перестановка, L и R – соответственно левый и правый полублоки (длиной 32 бита) блока P, k_i – внутренний ключ шифрования i-го раунда длиной 48 бит (k_i=KS(i, K)), f – основная функция шифрования, на вход которой поступает блок длиной 32 бита, а на выходе формируется блок длиной также 32 бита.

Шифрование блока открытого текста P

1. $L_0R_0=IP(P)$.
2. Сеть Фейстела с количеством раундов, равным 16.
3. $C=IP^{-1}(R_{16}L_{16})$.

Алгоритм выполнения функции f

1. Расширение R_{j-1} до 48 бит путем копирования 16 крайних элементов из 8 четырехбитных подблоков исходного R_{i-1} (получение R_{i-1}').
2. $R_{i-1}' = R_{i-1}' \oplus k_i$.
3. Выполнение блока подстановки (S-бокса). На выходе блока подстановки получаем текст длиной 32 бита.
4. Выполнение блока перестановки (P-бокса), иначе называемого блоком проволочной коммутации.

Режимы работы DES

- В режиме *электронной кодовой книги* (Electronic Code Book, ECB) каждый блок открытого текста зашифровывается независимо от других блоков:

$\forall$ i, $1 \le i \le n$ $C_i = E_k(P_i)$

- Расшифрование в режиме ECB выполняется следующим образом:

$\forall$ i, $1 \le i \le n$ $P_i = D_k(C_i)$.

Режимы работы DES

- Режим *сцепления блоков шифра* (Cipher Block Chaining, CBC): каждый блок открытого текста перед шифрованием складывается по модулю 2 с предыдущим блоком шифротекста, а первый блок – с *вектором инициализации* (синхропосылкой) IV (дополнительным параметром шифра, который должен сохраняться и передаваться вместе с ключом шифрования):

$\forall i,\ 1 \le i \le n\ C_i = E_k(P_i \oplus C_{i-1}),\ C_0 = IV.$

- Расшифрование в режиме CBC выполняется так:

$\forall i,\ 1 \le i \le n\ P_i = C_{i-1} \oplus D_k(C_i),\ C_0 = IV.$

Режимы работы DES

- Последний блок шифротекста C_n является функцией ключа шифрования, вектора инициализации и всех блоков открытого текста – кодом аутентификации сообщения (Message Authentication Code, MAC).
- Блок MAC может использоваться для проверки подлинности и целостности полученного сообщения с помощью тех же значений ключа и вектора инициализации.

Режимы работы DES

- Режим *обратной связи по шифротексту* (Cipher FeedBack, CFB) использует регистр замены (сдвига), в который первоначально помещается вектор инициализации. После шифрования блока в регистре замены происходит его сдвиг влево (например, на ¼ длины регистра замены), и сложение по модулю 2 вытесняемой части регистра с очередной порцией открытого текста. Результат последней операции образует очередную порцию шифротекста и одновременно помещается в освободившуюся часть регистра сдвига:

$\forall\ i,\ 1 \le i \le m\ C_i = P_i \oplus E_k(C_{i-1}),\ C_0 = IV$ (m – количество порций открытого текста).

- Расшифрование в режиме CFB производится следующим образом:

$\forall\ i,\ 1 \le i \le m\ P_i = C_i \oplus E_k(C_{i-1}),\ C_0 = IV.$

Режимы работы DES

- Последний блок шифротекста зависит ото всех блоков открытого текста, а также от вектора инициализации и ключа шифрования, поэтому он также может использоваться в качестве кода аутентификации сообщения.

Режимы работы DES

- В режиме *обратной связи по выходу* (Output FeedBack, OFB) также используются регистр замены и вектор инициализации. После шифрования блока в регистре замены и сдвига вытесняемая часть замещает свободную область регистра и одновременно складывается по модулю 2 с очередной порцией открытого текста. Результат последней операции и образует очередную порцию шифротекста:

$\forall$ i, $1 \le i \le m$ $C_i = P_i \oplus S_i$, $S_i = E_k(S_{i-1})$, $S_0 = IV$ (m – количество порций открытого текста).

- Расшифрование в режиме OFB производится так:

$\forall$ i, $1 \le i \le m$ $P_i = C_i \oplus S_i$, $S_i = E_k(S_{i-1})$, $S_0 = IV$.

Модификации DES

- В тройном DES (3-DES) к одному и тому же блоку открытого текста P функция шифрования применяется трижды с тремя разными ключами (k1, k2 и k3), что обеспечивает увеличение длины ключа окончательного шифрования и количества раундов в три раза:

$C=E_{k3}(D_{k2}(E_{k1}(P)))$.

- Расшифрование выполняется следующим образом:

$P=D_{k1}(E_{k2}(D_{k3}(C)))$.

- На втором шаге тройного DES используется не функция шифрования, а функция расшифрования, поскольку при k1=k2=k3 результат шифрования по алгоритму 3-DES совпадает с шифрованием по алгоритму DES на ключе k1.

