Лекция 13. Асимметричные криптосистемы

1. Принципы создания и свойства асимметричных криптосистем.
2. Криптосистемы RSA и Диффи-Хеллмана.
3. Электронная подпись и ее использование.

Принципы построения асимметричных криптосистем

В основе асимметричных криптографических систем лежит понятие однонаправленной функции f, обладающей следующими свойствами:

1. простое (не требующее больших ресурсов) вычисление значения функции $y=f(x)$;
2. существование обратной функции f^{-1};
3. сложное (требующее ресурсов за переделами возможностей современных компьютеров) вычисление значения обратной функции $x=f^{-1}(y)$.

Принципы построения асимметричных криптосистем

- Фактически в асимметричной криптографии используется подкласс однонаправленных функций – однонаправленные функции с обходными путями, для которых обратная функция может быть вычислена так же просто, как и прямая, только если известна специальная информация об обходных путях. Эта специальная информация исполняет роль секретного (закрытого) ключа.

Требования к асимметричным криптосистемам

Пусть pk – открытый ключ, а sk –закрытый ключ. Должны выполняться следующие условия:

1. $D_{sk}(E_{pk}(P))=P$ (расшифрование должно восстанавливать открытый текст P).
2. Функции E_{pk} и D_{sk} должны быть просты в реализации.
3. При раскрытии преобразования, выполняемого с помощью E_{pk}, не должно раскрываться преобразование, выполняемое с помощью D_{sk} (из открытого ключа нельзя получить закрытый ключ).

Требования к асимметричным криптосистемам

4. $D_{pk}(E_{sk}(P))=P$ (возможно использование закрытого ключа для шифрования, а открытого – для расшифрования).

- Четвертое условие является необязательным и не все асимметричные криптосистемы им обладают. Оно необходимо для использования асимметричной криптосистемы в механизме электронной цифровой подписи.

Применение асимметричных криптосистем

- Шифрование и расшифрование коротких сообщений.
- Передача ключа симметричного шифрования по открытой сети (отправитель зашифровывает этот ключ с помощью открытого ключа получателя, который только и сможет расшифровать полученное сообщение с помощью своего закрытого ключа) – обмен ключами.

Передача сеансового ключа по открытому каналу

Отправитель A:

1. Генерация сеансового ключа k.
2. Шифрование открытого текста P с помощью симметричного криптоалгоритма и сеансового ключа: $C=E_k(P)$.
3. Шифрование сеансового ключа с помощью асимметричного криптоалгоритма и открытого ключа получателя pkb: $EK=E_{pkb}(k)$.
4. Передача получателю C и EK.

Передача сеансового ключа по открытому каналу

Получатель B:

1. Расшифрование сеансового ключа с помощью асимметричного криптоалгоритма и своего закрытого ключа skb: $k=D_{skb}(EK)$.
2. Расшифрование шифротекста и восстановление открытого текста с помощью симметричного криптоалгоритма и сеансового ключа: $P=D_k(C)$.

Применение асимметричных криптосистем

- В системах электронной подписи для защиты электронных документов (создатель документа удостоверяет его подлинность с помощью своего закрытого ключа, после чего любой владелец соответствующего открытого ключа сможет проверить аутентичность и целостность данного документа) – асимметричная криптосистема должна удовлетворять четвертому из приведенных ранее условий.

Свойства асимметричных криптосистем

- К особенностям современных асимметричных криптосистем, которые не позволяют им полностью заменить симметричные криптосистемы, относятся:
- большая продолжительность процедур шифрования и расшифрования (примерно в 1000 раз больше);
- необходимость использования существенно более длинного ключа шифрования для обеспечения той же криптостойкости шифра (например, симметричному ключу длиной 56 бит будет соответствовать асимметричный ключ длиной 384 бита, а симметричному ключу длиной 112 бит – асимметричный ключ длиной 1792 бита).

Современные асимметричные криптосистемы

- RSA (стойкость основана на вычислительной сложности задачи факторизации произвольного целого числа).
- Диффи-Хеллмана (стойкость основана на вычислительной сложности задачи дискретного логарифмирования).
- Эль-Гамаля (модификация криптосистемы Диффи-Хеллмана для использования в системах электронной подписи).

