Шифрование данных (2 часть)

План лекции № 10

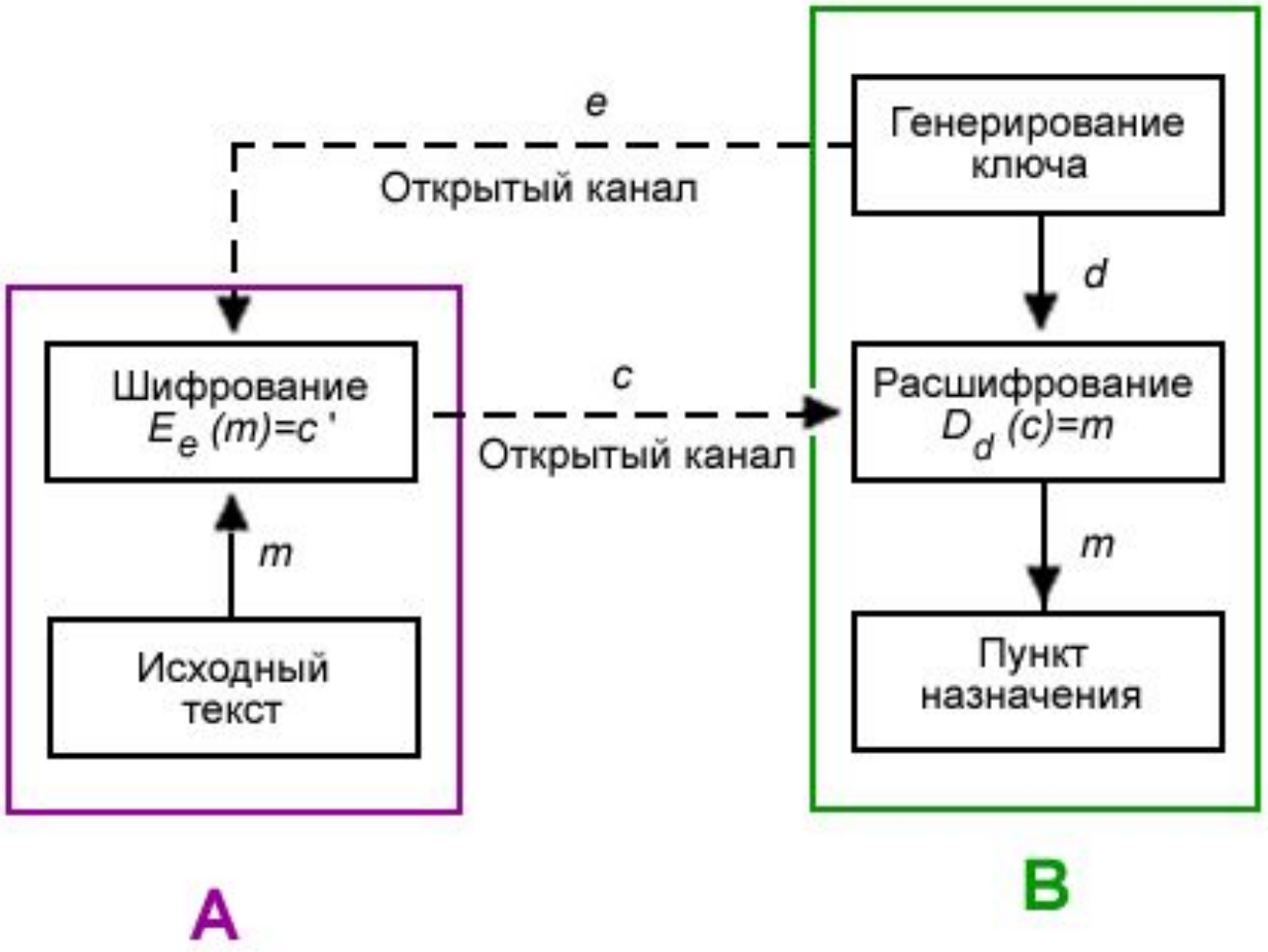
1. Асимметричное шифрование
2. Криптографические протоколы:
   a. протоколы распределения ключей
   b. протокол электронных платежей

Асимметричное шифрование

Криптографический алгоритм с открытым ключом (или асимметричное шифрование, асимметричный шифр) - система криптопреобразований с двумя связанными ключами:

- **открытый (public) ключ** передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу, и используется для шифрования сообщения и проверки ЭЦП;.
- **закрытый (private) ключ** хранится у владельца и используется для расшифрования сообщения (зашифрованного на парном открытом ключе) и для формирования ЭЦП.

