Лабораторная работа № 3

Алгоритм RSA. Обмен ключами симметричных алгоритмов с использованием ассиметричных криптосистем.

Цель:

- Ознакомиться с математическими принципами функционирования алгоритма RSA.
- Научиться проводить шифрование/дешифрование с помощью данного алгоритма.
- Ознакомиться с принципом реализации обмена ключами с использованием схемы Диффи-Хеллмана.
- Освоить данный алгоритм обмена ключами.

Задачи:

1. Рассмотреть общие математические принципы организации процедуры шифрования/дешифрования при использовании метода RSA.
2. Рассмотреть схему обмена ключами по алгоритму Диффи-Хеллмана.
3. Реализовать программно алгоритм шифрования и дешифрования методом RSA.
4. Провести шифрование открытого текста, выбранного согласно варианту, указанному преподавателем, и его последующее восстановление.
5. Рассмотреть схему Диффи-Хеллмана с общим простым числом q и первообразным корнем a. Вами выбран секретный ключ X_A. При обмене ключами с вашим респондентом, имеющим открытый ключ Y_B, вы получили от него общий секретный ключ K. Состоялся ли обмен ключами? Обоснуйте ответ. Вычислите значение открытого ключа Y_A.

Значения параметров q, a, X_A, Y_B, K выбрать согласно варианту.

Теоретические сведения

Алгоритм RSA
Системах шифрования с открытым ключом

В криптографии существует два вида ключей: открытый и закрытый. В симметричной криптографии каждая из переписывающихся сторон имеет копию общего открытого ключа.

Открытый ключ может быть опубликован в справочнике наряду с именем пользователя. В результате любой желающий может зашифровать с его помощью свое письмо и послать закрытую информацию владельцу соответствующего секретного ключа. Расшифровать посланное сообщение сможет только тот, у кого есть секретный ключ. Более точно, имеют место преобразования:

сообщение + ОТКРЫТЫЙ КЛЮЧ ПОЛЬЗОВАТЕЛЯ А = ШИФРОТЕКСТ

ШИФРОТЕКСТ + секретный ключ пользователя А = сообщение

Таким образом, каждый может послать пользователю А секретную информацию, воспользовавшись его открытым ключом. Но только пользователь А в состоянии расшифровать сообщение, поскольку лишь у него есть соответствующий секретный ключ.

Причина работоспособности таких криптосистем заключается в односторонней математической связи, существующей между двумя ключами, при которой информация об открытом ключе никак не помогает восстановить секретный, но владение секретным ключом обеспечивает возможность расшифровывать сообщения, зашифрованные открытым.

Идея криптографии с открытым ключом впервые появилась в 1976 г. в революционной работе Диффи и Хеллмана «Новые направления в криптографии». Но только год спустя была опубликована первая (и наиболее успешная) криптосистема с открытым ключом, а именно, RSA.

Описание алгоритма шифрования

Алгоритм RSA стоит у истоков асимметричной криптографии. Он был предложен тремя исследователями-математиками: Рональдом Ривестом (R.Rivest) , Ади Шамиром (A.Shamir) и Леонардом Адльманом (L.Adleman) в 1977-78 годах.

Первым этапом любого асимметричного алгоритма является создание пары ключей : открытого и закрытого и распространение открытого ключа "по всему миру". Для алгоритма RSA этап создания ключей состоит из следующих операций:

1. Выбираются два простых (!) числа p и q
2. Вычисляется их произведение n=p×q.
3. Вычисляется функция Эйлера φ(n)=(p-1)(q-1).
4. Выбирается произвольное число e (e<n), такое, что НОД(e, φ(n)) = 1. То есть e должно быть взаимно простым числом с φ(n).
5. Методом Евклида решается в целых числах (!) уравнение e×d+φ(n)×y=1. Здесь неизвестными являются переменные d и y – метод Евклида как раз и находит множество пар (d,y), каждая из которых является решением уравнения в целых числах.
6. Два числа (e,n) – публикуются как открытый ключ.
7. Число d хранится в строжайшем секрете. Пара чисел (d,n) – это и есть закрытый ключ, который позволит читать все послания, зашифрованные с помощью пары чисел (e,n).