Современные асимметричные криптосистемы

- На основе эллиптических кривых (стойкость основана на вычислительной сложности задачи отыскания одной из двух точек кривой, которая вместе с известной другой точкой использовалась для получения третьей точки кривой).

Криптосистема RSA

RSA (Rivest, Shamir, Adleman).

Выбор ключей шифрования:

1. выбираются два больших простых числа p и q;
2. вычисляется значение модуля $n=p \bullet q$;
3. выбирается достаточно большое целое число y (или d), которое является взаимно простым с $\varphi(n)$ и вместе с n образует закрытый ключ шифрования (y, n) ($\varphi(n)$ – функция Эйлера);
4. вычисляется целое число x (или e), которое является мультипликативно обратным числу y по модулю $\varphi(n)$ и вместе с n образует открытый ключ шифрования (x, n).

Криптосистема RSA

Шифрование по алгоритму RSA выполняется следующим образом:

$C=P^x \{mod\ n\}$, где

- P – открытый текст;
- C – шифротекст.

Для расшифрования шифротекста производится следующее действие:

$P=C^y \{mod\ n\}$. Если P и n являются взаимно простыми, то $C^y \{mod\ n\}=(P^x)^y \{mod\ n\}=P^{xy} \{mod\ n\}=P^{1+\varphi(n)\bullet k} \{mod\ n\}=P\bullet P^{\varphi(n)\bullet k} \{mod\ n\} = P\bullet 1^k \{mod\ n\}=P$ (из теоремы Эйлера).

Криптосистема RSA

- Если криптоаналитику удастся разложить n на множители p и q, то он сможет вычислить значение φ(n)=(p-1)(q-1), затем определить значение y и раскрыть тем самым параметры шифрования. На современном уровне развития компьютерных технологий значение n должно содержать не менее 1024 бит.

Криптосистема RSA

Пример. Зашифровать и расшифровать P=33. Выбор ключей: p=5, q=11, n=55, φ(n)=40, y=7 (взаимно простое с φ(n)), x=23 (x·y=1 {mod φ(n)}.

Шифрование. P<n. $C=33^{23}\{\text{mod } 55\}=3^{23}\{\text{mod } 55\}\cdot 11^{23}\{\text{mod } 55\}$. $C_1=3^{23}\{\text{mod } 55\}=3^{16}\cdot 3^4\cdot 3^3\{\text{mod } 55\}=26^4\cdot 26\cdot 27\{\text{mod } 55\}=2^4\cdot (13^2)^2\cdot 2\cdot 13\cdot 3\cdot 9\{\text{mod } 55\}=16\cdot 16\cdot 2\cdot 7\cdot 3\ \{\text{mod } 55\}=2\cdot 41\ \{\text{mod } 55\}=27$. $C_2=11^{23}\ \{\text{mod } 55\}=11^{16}\cdot 11^4\cdot 11^2\cdot 11\{\text{mod } 55\}=11^8\cdot 11^2\cdot 11\cdot 11\{\text{mod } 55\}=11$. $C=27\cdot 11\{\text{mod } 55\}=3\cdot 9\cdot 11\{\text{mod } 55\}=3\cdot 44\{\text{mod } 55\}=22$.

Продолжение примера

Расшифрование. $P=22^{7}\{\text{mod } 55\} = 2^{7}\cdot 11^{7} \{\text{mod } 55\} = 18\cdot 11 \{\text{mod } 55\} = 2\cdot 9\cdot 11 \{\text{mod } 55\} = 2\cdot 44 \{\text{mod } 55\} = 33.$

Криптосистема Диффи-Хеллмана

Предназначена только для генерации ключа симметричного шифрования, который затем будет использован субъектами A и B для защищенного обмена сообщениями по открытой сети:

1. A: выбирает x_a и вычисляет $y_a = a^{xa} \{mod\ p\}$ (p – простое число или степень простого числа, $1<a<p-1$).
2. B: выбирает x_b и вычисляет $y_b = a^{xb} \{mod\ p\}$.
3. A->B: y_a.
4. B->A: y_b.