Модификации DES

- Недостатком алгоритма 3-DES является снижение производительности шифрования в три раза по сравнению с алгоритмом DES. Этого недостатка лишен алгоритм DESX:

$C=k2 \oplus E_k(k1 \oplus P)$, где

- k – ключ DES-шифрования длиной 56 бит;
- k1 и k2 – дополнительные ключи шифрования длиной 64 бита каждый.
- Общая длина ключа шифрования, используемого в алгоритме DESX, составляет, таким образом, 184 бита. Расшифрование шифротекста по алгоритму DESX производится следующим образом:

$P=D_k(C \oplus k2) \oplus k1$.

Особенности алгоритма ГОСТ 28147-89

- Используется ключ шифрования k длиной 256 бит, который может рассматриваться как массив из 8 32-битных элементов k_0, k_1, … , k_7 (внутренних ключей).
- Дополнительным ключевым элементом алгоритма является таблица замен H, представляющая собой матрицу из 8 строк и 16 столбцов, элементы которой – целые числа от 0 до 15. Каждая строка таблицы замен должна содержать 16 различных чисел. Таким образом, общий размер таблицы замен составляет 512 бит.

Основная функция шифрования

N – преобразуемый блок длиной 64 бита, K – один из внутренних ключей шифрования длиной 32 бита. $N=N_1||N_2$ (два полублока по 32 бита).

1. $S=N_1+K \{mod\ 2^{32}\}$, $S=S_0S_1\ldots S_7$ (8 элементов по 4 бита).
2. $\forall\ i=0, 1, \ldots, 7: S_i=H[i, S_i]$.
3. Циклический сдвиг S на 11 бит влево.

Режимы ГОСТ 28147-89

- Режим *простой замены* соответствует режиму ECB криптосистемы DES.
- Режим *гаммирования* похож на режим OFB криптосистемы DES, но не используется регистр сдвига, а блоки открытого текста складываются с результатом шифрования очередного элемента псевдослучайной последовательности, генерируемой на основе двух рекуррентных соотношений – одного для старшей части псевдослучайного числа и другого для младшей части.

Режимы ГОСТ 28147-89

- Режим *гаммирования с обратной связью* похож на режим CFB криптосистемы DES, но в нем не используется регистр сдвига.
- Дополнительный режим *выработки имитовставки* используется с одним из основных режимов и предназначен для обеспечения подлинности и целостности шифротекста:

$\forall$ i, $1 \le i \le n$ $S_i = E_k(S_{i-1} \oplus P_i)$, $S_0 = 0$ (в качестве имитовставки берется младшая часть (32 бита) полученного двоичного числа S_n)

Использование симметричной криптосистемы для создания защищенного канала связи

1. Безопасное создание, распространение и хранение сеансового ключа k.
2. Получение шифротекста для открытого текста $C=E_k(P)$.
3. Вычисление имитовставки (кода аутентификации сообщения, MAC) для открытого текста P и присоединение ее к шифротексту:
   - Вычисление MAC.
   - C’=C || MAC.
4. Передача шифротекста по незащищенному каналу связи.

Использование симметричной криптосистемы для создания защищенного канала связи

5. Отделение имитовставки (кода аутентификации сообщения, MAC) от шифротекста C’=C || MAC.
6. Расшифрование полученного шифротекста (неявная аутентификация полученного шифротекста, так как только имевший сеансовый ключ k мог выполнить шифрование) $P=D_k(C)$.
7. Вычисление имитовставки (кода аутентификации сообщения, MAC) для полученного открытого текста.
8. Сравнение полученного и вычисленного MAC (проверка целостности полученного открытого текста).

Генерация ключей

- Генерация случайного ключа шифрования возможна с помощью программного или аппаратного датчика псевдослучайных чисел и случайных событий, создаваемых пользователем при нажатии клавиш на клавиатуре или движением мыши. Ключ шифрования будет в этом случае создан из элементов псевдослучайной последовательности, соответствующих моментам возникновения инициированных пользователем событий.

Генерация ключей

- Другой источник случайных событий – аппаратные средства компьютера («шум» звуковой карты, счетчик тактов процессора и т.п.).

Хранение ключей

- Общедоступные электронные носители (ключи должны храниться только в зашифрованном с помощью мастер-ключа виде). Мастер-ключ не зашифровывается, но хранится в защищенной части аппаратуры КС (например, на смарт-карте или токене), причем его потеря в результате аппаратной ошибки не должна приводить к потере зашифрованных с его помощью данных.

Распределение ключей

- С помощью центров распределения ключей (Key Distribution Center, KDC). На каждом объекте КС должен храниться ключ шифрования для связи с KDC. Недостатком применения центра распределения ключей является то, что в KDC возможно чтение всех передаваемых в КС сообщений. Для организации анонимного распределения ключей симметричного шифрования могут использоваться протоколы, основанные на криптографии с открытым ключом.

Распределение ключей

- С помощью прямого обмена данными между субъектами КС. Основной проблемой при этом является взаимное подтверждение подлинности субъектов сети. Для решения этой задачи могут применяться протоколы «рукопожатия». Для этого также используются методы асимметричной криптографии (например, криптосистема Диффи-Хеллмана).