Билет №2.24

Шифрование с открытым ключом. Алгоритмы RSA и Эль-Гамаля. Методы распределение ключей. Алгоритмы разделения секрета.

1 Шифрование с открытым ключом

Криптографическая система с открытым ключом (или **Асимметричное шифрование, Асимметричный шифр**) — система шифрования в которой открытый ключ передаётся по незащищённому каналу, и используется только для шифрования сообщения. Для расшифровывания сообщения используется секретный ключ.

Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах *TLS* и его предшественнике *SSL* (лежащих в основе *HTTPS*), а так же *SSH*, *PGP*, *S/MIME* и т. д.

Рассмотрим случай, когда отправитель хочет послать получателю секретное сообщение.

1. Получатель генерирует 2 ключа. Один их них открытый, другой закрытый (секретный). При этом закрытый ключ не должен передаваться по открытому каналу.
2. Отправитель с помощью открытого ключа шифрует сообщение.
3. Получатель с помощью закрытого ключа дешифрует сообщение.

1.1 Преимущества

Преимущество асимметричных шифров перед симметричными шифрами состоит в отсутствии необходимости предварительной передачи секретного ключа по надёжному каналу. Сторона, желающая принимать зашифрованные тексты, в соответствии с используемым алгоритмом вырабатывает пару «открытый ключ — закрытый ключ». Значения ключей связаны между собой, однако вычисление закрытого ключа по открытому должно быть невозможным с практической точки зрения. Открытый ключ публикуется в открытых справочниках и используется для шифрования информации контрагентоми. Закрытый ключ держится в секрете и используется для расшифровывания сообщения, переданного владельцу пары ключей. Для удостоверения аутентичности самих публичных ключей, передаваемых по открытому каналу или получаемых из справочника, обычно используют сертификаты.

1.2 Недостатки

Асимметричные криптосистемы в чистом виде требуют существенных вычислительных ресурсов, потому на практике используются в сочетании с другими алгоритмами. Обычно сообщение шифруют временным (сессионным) симметричным ключом, а сам симметричный ключ шифруют асимметричным.

1.3 Электронная цифровая подпись

Для ЭЦП сообщение предварительно подвергается хешированию, а с помощью асимметричного ключа подписывается лишь относительно небольшой результат хеш-функции.

2 Алгоритмы RSA и Эль-Гамаля

2.1 RSA

Описание **RSA** было опубликовано в 1977 году *Рональьдом Райвестом (Ronald Linn Rivest), Ади Шамиром (Adi Shamir)* и *Леонардом Адлеманом (Leonard Adleman)* из MIT.

Принцип работы шифросистемы. Для того, чтобы сгенерировать пару ключей выполняются следующие действия:

1. Выбираются два больших случайных простых числа p и q.
2. Вычисляется их произведение $n = pq$.
3. Вычисляется Функция Эйлера $\varphi(n) = (p-1)(q-1)$. (**Функция Эйлера** $\varphi(n)$, где n — натуральное число, равна количеству натуральных чисел, не больших n и взаимно простых с ним.)

4. Выбирается целое e такое, что $1 < e < \varphi(n)$ и e взаимно простое с $\varphi(n)$.

5. С помощью расширенного алгоритма Евклида находится число d такое, что $ed \equiv 1 \pmod{\varphi(n)}$. Это значит, что $de = 1 + k\varphi(n)$ при некотором целом k.

Число n называется модулем, а числа e и d — открытой и секретной экспонентами, соответственно. Пара чисел (n, e) является открытой частью ключа, а d — секретной. Числа p и q после генерации пары ключей могут быть уничтожены, но ни в коем случае не должны быть раскрыты.

Шифрование. Для того, чтобы зашифровать сообщение $m < n$ вычисляется $c = m^e \bmod n$. Число c и используется в качестве шифротекста.