Криптосистема Диффи-Хеллмана

5. A: вычисляет $k_a=(y_b)^{xa}$ {mod p}.
6. B: вычисляет $k_b=(y_a)^{xb}$ {mod p}.
7. Конец ($k_a=(y_b)^{xa}$ {mod p}=$(a^{xb})^{xa}$ {mod p}=$a^{xb\cdot xa}$ {mod p}=$a^{xa\cdot xb}$ {mod p}=k_b и созданный ключ может теперь использоваться для защищенного обмена сообщениями между A и B).

- Открытый ключ: a, p, y_a (y_b).
- Закрытый ключ: x_a (x_b).

Криптосистема Диффи-Хеллмана

- Основана на вычислительной сложности задачи дискретного логарифмирования: вычисление $y=a^x \{mod\ p\}$ (p – простое число или степень простого числа, $1<x<p-1$, $1<a<p-1$) выполняется просто, но вычисление $x=\log_a y \{mod\ p\}$ выполняется весьма сложно.
- Значения a и p в системе Диффи-Хеллмана не являются секретными, поскольку, даже зная их, нарушитель не сможет решить задачу дискретного логарифмирования и найти значения x_a и x_b, чтобы вычислить сгенерированный ключ симметричного шифрования (однако необходимо получение A и B этих параметров из надежного источника).

Угрозы безопасности электронных документов

- подготовка документа от имени другого субъекта (маскарад);
- отказ автора документа от факта его подготовки (ренегатство);
- изменение получателем документа его содержания (подмена);
- изменение содержания документа третьим лицом (активный перехват);
- повторная передача по компьютерной сети ранее переданного документа (повтор).

Электронная подпись (ЭП)

- Представляет собой относительно небольшой по объему блок данных, передаваемый (хранящийся) вместе (реже – отдельно) с подписываемым с ее помощью документом.
- Механизм ЭП состоит из двух процедур – получения (простановки) подписи с помощью закрытого ключа автора документа и проверки ЭП при помощи открытого ключа автора документа.

Алгоритм получения ЭП под документом P

1. Вычисление хеш-значения H(P) для документа P.
2. Шифрование H(P) с помощью закрытого ключа автора документа ska – $E_{ska}(H(P))$ (полученный шифротекст и будет являться ЭП).

Алгоритм проверки ЭП S под документом P

1. Вычисления хеш-значения H(P) для документа P.
2. Расшифрование ЭП с помощью открытого ключа автора документа pka – $D_{pka}(S)=D_{pka}(E_{ska}(H(P)))=H(P)$.
3. Сравнение вычисленного и расшифрованного хеш-значений для документа P.

Требования к механизму ЭП

Перед получением ЭП в подписываемый документ должны быть включены дата и время простановки подписи, а при проверке ЭП должны быть известны:

- срок окончания действия и другие ограничения закрытого ключа данной подписи;
- имя подписывающего лица;
- идентификатор закрытого ключа (для возможности выбора лицом, проверяющим ЭП, нужного открытого ключа).