Асимметричное шифрование



Асимметричное шифрование

Формирование системы *RSA*

1. Выбираем два различных простых числа p и q.
2. Вычисляем $n = pq$ и

$$\varphi(n) = (p - 1)(q - 1).$$

3. Выбираем число e, взаимно простое с $\varphi(n)$.
4. Вычисляем число d из уравнения

$$de \equiv 1 \ mod \ \varphi(n).$$

5. Определяем открытые ключи e и n.
6. Определяем закрытые ключи d, p, q и $\varphi(n)$.

Асимметричное шифрование

Функция зашифрования

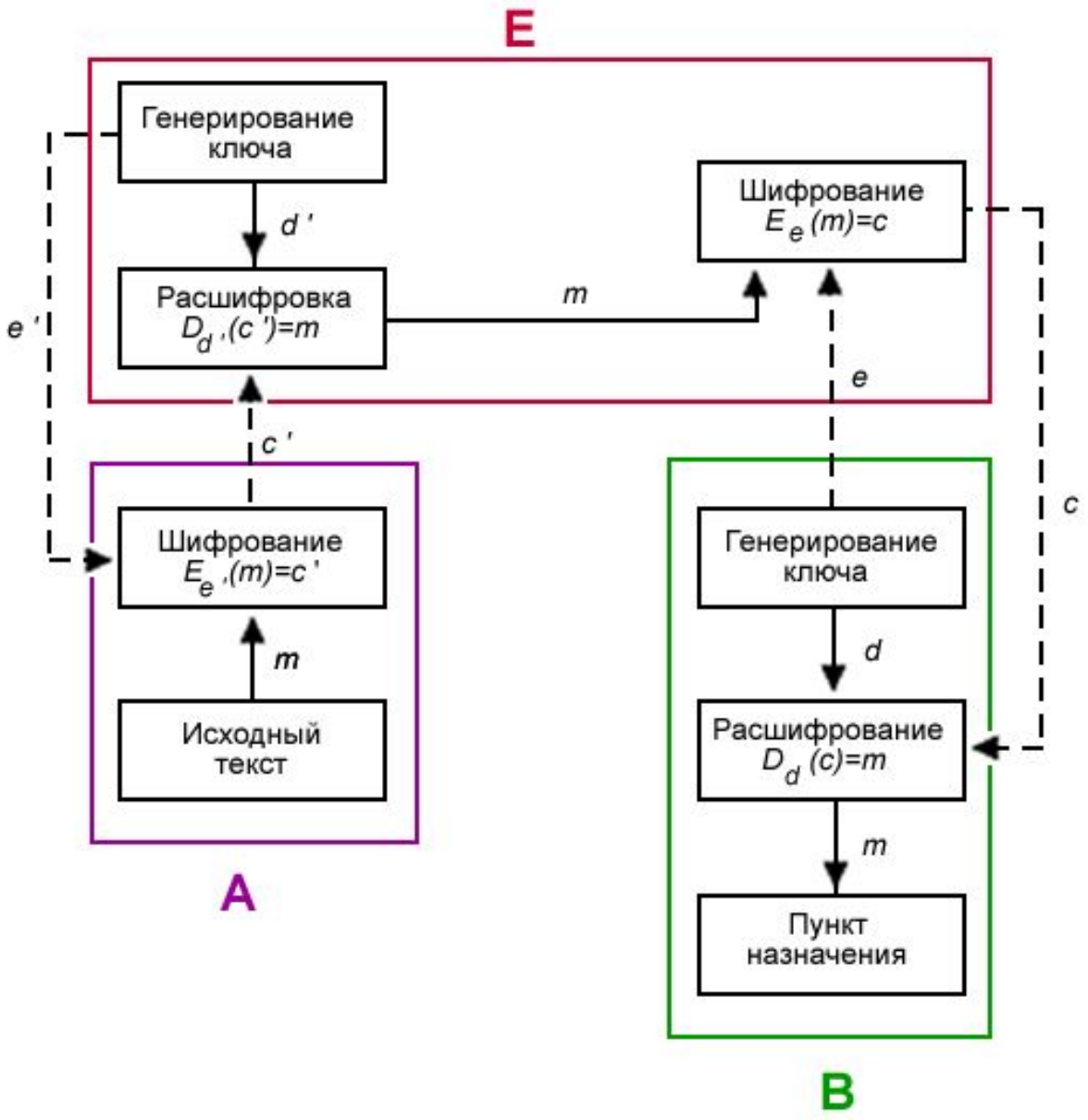
1. Дан текст сообщения M.
Шифротекст C вычисляется по формуле

$$C = E_k(M) = M^e \bmod n.$$

Функция расшифрования

1. Дан шифротекст C.
2. Текст сообщения M вычисляется по формуле

$$M = D_k(C) = C^d \bmod n = (M^e)^d \bmod n = M.$$



Криптоанализ алгоритмов с открытым ключом

Асимметричное шифрование

Преимущества асимметричных шифров перед симметричными:

- не нужно предварительно передавать секретный ключ по надёжному каналу;
- только одной стороне известен ключ расшифрования, который нужно держать в секрете (в симметричной криптографии такой ключ известен обеим сторонам и должен держаться в секрете обеими);
- в больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

Недостатки алгоритмов асимметричного шифрования в сравнении с симметричным:

- Необходима аутентификация абонентов
- Требуются более длинные ключи
- шифрование-расшифровывание с использованием пары ключей проходит на два-три порядка медленнее
- требуются существенно большие вычислительные ресурсы,

Асимметричное шифрование

Преимущества асимметричных шифров перед симметричными:

- не нужно предварительно передавать секретный ключ по надёжному каналу;
- только одной стороне известен ключ расшифрования, который нужно держать в секрете (в симметричной криптографии такой ключ известен обеим сторонам и должен держаться в секрете обеими);
- в больших сетях число ключей в асимметричной криптосистеме значительно меньше, чем в симметричной.

Недостатки алгоритмов асимметричного шифрования в сравнении с симметричным:

- Необходима аутентификация абонентов
- Требуются более длинные ключи
- шифрование-расшифровывание с использованием пары ключей проходит на два-три порядка медленнее
- требуются существенно большие вычислительные ресурсы,

Криптографические протоколы

Протокол (protocol) — описание распределенного алгоритма, в процессе выполнения которого два(или более) участника последовательно выполняют определенные действия и обмениваются сообщениями для совместного решения какой-либо задачи.

Криптографический протокол – это протокол на основе криптографических преобоазований.

Криптографические протоколы

Объектами изучения теории криптографических протоколов являются *удаленные абоненты*, *взаимодействующие* по *открытым* каналам связи.

Целью взаимодействия является *решение* какой-либо практической задачи, например:

- распределение ключей,
- обмен сообщениями,
- электронное голосование,
- электронные платежи и др.

Криптографические протоколы

Модель криптографического протокола предусматривает наличие *противника*, преследующего собственные цели.

Противник может выдавать себя за *законного* субъекта взаимодействия, *вмешиваться* в информационный обмен между абонентами и т. п.

Участники протокола в общем случае ***не доверяют друг другу,*** т.е. некоторые протоколы должны быть рассчитаны на ситуацию, когда ***противником*** может оказаться даже ***один из абонентов или несколько абонентов***, вступивших в сговор

Криптографические протоколы

Функции криптографических протоколов:

- Аутентификация источника данных
- Аутентификация сторон
- Конфиденциальность данных
- Невозможность отказа
- Невозможность отказа с доказательством получения
- Невозможность отказа с доказательством источника
- Целостность данных
- Обеспечение целостности соединения без восстановления
- Обеспечение целостности соединения с восстановлением
- Разграничение доступа

Криптографические протоколы

Протокол чаще всего является ***интерактивным***, т.е, предусматривает многоходовый обмен сообщениями между участниками, и включает в себя:

- *распределенный алгоритм,* т. е. характер и последовательность действий каждого из участников;
- *спецификацию форматов пересылаемых сообщений;*
- *спецификацию синхронизации действий участников;*
- *описание действий при возникновении сбоев.*

Схема Диффи-Хелманна

1976 - первый из опубликованных алгоритмов на основе открытых ключей опубликован в работе ***Диффи и Хеллмана*** в которой было определено само понятие криптографии с открытым ключом.

Обычно этот алгоритм называют ***протоколом обмена ключами по схеме Диффи-Хеллмана***.

Стойкость алгоритма Диффи-Хеллмана опирается на ***трудность вычисления дискретных логарифмов.***

Схема Диффи-Хелманна

Открытыми параметрами являются большое простое число p и число g, являющееся первообразный корень числа p.