Шифрование с помощью этих чисел:

1. Отправитель разбивает свое сообщение на блоки, равные k=[log2(n)] бит, где квадратные скобки обозначают взятие целой части от дробного числа.
2. Подобный блок может быть интерпретирован как число из диапазона (0;2k-1). Для каждого такого числа (назовем его mi) вычисляется выражение:

$$c_i = ((m_i) ¿¿ e) \bmod n ¿$$

Блоки c_i и есть зашифрованное сообщение. Их можно спокойно передавать по открытому каналу, поскольку операция возведения в степень по модулю простого числа, является необратимой математической задачей. Обратная ей задача носит название "логарифмирование в конечном поле" и является на несколько порядков более сложной задачей. То есть даже если злоумышленник знает числа e и n, то по c_i прочесть исходные сообщения mi он не может никак, кроме как полным перебором m_i.

Пример:

Выбираем два простые числа p = 7; q = 17 (на практике эти числа во много раз длиннее). В этом случае n = p×q будет равно 119. Теперь необходимо выбрать e, выбираем e= 5. Следующий шаг связан с формированием числа d так, чтобы d*e=1 mod [(p-1)(q-1)]. D = 77 (использован расширенный алгоритм Эвклида). d - секретный ключ, а e и n характеризуют открытый ключ. Пусть текст, который нам нужно зашифровать представляется M = 19. C = M^e (mod n). Получаем зашифрованный текст C = 66. Этот “текст” может быть послан соответствующему адресату. Получатель дешифрует полученное сообщение, используя M= C^d (mod n) и C=66. В результате получается M = 19.

На практике общедоступные ключи могут помещаться в специальную базу данных. При необходимости послать партнеру зашифрованное сообщение можно сделать сначала запрос его открытого ключа. Получив его, можно запустить программу шифрации, а результат ее работы послать адресату. На использовании общедоступных ключей базируется и так называемая электронная подпись, которая позволяет однозначно идентифицировать отправителя. Сходные средства могут применяться для предотвращения внесения каких-либо корректив в сообщение на пути от отправителя к получателю. Быстродействующие аппаратные 512-битовые модули могут обеспечить скорость шифрования на уровне 64 кбит в сек. Готовятся ИС, способные выполнять такие операции со скоростью 1 Мбайт/сек. Разумный выбор параметра e позволяет заметно ускорить реализацию алгоритма.

На рис.1 проиллюстрирован принцип шифрования/дешифрования методом RSA.