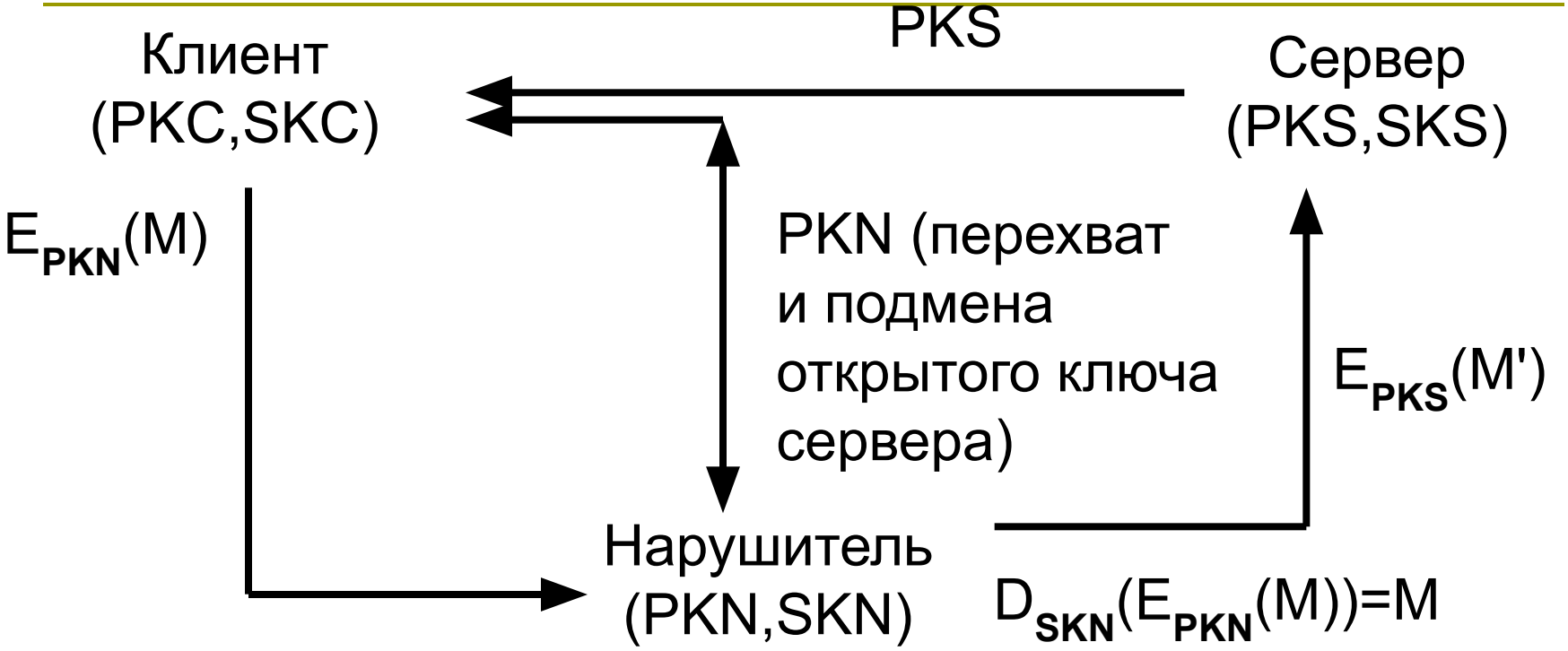
Механизм ЭП

- Принципиальным моментом является то, что подпись под электронным документом невозможно подделать без знания закрытого ключа автора документа, поэтому компрометация закрытого ключа недопустима.
- Способы хранения личного ключа: в файле, зашифрованном с помощью ключа, выводимого из парольной фразы; на устройстве, защищенном PIN-кодом от несанкционированного чтения; на сервере с возможностью его безопасной передачи на рабочую станцию.

Системы ЭП

- RSA (на основе асимметричной криптосистемы RSA);
- DSS (Digital Signature Standard, стандарт США на основе асимметричной криптосистемы Эль-Гамаля);
- ECDSS (Digital Signature Standard, стандарт США на основе криптосистемы эллиптических кривых);
- ГОСТ Р 34.10-2012 (российский стандарт ЭП, использующий асимметричную криптосистему на основе эллиптических кривых).

Угроза предъявления нарушителем ложного открытого ключа



- Разновидность атаки «человек посередине».
- Аутентичность сертификата открытого ключа сервера должна обеспечиваться ЭП УЦ.

Структура сертификата открытого ключа (стандарт X.509 ITU)

- Серийный № (назначается издателем).
- Идентификатор алгоритма ЭП для сертификата.
- Имя издателя сертификата.
- Начало и окончание периода действия.
- Имя владельца сертификата (субъекта).
- Открытый ключ и идентификатор асимметричного криптоалгоритма.
- Дополнения (необязательная часть).
- ЭП под сертификатом.

Элементы инфраструктуры открытых ключей (PKI)

PKI – совокупность организаций, методов и средств для создания, проверки и распределения открытых ключей группе пользователей, отдельной организации или всем гражданам.

Основные компоненты PKI:

- удостоверяющий центр;
- регистрационный центр (необязательный);
- реестр сертификатов;
- архив сертификатов;
- конечные пользователи.