1. Пользователь А выбирает случайное число ***a***, равновероятное из целых 1...***p***-1. Это число он держит в секрете, а пользователю В посылает по открытому каналу число

$$y_1 = g^a \bmod p$$

2 Аналогично поступает и пользователь В, генерируя случайное число ***b***, вычислив

$$y_2 = g^b \bmod p,$$

и отправляет его пользователю А.

Схема Диффи-Хелманна

3. После этого пользователь *A* вычисляет значение

$$k_{ab} = (y_2)^a \bmod p = (g^b \bmod p)^a \bmod p$$

4. То же делает и пользователь *B*:

$$k_{ba} = (y_1)^b \bmod p = (g^a \bmod p)^b \bmod p$$

5. По правилам модулярной арифметики

$$k_{ab} = k_{ba} = g^{ba} \bmod p = g^{ab} \bmod p$$

Классификация протоколов по методу доказательств

Это ***примитивные протоколы***, математические модели, которые используются в качестве своеобразных строительных блоков при создании ***прикладных*** протоколов:

- ***интерактивная система доказательств (Interactive Proof System);***
- ***доказательств с нулевым разглашением знаний (Zero-Knowledge Proofs).***

Классификация протоколов по количеству участников

1. ***Двусторонний протокол***
2. ***Трехсторонний протокол с судейством***
3. ***Многосторонний протокол***

Классификация протоколов по цели и задачам использования

Это **прикладные протоколы**, решающие ***конкретную задачу***, которая может возникнуть на практике:

- Протоколы электронных голосований,
- Протоколы разделения секрета,
- Протоколы электронных платежей,
- Протоколы совместных вычислений
- Протоколы взаимной и односторонней аутентификации

Интерактивная система доказательств (Interactive Proof System)

Протокол (**P**,*V*,*S)* взаимодействия двух субъектов:

1. доказывающего (претендента) ***P***
2. проверяющего (верификатора) *V*.

Интерактивная система доказательств (Interactive Proof System)

Абонент ***P*** хочет доказать ***V***, что утверждение ***S*** истинно.

При этом считается, что

- абонент ***V*** самостоятельно проверить утверждение ***S*** не в состоянии
- абонент ***V*** не может быть противником,
- абонент ***P*** может быть противником, пытающимся доказать истинность ложного утверждения ***S***.

Интерактивная система доказательств (Interactive Proof System)

Протокол состоит из некоторого числа раундов обмена сообщениями между ***P*** и ***V*** и должен удовлетворять двум условиям:

- ***полноте*** — если ***S*** действительно истинно, то доказывающий убедит проверяющего признать это;
- ***корректности*** - если ***S*** ложно, то доказывающий не сможет убедить проверяющего в обратном.

Интерактивная система доказательств (Interactive Proof System)

Классическим примером задачи, решаемой двумя удаленными абонентами, является *генерация случайного бита*.

Задача решается на *основе бросания жребия*, например, с помощью подбрасывания монеты.

Это необходимо делать так, чтобы абонент ***A***, подбрасывающий монету, ***не мог изменить*** результат ***после получения догадки*** от абонента ***B***, угадывающего этот результат.

.

Интерактивная система доказательств (Interactive Proof System)

Схема М. Блюма - С. Микали:

Имеется *односторонняя* ***функция*** $F: X \rightarrow Y$, *удовлетворяющая следующим требованиям:*

- *X - конечное множество целых чисел, содержащее одинаковое количество четных и нечетных чисел:*
- *любые числа* $x_1, x_2 \in X$, *такие, что* $F(x_1) = F(x_2)$, *имеют одинаковую четность;*
- *по заданному значению* $F(x)$ *невозможно определить четность аргумента* x.

Интерактивная система доказательств (Interactive Proof System)

Схема М. Блюма - С. Микали:

- *Абонент **A** выбирает случайное число $x_A \in X$ (подбрасывает монету), вычисляет $y_A = F(x_A)$ и посылает y_A абоненту **B**.*
- *Абонент **B**, получив y_A, пытается угадать четность x_A и посылает свою догадку **A**.*
- *Абонент **A**, получив догадку от **B**, сообщает последнему, угадал ли он, посылая ему выбранное число x_A.*
- *Абонент **B**, получив x_A, проверяет, не обманывает ли **A**, вычисляя значение $F(x_A)$ и сравнивая его с полученным на втором шаге значением.*

Доказательства с нулевым разглашением знаний (Zero-Knowledge Proofs)

Протокол состоит из некоторого числа раундов обмена сообщениями между ***P*** и ***V*** и должен удовлетворять двум условиям:

- ***полноте*** - если ***S*** действительно истинно, то доказывающий убедит проверяющего признать это;
- ***корректности*** - если ***S*** ложно, то доказывающий не сможет убедить проверяющего в обратном;
- ***нулевому разглашению*** - в результате работы протокола абонент ***V*** не увеличит своих знаний об утверждении ***S***

Доказательства с нулевым разглашением знаний (Zero-Knowledge Proofs)

Протокол используется, если предположить, что

V может быть **противником**, который хочет получить информацию об **утверждении *S***.