Дешифрование. Для расшифровывания нужно вычислить $m = c^d \bmod n$. Нетрудно убедиться, что при расшифровывании мы восстановим исходное сообщение:

$$c^d \equiv (m^e)^d \equiv m^{ed} \pmod{n}.$$

Из условия $ed \equiv 1 \pmod{\varphi(n)}$ следует, что $ed = k\varphi(n) + 1$ для некоторого целого k, следовательно

$$m^{ed} \equiv m^{k\varphi(n)+1} \pmod{n}.$$

Согласно теореме Эйлера $m^{\varphi(n)} \equiv 1 \pmod{n}$, поэтому

$$m^{k\varphi(n)+1} \equiv m \pmod{n} \quad \Rightarrow \quad c^d \equiv m \pmod{n}.$$

Криптостойкость. Безопасность RSA основана на трудности задачи разложения на множители.

Цифровая подпись. RSA может использоваться не только для шифрования, но и для цифровой подписи. Подпись s сообщения m вычисляется с использованием секретного ключа по формуле: $s = m^d \bmod n$. Для проверки правильности подписи нужно убедиться, что выполняется равенство $m = s^e \bmod n$.

2.2 Elgamal

Шифросистема **Эль-Гамаля** *(Elgamal)* — была предложена в 1984 году. В частности стандарты электронной цифровой подписи в США и России базируются именно на ней.

Принцип работы шифросистемы.

1. Генерируется случайное простое число p.

2. Выбираются случайные числа x и g так, что $1 < x < p$, $1 < g < p$.

3. Вычисляется $y = g^x \mod p$.

Открытым ключом является тройка (p, g, y), закрытым ключом — число x.

Шифрование. Будем обозначать исходное сообщение M.

1. Выбирается случайное секретное число k, взаимно простое с $p - 1$.

2. Вычисляется $a = g^k \bmod p$, $b = y^k M \bmod p$, где M — исходное сообщение.

Пара чисел (a, b) является шифротекстом. При этом длина шифротекста больше длины исходного сообщения M вдвое.

Дешифрование. Зная закрытый ключ x, исходное сообщение получается из шифротекста (a, b) по формуле: $M = b/a^x \bmod p$.

Нетрудно проверить, что

$$a^x \equiv g^{kx} \pmod{p} \quad \text{и} \quad \frac{b}{a^x} \equiv \frac{y^k M}{a^x} \equiv \frac{g^{xk} M}{g^{xk}} \equiv M \pmod{p}.$$

Криптостойкость. Криптостойкость данной схемы основана на сложности проблемы дискретного логарифмирования (по известным p, g и y приходится искать показатель степени x: $y \equiv g^x \pmod p$).

3 Методы распределение ключей

Протокол распределения ключей *([secret] key distribution [agreement, sharing, exchange, generation] protocol)* — это протокол, который позволяет его участникам выработать общую секретную информацию (общий секретный ключ), обмениваясь сообщениями по открытым для прослушивания каналам. В протоколе может предполагаться наличие некоторого дополнительного участника, пользующегося абсолютным доверием всех остальных участников, которого мы будем называть центром доверия. Подчеркнем, что перед началом выполнения протокола не предполагается наличие у участников какой-либо общей секретной информации. В процессе выполнения протокола участники обмениваются сообщениями по открытым каналам связи, после чего каждый участник вычисляет свой элемент некоторого множества K, называемого пространством ключей. Если все участники вычислили один и тот же элемент из K, то этот элемент и является общим секретным ключом.

Задача противника состоит в вычислении общего секретного ключа. Для этого он может как просто подслушивать сообщения участников друг другу *(пассивный противник (passive adversary, eavesdropper))*, так и вмешаться в выполнение протокола путем замены сообщений участников своими сообщениями, выдавая себя за одного из законных участников *(активный противник (active adversary, impersonator))*.

3.1 Алгоритм Диффи-Хелмана

Эта схема используется в *SSL*. Рассмотрим взаимодействие двух участников — Алисы и Боба.

1. Алиса и Боб выбирают конечную циклическую группу G и элемент $g \in G$. (Это обычно происходит заранее: G и g являются публичными данными, т. е. известными всем противникам.)
2. Алиса выбирает случайное число a и посылает Бобу g^a.
3. Боб выбирает случайное число b и посылает Алисе g^b.
4. Алиса вычисляет $K = (g^b)^a$.
5. Боб вычисляет $K = (g^a)^b$.