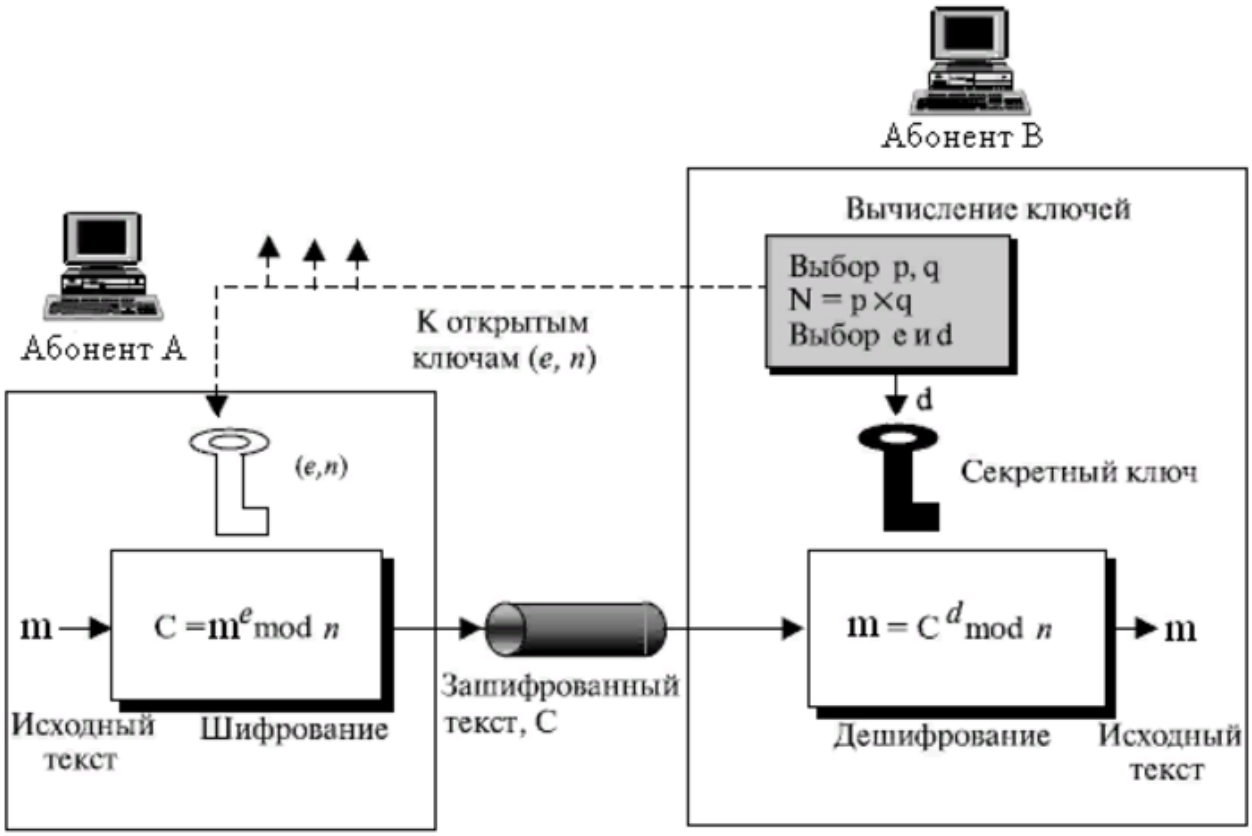

Рис. 1. Криптосистема RSA

Принцип дешифрования

На приемной стороне процесс дешифрования возможен при условии, что известно число d. Достаточно давно была доказана теорема Эйлера, частный случай которой утверждает, что если число n представимо в виде двух простых чисел p и q, то для любого x имеет место равенство $(x^{(p-1)(q-1)})mod\ n = 1$. Для дешифрования RSA-сообщений воспользуемся этой формулой.

Возведем обе ее части в степень (-y) : $(x^{(-y)(p-1)(q-1)})mod\ n = 1^{(-y)} = 1$. Теперь умножим обе ее части на x : $(x^{(-y)(p-1)(q-1)+1})mod\ n = 1 \times x = x$.

А теперь вспомним как мы создавали открытый и закрытый ключи. Мы подбирали с помощью алгоритма Евклида d такое, что e*d+(p-1)(q-1)*y=1, то есть e × d=(-y)(p-1)(q-1)+1. А следовательно в последнем выражении предыдущего абзаца мы можем заменить показатель степени на число (e×d).

Получаем $(x^e \times x^d) \bmod n = x$. То есть для того чтобы прочесть сообщение $c_i=((m_i)^e) \bmod n$ достаточно возвести его в степень d по модулю m :

$$((c_i)^d) \bmod n = ((m_i)^{e \times d}) \bmod n = m_i.$$

На самом деле операции возведения в степень больших чисел достаточно трудоемки для современных процессоров, даже если они производятся по оптимизированным по времени алгоритмам. Поэтому обычно весь текст сообщения кодируется обычным блочным шифром (намного более быстрым), но с использованием ключа сеанса, а вот сам ключ сеанса шифруется как раз асимметричным алгоритмом с помощью открытого ключа получателя и помещается в начало файла.