В результате реализации протокола

- абонент ***P*** сможет доказать абоненту ***V***,
- что он владеет некоторой ***секретной*** информацией,
- но ***не разглашая*** ее сути.

Доказательства с нулевым разглашением знаний (Zero-Knowledge Proofs)

Верификатор ***V*** задает серию случайных вопросов, каждый из которых, допускает ответ "да" или "нет".

После первого вопроса ***V*** убеждается в том, что

***P* заблуждается с вероятностью 1/2**.

После второго вопроса ***V*** убеждается в том, что

***P* заблуждается с вероятностью 1/4,**

и т.д.

После каждого вопроса знаменатель удваивается.

Доказательства с нулевым разглашением знаний (Zero-Knowledge Proofs)

Протокол электронных платежей.

«Электронные деньги» - **Д. Шаум**, основатель фирмы **DigiCash**.

DigiCash разработала и запатентовала криптографическую технологию безопасных электронных платежей (**MasterCard).**

Доказательства с нулевым разглашением знаний (Zero-Knowledge Proofs)

Протокол электронных платежей.

Электронные деньги *- бессрочные денежные обязательства банковской или другой коммерческой структуры, представленные в электронной форме, сопровождаемые электронной подписью выдавшей их структуры и погашаемые в момент предъявления обычными денежными средствами.*

Доказательства с нулевым разглашением знаний (Zero-Knowledge Proofs)

Номинал 1000$
Номер купюры 12239555622491219 7
ЭЦП банка-эмитента SETAg19061055XVmu0778y71

Доказательства с нулевым разглашением знаний (Zero-Knowledge Proofs)

Доказательства с нулевым разглашением знаний (Zero-Knowledge Proofs)

Протокол слепой подписи по схеме RSA.

1. Банк C выбирает два секретных больших простых числа p и g, вычисляет их произведение n = pq, а также находит e и d- соответственно открытый k_c^{public} и секретный k_c^{secret} ключи банка.

2. Выбирается односторонняя функция

$f: Z_n \rightarrow Z_n$

3. Числа n, e и функция f публикуются. При этом пара ключей (e, d) используется банком для создания купюр одного фиксированного номинала. Для создания купюр другого номинала используется своя пара ключей.

Доказательства с нулевым разглашением знаний (Zero-Knowledge Proofs)

Протокол слепой подписи по схеме RSA.

Протокол транзакции заказа электронной наличности (снятия со счета) с использованием слепой подписи:

1. *Клиент А выбирает случайное число (по сути, номер купюры) $x \in Zn$ и вычисляет $f(x)$.*

2. *Клиент А инициирует начало протокола слепой подписи, выбирая случайное число $r \in Zn$, $r \neq 0$. Клиент А вычисляет*

$$y = f(x)\, r^e \bmod n,$$

где r^e - так называемый затемняющий множитель, и посылает запрос у абоненту С

Доказательства с нулевым разглашением знаний (Zero-Knowledge Proofs)

Протокол слепой подписи по схеме RSA.

3. Банк C подписывает купюру, вычисляя

$$y^d \bmod n,$$

и посылает клиенту A полученное значение

$$(f(x))^d \, r \bmod n$$

4. Клиент A "снимает" действие затемняющего множителя и получает подписанную купюру (x, s),

где

$s = (f(x))^d \bmod n)$ суть подпись банка C.

Доказательства с нулевым разглашением знаний (Zero-Knowledge Proofs)

Протокол транзакции платежа с использованием электронной наличности:

1. *Покупатель A передает продавцу B электронную купюру (x, s).*
2. *Продавец B посылает (x, s) банку C.*
3. *Банк C вычисляет f(x) и проверяет свою подпись, убеждаясь в справедливости равенства*

$$f(x) = s^e \bmod n.$$

4. *Банк C проверяет, не была ли купюра с данным номером потрачена ранее, и, если нет. перечисляет на счет клиента B сумму, равную номиналу купюры, и уведомляет его об этом.*