Боб и Алиса оба обладают элементом g^{ab} группы G, который они могут использовать как секретный ключ. Перед противниками стоит задача зная G, g, g^a и g^b определить g^{ab}. Считается, что эта задача *(проблема Диффи-Хелмана)* сложна.

4 Алгоритмы разделения секрета

С помощью алгоритмов разделения секрета можно разбить информацию на доли таким образом, что пока у вас не будет необходимого количества долей, вы не будете иметь никакого представления об этой информации, но если вы соберете нужное количество долей, то сможете ее восстановить.

Более формально, в схеме разделения секрета выделяется *дилер (dealer)* и n игроков. Дилер распределяет секрет между игроками таким образом, чтобы любая группа из t игроков (t называется *порогом*) могла восстановить секрет, но никакая группа из меньшего количества игроков не могла бы этого сделать. Такая система называется (t, n) пороговой схемой.

Для примера, представим, что дилер разделил секретное слово "`password`" на 4 части "`pa------`," "`--ss----`," "`----wo--`," и "`------rd`", и раздал 4 игрокам. Даже если соберется группа из 3 игроков, им придется гадать над значением неизвестных двух букв.

4.1 Тривиальные схемы

Пусть $t = n$. Рассмотрим следующие схемы.

1. Секрет — секретное число s. Дилер посылает каждому игроку $i \neq n$ случайное число r_i, а игроку с номером n число
$$s - r_1 - r_2 - \cdots - r_{n-1}.$$
Секрет равен сумме чисел, которые есть у игроков.

2. Секрет — число s с фиксированным числом битов. Дилер посылает каждому игроку $i \neq n$ случайное число b_i, а игроку с номером n
$$s \oplus b_1 \oplus b_2 \oplus \cdots \oplus b_{n-1}.$$
   Секрет равен XOR-у всех чисел, которые дилер послал игрокам.

4.2 Пороговая схема Шамира

Основная идея пороговой схемы Шамира заключается в том, что 2 точки задают прямую, 3 точки — параболу, 4 точки — кубическую кривую и т. д. Таким образом, нужна $n+1$ точка, чтобы определить полином степени n.

Предположим, необходимо построить (t, n) пороговую схему для разделения секрета s (НУО, будем считать s числом).

1. Дилер выбирает $t-1$ коэффициент $a_1, \ldots, a_{k-1}$ и полагает $a_0 = s$.

2. Определяет функцию $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-1} x^{k-1}$.

3. Посылает каждому игроку i пару $(i, f(i))$.

Таким образом, любая группа из k игроков располагает k точками, а значит может восстановить f по этим точкам и определить a_0, т. е. секрет s.

4.3 Схема Блекли

Две не параллельные прямые пересекаются в одной точке, три не параллельные плоскости также пересекаются в одной плоскости. В общем случае n n-размерных гиперплоскостей (из $\mathbb{R}^n$) пересекаются в одной точке.

Аналогично предыдущей схеме, построим (t, n) пороговую схему для разделения секрета s (НУО, будем считать s числом).

1. Дилер кодирует секрет в одной из координат некоторой точки в пространстве $\mathbb{R}^t$. (Если дилер закодирует сразу во всех координатах, то какой-нибудь противник сможет располагая набором из менее чем t “кусочков” сможет получить дополнительную информацию о секрете, т. к. он знает, что точка лежит на его плоскости.)

2. Дилер генерирует n непараллельных t-размерных гиперплоскостей, пересекающихся в точке с секретом, и посылает по одной каждому игроку.

Секрет в группе из t игроков восстанавливается посредством вычисления точки пересечения t гиперплоскостей.

Замечание. Схема Блекли менее эффективна по размеру посылаемых сообщений по сравнению со схемой Шамира. Это можно исправить введя ограничения на плоскости. Получившаяся схема будет эквивалентна схеме Шамира.