Обмен ключами симметричных алгоритмов с использованием ассиметричных криптосистем

Казалось бы, асимметричные криптосистемы лишены одного из самых главных недостатков симметричных алгоритмов – необходимости предварительного обмена сторонами секретным ключом по защищенной схеме (например, из рук в руки или с помощью поверенного курьера). Но оказывается не все так просто предположим абонент А - потенциальный собеседник абонента Б. Для того чтобы отправить зашифрованное сообщение, абонент А должен узнать, открытый ключ абонента Б. Если абонент Б не приносил мне его лично абоненту А на дискете, значит абонент А просто взял из информационной сети. А теперь главный вопрос: где доказательство, что данный набор байт является открытым ключом именно абонента Б? Ведь злоумышленник может сгенерировать произвольную пару (закрытый ключ, открытый ключ), затем активно распространять или пассивно подменять при запросе открытый ключ созданным абонента Б, созданный им. В этом случае при отправке сообщения 1) абонент А зашифрует его тем ключом, который по его мнению является ключом абонента Б, 2) злоумышленник, перехватив сообщение дешифрует его парным закрытым ключом, прочтет и более того : 3) может переслать дальше, зашифровав действительно уже открытым ключом абонента Б.

Распределение ключей — одна из фундаментальных задач криптографии. Существует несколько ее решений, подходящее из которых выбирается в зависимости от ситуации.

Физическое распределение. С помощью доверенных курьеров или вооруженной охраны ключи могут рассылаться традиционным физическим путем. До семидесятых годов двадцатого века это действительно был единственный безопасный путь распределения ключей при установке системы. Ему сопутствовал ряд трудностей, в особенности при расширении, масштабировании (модульном наращивании системы в рамках унифицированной архитектуры) криптосистемы, но основной недостаток, связанный с таким способом распределения, состоит в том, что криптостойкость системы зависит не столько от ключа, сколько от курьера. Если подкупить, похитить или просто убить курьера, то система будет скомпрометирована.

Распределение с помощью протоколов с секретным ключом. Если долговременные секретные ключи распределены между пользователями и неким центром, который обычно называют центром доверия, то его можно использовать для генерирования ключей и обмена между любыми двумя пользователями всякий раз, когда в этом возникает необходимость. Протоколы, предназначенные для этой цели, обычно достаточно эффективны, но не лишены и недостатков. В частности, этот способ распределения предусматривает, что как оба пользователя, так и центр работают в режиме онлайн. Кроме того, статичные ключи при этом должны распределяться физическим путем.

Распределение с помощью протоколов с открытым ключом. Используя криптосистемы с открытым ключом, партнеры, не доверяющие посредникам и лишенные возможности встретиться, могут договориться об общем секретном ключе в режиме онлайн в соответствии с протоколом об обмене ключей. Это наиболее распространенное приложение техники шифрования с открытым ключом. Вместо того, чтобы шифровать большой объем данных непосредственно с помощью открытого ключа, стороны предварительно согласовывают секретный ключ. Затем для шифрования

фактической информации применяется симметричный шифр с согласованным ключом. Для подобного распределения используются следующие типы протоколов:

- простое распределение;
- распределение с обеспечением конфиденциальности и аутентификации;
- гибридная схема.

Чтобы понять масштабность проблемы, отметим, что при обслуживании n пользователей, обменивающихся закрытой информацией друг с другом, необходимо n(n — 1)/2 разных секретных ключей.

С ростом n возникает проблема управления огромным числом ключей. Например, для небольшого университета с 10000 студентов нужно около пятидесяти миллионов отдельных секретных ключей. С большим количеством уже существующих ключей связано много проблем. Итак, большое число ключей порождает сложную проблему управления.

Одно из ее решений заключается в том, что за каждым пользователем закрепляется единственный ключ, используя который он может связываться с центром доверия. В этом случае система с n пользователями требует только n ключей. Когда двое пользователей хотят обменяться секретными сведениями, они генерируют ключ, который будет использован только для передачи этого сообщения. Его называют *сеансовым ключом.*

Простое распределение секретных ключей

Исключительно простую схему предложил Меркл (Merkle) (Рис. 2). Если инициатор А намерен обменяться данными с пользователем В, для этого предполагается следующая процедура.

