СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

А.Б. Левина

Криптография и криптографические протоколы

Гибридное шифрование

СПбГЭТУ «ЛЭТИ», 2022 г.

1. ВВЕДЕНИЕ

Продолжаем наше знакомство с **асимметричным шифрованием**, а вернее с примерами его комбинации с **симметричным.**

Сегодня на нашей лекции будет рассмотрено:

1. Гибридные криптосистемы.
2. Сравнение симметричного и асимметричного шифрования.

2. ГИБРИДНЫЕ КРИПТОСИСТЕМЫ

Рассмотрим работу гибридных криптосистем.

Определение 4.2.1 ***Гибридная (или комбинированная) криптосистема*** *— это система шифрования, совмещающая криптосистемы с открытым ключом с симметричными криптосистемами для решения проблемы передачи ключа при небольших временных затратах.*

Схематически работа гибридной криптосистемы представлена на рисунке 1:

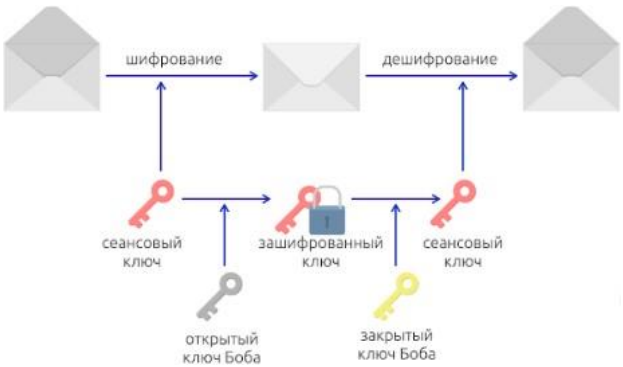

Рис. 1: Работа гибридной криптосистемы

Давайте разберем где же здесь у нас идет симметричное, а где асимметричное шифрование.

Мы помним, что асимметричное шифрование решает проблему передачи ключа, соответственно ключ в гибридных системах мы генерируем и передаем с помощью асимметричного шифрование. То есть Алиса сгенерировала сеансовый ключ с помощью **открытого** ключа Боба, он, зная свой **закрытый** ключ смог дешифровать сеансовый ключ, присланный Евой, и у них у обоих есть общий сеансовый ключ. Далее они уже шифруют информацию с помощью симметричного шифрования.

1. Этап отправки:

1. Алиса генерирует случайный сеансовый ключ;
2. Сообщение Алисы шифруется сеансовым ключом (**с помощью симметричного алгоритма**);
3. Сеансовый ключ шифруется открытым ключом Боба (**асимметричным алгоритмом**);
4. Алиса посылает Бобу зашифрованное сообщение и зашифрованный сеансовый ключ.

2. Этап приёма:

1. Боб получает зашифрованное сообщение Алисы и зашифрованный сеансовый ключ;
2. Боб расшифровывает сеансовый ключ своим закрытым ключом (**асимметричный алгоритм**);
3. При помощи полученного, таким образом, сеансового ключа Боб расшифровывает зашифрованное сообщение Алисы (**симметричный алгоритм**).

И вот теперь, наконец, мы получили прекрасную криптосистему, соединяющую в себе все плюсы симметричного и асимметричного шифрования, и лишенную их минусов.

Гибридные криптосистемы используются в протоколах PGP, TLS, SSL, Web-браузерах и Web-сервисах.

3. КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ, СРАВНЕНИЕ С СИММЕТРИЧНЫМИ КРИПТОСИСТЕМАМИ

Давайте обсудим плюсы и минусы криптосистем с открытым ключом.

- **Преимущества:**

1. не нужно предварительно передавать секретный ключ по надёжному каналу;
2. только одной стороне известен ключ дешифрования, который нужно держать в секрете;
3. в больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

Несмотря на то, что криптосистемы с открытым ключом полностью решили проблему передачи ключа, они не смогли вытеснить симметричное шифрование из-за ряда недостатков.

- **Недостатки:**

1. в алгоритм сложнее внести изменения;
2. более длинные ключи.

Рассмотрим при каких длинах ключа симметричное и асимметричное шифрование обеспечивают одинаковый уровень безопасности. В таблице, на рисунке 2, сопоставлена длина ключа симметричного алгоритма с длиной ключа RSA с аналогичной криптостойкостью.

Длина симметричного ключа	Длина ключа RSA
56 бит	384 бит
64 бит	512 бит
80 бит	768 бит
112 бит	1792 бит
128 бит	2304 бит

Рис. 2: Сравнение длин ключа симметричного шифрования с длиной ключа RSA с аналогичной криптостойкостью

Как мы видим, асимметричное шифрование проигрывает здесь в разы. Для асимметричного шифрования требуются существенно более мощные вычислительные ресурсы, поэтому на практике асимметричные криптосистемы используются в сочетании с другими алгоритмами:

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

2. для шифрования, асимметричные криптосистемы используются в форме гибридных криптосистем, где большие объёмы данных шифруются симметричным шифром на сеансовом ключе, а с помощью асимметричного шифра передаётся только сам сеансовый ключ.

На следующих лекциях мы познакомимся подробно с хеш-функциями и ЭЦП.

Алгоритмы асимметричного шифрования можно использовать:

1. как самостоятельное средство для защиты передаваемой и хранимой информации,

2. как средство распределения ключей,

3. как средство аутентификации пользователей.

Наиболее известны следующие алгоритмы:

1. Алгоритм RSA (Rivest-Shamir-Adleman) - основан на задаче RSA;

2. Алгоритм DSA (Digital Signature Algorithm) - алгоритм подписи;

3. Криптосистема Elgamal (Эль-Гамаль) - основана на задаче Дискретного Логарифмирования;

4. Алгоритм Diffie-Hellman (обмен ключами Диффи — Хелмана) - основан на задаче ДХ;

5. Алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm) — алгоритм с открытым ключом для создания цифровой подписи на эллиптических кривых;

6. Алгоритм ГОСТ Р 34.10-2012;

7. Криптосистема Rabin - основана на задаче извлечения квадратичных корней;

8. Криптосистема McEliece - криптосистема рюкзак;

9. Криптосистема Уильямса - была разработана на замену RSA.

Рассмотрев все минусы и плюсы асимметричного шифрования, мы поняли, что асимметричное шифрование надо комбинировать с симметричным, что бы взять все лучшее из двух направлений, и как раз для этого были придуманы гибридные криптосистемы.

4. ЗАКЛЮЧЕНИЕ

В этой лекции мы рассмотрели работу гибридных криптосистем и провели сравнение асимметричного и симметричного шифрования.