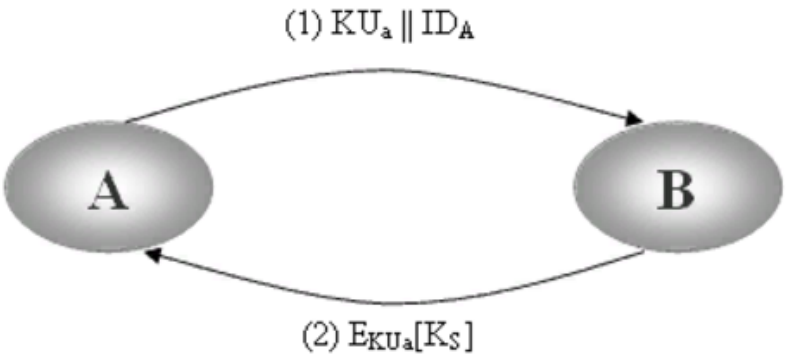

Рис. 2. Простое использование шифрования с открытым ключом при выборе сеансового ключа

1. Сторона А генерирует пару открытый/личный ключи {KUa, KRa} и передает сообщение стороне В, содержащее KUa и идентификатор отправителя А, ID_a.
2. Получатель В генерирует секретный ключ Ks и передает этот ключ инициатору сообщения А зашифрованным с помощью открытого ключа инициатора А.
3. Пользователь А вычисляет $D_{KRa}[E_{KUa}[K_S]]$, чтобы восстановить секретный ключ. Поскольку только пользователь А может дешифровать это сообщение, только участники обмена данными А и В будут знать значение K_S.
4. Участник А выбрасывает ключ KRa, а участник В - выбрасывает ключ KUa. Теперь обе стороны, А и В, могут использовать связь, защищенную традиционным шифрованием с сеансовым ключом K_S. По окончанию обмена данными и А, и В выбрасывают K_S. Несмотря на простоту, этот протокол весьма привлекателен. Никаких ключей не существуют перед началом связи и никаких ключей не остается после завершения связи. Поэтому риск компрометации ключей минимален. В то же время связь оказывается защищенной от подслушивания.

Этот протокол уязвим в отношении активных атак. Если противник E имеет возможность внедрения в канал связи, то он может скомпрометировать связь без того, чтобы быть обнаруженным, следующим образом:

1. Участник A генерирует пару открытый/личный ключи {KUa, KRa} и передает сообщение адресату B, содержащее KUa и идентификатор отправителя A, IDa.
2. Противник E перехватывает сообщение, создает собственную пару открытый/личный ключи {KUe, KRe} и передает сообщение адресату B, содержащее KUe || IDa.
3. B генерирует секретный ключ Ks и передает KUe[KS].
4. Противник E перехватывает это сообщение и узнает KS, вычисляя $D_{KRe}[E_{KUe}[K_S]]$.
5. Противник E передает участнику A сообщение $E_{KUa}[K_S]$.

В результате оба участника, A и B, будут знать KS, но не будут подозревать, что KS также известен и противнику E. Поэтому стороны A и B могут начать обмен сообщениями, используя KS. Противник E больше не будет активно вмешиваться в канал связи, а просто будет перехватывать сообщения. Зная KS, он сможет дешифровать любое сообщение, а участники A и B даже не будут подозревать о существовании проблемы. Таким образом, этот простой протокол оказывается полезным только в случае, когда единственной возможной угрозой является пассивный перехват сообщений.

Распределение секретных ключей с обеспечением конфиденциальности и аутентификации

Схема на рис.2 обеспечивает защиту и от активной, и от пассивной форм атак. В качестве исходных условий предположим, что A и B уже обменялись открытыми ключами. Далее следует выполнить следующие действия.

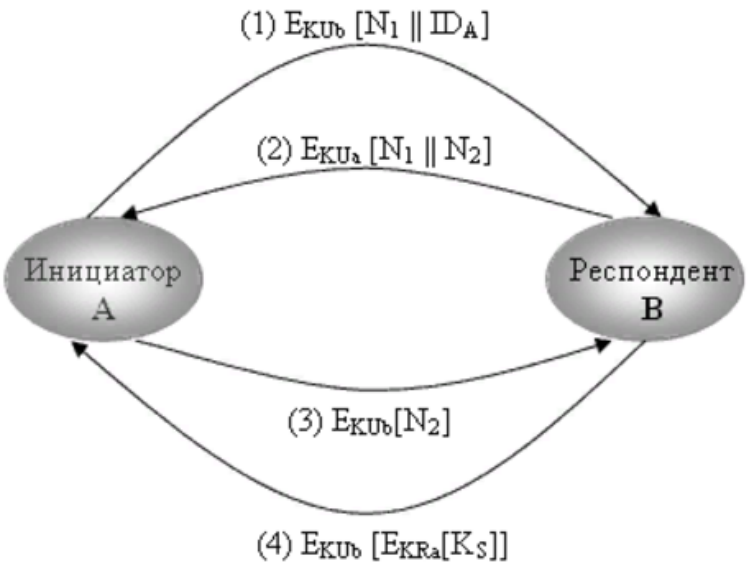

Рис. 2. Распределение секретных ключей с обеспечением конфиденциальности и аутентификации

1. Сторона A использует открытый ключ стороны B, чтобы переслать стороне B шифрованное сообщение, содержащее идентификатор участника A (ID_A) и оказию (N_1), используемую для идентификации данной конкретной транзакции.
2. Пользователь B посылает сообщение пользователю A, зашифрованное с помощью KUa и содержащее полученную от него оказию (N_1) и новую оказию (Na), сгенерированную пользователем B. Ввиду того что только участник B мог дешифровать сообщение (1), присутствие N_1 в сообщении (2) убеждает участника A в том, что респондентом является сторона B.
3. Сторона A возвращает Na, шифруя сообщение открытым ключом стороны B, чтобы гарантировать ей, что его респондентом является сторона A.

4. Участник А выбирает секретный ключ K_S и посылает участнику В сообщение $M = E_{KUb}[E_{KRa}[KS]]$. Шифрование этого сообщения открытым ключом стороны В гарантирует, что только участник В сможет прочитать его, а шифрование личным ключом участника А – что только участник А мог послать его.
5. Сторона В вычисляет $D_{KUa}[E_{KRb}[M]]$,чтобы восстановить секретный ключ.

В результате при обмене секретными ключами эта схема гарантирует как конфиденциальность, так и аутентификацию.

Гибридная схема

Еще одна схема использования шифрования с открытым ключом при распределении секретных ключей представляет гибридный подход. Эта схема предполагает участие центра распределения ключей (ЦРК), с которым каждый пользователь использует свой главный секретный ключ, и распределение секретных сеансовых ключей, шифруемых главным ключом. Схема шифрования с открытым ключом служит для распределения главных ключей. В основе такого трехуровневого подхода лежит следующая логика:

- Скорость выполнения процедуры. Существует много приложений, особенно ориентированных на передачу транзакций, где сеансовые ключи должны меняться очень часто. Распределение сеансовых ключей с помощью схемы с открытым ключом могло бы сделать производительность системы слишком низкой из-за относительно высоких требований к вычислительным ресурсам при шифровании и дешифровании по такой схеме. В случае трехуровневой иерархии шифрование с открытым ключом применяется лишь иногда, чтобы изменитъ главный ключ, разделяемый пользователем и ЦРК.
- Обратная совместимость. Гибридную схему можно легко реализовать в виде расширения уже имеющейся схемы, предполагающей использование ЦРК, с минимальными изменениями предусмотренной процедуры и программного обеспечения.

Добавление уровня шифрования с открытым ключом обеспечивает защищенное и эффективное средство распределения главных ключей. Это является преимуществом в конфигурации, когда один ЦРК обслуживает большое число пользователей, находящихся на значительном расстоянии друг от друга.

Среди алгоритмов распределения на основе открытых ключей наиболее популярными являются схема Диффи-Хеллмана и метод эллиптических кривых.

Схема Диффи-Хеллмана

Первый из опубликованных алгоритмов на основе открытых ключей появился в работе Диффи и Хеллмана. в которой было определено само понятие криптографии с открытым ключом. Обычно этот алгоритм называют обменом ключами по схеме Диффи-Хеллмана. Данная технология обмена ключами реализована в целом ряде коммерческих продуктов.

Цель схемы - обеспечить двум пользователям защищенную возможность сообщить друг другу ключ, чтобы они могли прибегнуть к ней для шифрования следующих сообщений. Сам по себе алгоритм ограничивается процедурой обмена ключами,

Эффективность алгоритма Диффи-Хеллмана опирается на трудность вычисления дискретных логарифмов. Формально дискретный логарифм можно определить следующим образом. Сначала определяется первообразный корень простого числа p как число, степени которого порождают все целые числа от 1 до p - 1. Это значит, что если a является первообразным корнем простого числа p, то все числа

$$a \bmod p,\ a^2 \bmod p,\ \ldots,\ a^{p-1} \bmod p$$

должны быть разными и представлять все целые числа от 1 до p – 1 в некоторой перестановке.

Для любого целого числа b и любого первообразного корня, а простого числа p однозначно определяется показатель степени i, при котором

$$b = a^i \bmod p \text{ где } 0 \le i \le (p-1).$$

Этот показатель степени обычно называется дискретным логарифмом, или индексом b по основанию a, рассматриваемому по модулю p. Это значение записывается в форме $\text{ind}_{a,p}(b)$.

Теперь мы можем описать обмен ключами по схеме Диффи-Хеллмана. Имеется два открытых для всех числа: простое число q и целое число a, являющееся первообразным корнем q. Предположим, пользователи A и B намерены обменяться ключами. Пользователь A выбирает случайное целое число $X_A < q$ и вычисляет $Y_A = a^{XA} \bmod q$. Точно также пользователь B независимо выбирает случайное целое число $X_B < q$ и вычисляет $Y_B = a^{XB} \bmod q$. Каждая сторона сохраняет значение X в тайне и делает значение Y свободно доступным другой стороне. Пользователь A вычисляет ключ по формуле К=¿¿ mod q, а пользователь B - по формуле К = ¿¿ mod q. Этидае формулы вычисления дают одинаковые результаты, как показано ниже.

$$\begin{aligned} K &= (Y_B)^{X_A} \bmod q \\ &= (a^{X_B} \bmod q)^{X_A} \bmod q \\ &= (a^{X_B})^{X_A} \bmod q \\ &= (a^{X_A})^{X_B} \bmod q \\ &= (Y_A)^{X_B} \bmod q. \end{aligned}$$

Итак, обе стороны обменялись секретнбым ключом. А поскольку при этом XA и XB были только в личном использовании и поэтому сохранились в тайне, противнику придется работать только с q, a, YA и YB. Таким образом, ему придется вычислять дискретный логарифм, чтобы определить ключ. Например, чтобы определить ключ пользователя B, противнику нужно вычислить

$$X_B = \text{ind}_{a,q}(Y_B).$$

После этого он сможет вычистить ключ К точно так же, как это делает пользователь B.

Защищенность обмена ключами по схеме Диффи-Хеллмана опирается фактически на то, что в то время, как степени по модулю некоторого простого числа вычисляются относительно легко, вычислять дискретные логарифмы оказывается очень трудно. Для больших простых чисел последнее считается задачей практически неразрешимой.

Пример

Обмен ключами строится на использовании простого числа q = 97 и его первообразном корне a = 5. Пользователи A и B выбирают секретные Ключи XA = 36 и XB = 58 соответственно. Каждый вычисляет свой открытый ключ:

$$Y_A = 5^{36} = 50 \bmod 97,$$

$$Y_B = 5^{58} = 44 \bmod 97.$$

После того как пользователи обменяются открытыми ключами, каждый из них может вычислить общий секретный ключ:

$$K = (Y_B)^{X_A} \bmod 97 = 44^{36} = 75 \bmod 97,$$

$$K = (Y_A)^{X_B} \bmod 97 = 50^{58} = 75 \bmod 97.$$

Пример:

Зашифруем и расшифруем сообщение "CAB" по алгоритму RSA. Для простоты возьмем небольшие числа - это сократит наши расчеты.

- Выберем p=3 and q=11.
- Определим n= 3*11=33. (n= p*q)
- Найдем (p-1)*(q-1)=20. Следовательно, d будет равно, например, 3: (d=3).
- Выберем число e по следующей формуле: (e*3) mod 20=1. Значит e будет равно, например, 7: (e=7).
- Представим шифруемое сообщение как последовательность чисел в диапозоне от 0 до 32 (незабывайте, что кончается на n-1). Буква A =1, B=2, C=3.

Теперь зашифруем сообщение, используя открытый ключ {7,33}, т е {e,n}
Последовательность чисел M(i) находится по формуле C(i)=(M(I)^e)mod n.
C1 = (3^7) mod 33 = 2187 mod 33 = 9;
C2 = (1^7) mod 33 = 1 mod 33 = 1;
C3 = (2^7) mod 33 = 128 mod 33 = 29;

Теперь расшифруем данные, используя закрытый ключ {3,33}, т е {d,n}
M(i) = (C(i)^d) mod n

M1=(9^3) mod 33 =729 mod 33 = 3(C);
M2=(1^3) mod 33 =1 mod 33 = 1(A);
M3=(29^3) mod 33 = 24389 mod 33 = 2(B);

Контрольные вопросы:

1. В чем заключается проблема распределения ключей?
2. Какие подходы к решению проблемы распределения ключей вам известны?
3. Опишите протоколы распределения открытых ключей с помощью систем с открытым ключом.
4. Что такое сеансовый ключ?
5. Опишите алгоритм шифрования RSA.
6. Что обеспечивает криптостойкость алгоритма шифрования RSA?
7. Какие математические приемы применяются при формировании ключей RSA?
8. Опишите процедуру обмена ключами, основанную на схеме Диффи-Хеллмана.
9. Что обеспечивает эффективность алгоритма Диффи-Хеллмана?
10. Что такое первообразный корень?
11. Определите цель схемы Дифии-Хеллмана.

Варианты:

№ варианта	Задание 3	Задание 4				
		q	a	X_A	Y_B	K
1	абитуриентка	5	2	4	3	5
2	балансировка	7	3	5	5	3
3	вегетарианец	11	6	8	9	10
4	глобальность	97	5	3	23	44
5	декомпрессия	13	2	8	2	9
6	здравомыслие	17	3	6	11	12
7	интерполятор	71	7	5	11	23
8	калорийность	19	5	4	7	14
9	легитимность	23	5	9	11	16
10	магнитосфера	29	3	11	7	23
11	нормирование	7	5	2	4	9
12	общественник	11	8	3	7	4
13	паритетность	13	2	11	2	6
14	самозагрузка	71	7	8	44	54
15	сердцебиение	19	5	6	6	7
16	скейтбордист	11	7	3	9	3
17	стабильность	23	5	6	14	3
18	термостатика	29	3	8	13	12
19	упадничество	11	6	7	5	3
20	факторизация	17	3	7	5	10
21	хронометрист	7	3	4	3	2
22	цветоводство	97	5	36	44	75
23	шунтирование	11	2	5	6	8
24	эксплуататор	13	2	3	11	5
25	юрисконсульт	29	3	8	17	1