Сабирова Нигора
Студентка кафедры «Программная инженерия» факультета вычислительной техники Нукусского филиала Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИСТОЧНИКОВ ИНФОРМАЦИИ, ХРАНИМЫХ В ИНТЕРНЕТЕ

Аннотация: В данной статье говорится об обеспечении безопасности информации, товаров, материальных ценностей и других услуг, хранящихся в системе Интернет, а также о реализации дистанционной связи и использовании других возможностей.

Ключевые слова: интернет, информация, система, шифрование, симметричный, метод, криптография.

Осуществление финансовых операций через интернет-систему, заказ товаров, товаров и услуг, с использованием пластиковых карт, дистанционной связи и использование других возможностей, в свою очередь, требует обеспечения информационной безопасности. Любая информация, распространяемая через Интернет-систему, всегда проходит через несколько маршрутов и серверов и достигает нужного пункта назначения. В этих областях могут возникать различные внешние угрозы целостности и целостности информации в системе. В целом система Интернета должна обеспечивать возможность неограниченного доступа к любому источнику информации. Проблема информационной безопасности приводит к системе ограничений на использование информации. Однако с помощью методов криптографии можно защитить пользователя, не ограничивая возможности. Криптографические методы основаны на алгоритме шифрования для обеспечения конфиденциальности информации. Но для возврата в исходное состояние нужен ключ для определения алгоритма шифрования. Таким образом, алгоритм и ключ являются базовой концепцией криптографии. Алгоритмы симметричного шифрования считаются неподходящими для пользователей. Основой информационной безопасности является уровень конфиденциальности симметричных ключей. Уровень безопасности оценивается количеством вариантов ключа для данного алгоритма шифрования. До сих пор очевидны некоторые недостатки шифрования с использованием симметричного закрытого ключа. Сложности возникают при генерации, хранении и доставке ключей для отправителя и получателя информации при сохранении конфиденциальности. Например, поскольку в банковской системе большое количество финансовых

клиентов, обеспечить каждого из них отдельным секретным ключом практически невозможно. Поэтому становятся известны преимущества асимметричного ключа в обеспечении информационной безопасности. В методе асимметричного ключа отправитель информации шифрует информацию с помощью открытого ключа, а получатель расшифровывает файл с помощью закрытого ключа (открывает скрытую информацию). В настоящее время широко используется свободный от недостатков симметричного метода шифрования метод шифрования на основе асимметричных ключей RSA, открытый американскими учеными Р. Ривестом, А. Шамиром и Л. Адельманом. Секретность электронной подписи, широко используемой в банковской системе, возлагается на методы, близкие к методу PC A.

Алгоритм генерации RSA-ключа:

1. Выбираются неравные друг другу простые числа;

2. n=p*q — модуль;

3. вычисляется n=(p-l)(q-l);

4. 1 <d<n определено, если оно удовлетворяет неравенству и является обратным радикалом с номером n;

5. Выбирается скрытое число d (d*e) mod n=1, удовлетворяющее уравнению; Таким образом, мы создали пару (e, ri) - открытый и (d, ri) - закрытый ключи.

Шифрование и дешифрование RSA. Чтобы зашифровать текст (e, ri) с помощью открытого ключа:

• разбиваем зашифрованный текст на блоки M(i) = 0,1,2,...,n-1;

• шифруем фрагмент текста M(i) по формуле C(i)=(M(i)e) mod n;

• создаем исходный текст, расшифровывая фрагмент зашифрованного текста C(i) с помощью закрытого ключа (d,ri) по формуле M(i)=(C(i) d) mod n.

• Открыть закрытый ключ становится неразрешимой проблемой:

• 1. Необходимо выбрать два очень больших простых числа (например, по 1024 бита каждое), не слишком далеко и не слишком близко друг к другу;

• 2. Наибольшие общие делители числа (p-l)(p-l) и (#-l)(<?-!) должны быть как можно ближе друг к другу;

• 3. Простые числа Ферма обычно принимают за число e: 17, 257, 65537, ...;

• 4. Закрытый ключ должен храниться в секрете. Упражнение 1.

• мы можем выбрать числа p=3 и q=\1; • n= 3 • Определяем число 11=33;

• (п-1)

• (q-1)=20. Так, по условию, например, e=7;

• Если мы удовлетворяем условию (d-1) mod 20=1, будет сгенерировано d= 3 числа;

• Пронумеруем буквы латинского алфавита в порядке от 0 до 26: A=1, V=2, S=3;

• шифруем текст открытым (7.33) ключом; . C(l) = (37) mod 33 = 2187 mod 33 = 9;

• C(2) = (17) mod 33 = 1 mod 33 = 1; . C(3)= (27) по модулю 33 = 128 по модулю 33 = 29

. • Расшифровать с помощью закрытого (3.33) ключа: . M(1)=(93) mod 33 = 729 mod 33 = 3-+S;

• M(2)=(13) по модулю 33 =1 по модулю 33 = 1—>A; . M(3)=(293) по модулю 33 = 24389 по модулю 33 = 2-+V. В 1977 году известный писатель и энтузиаст точных наук Мартин Гарднер опубликовал в журнале Scientific American интересный математический трактат под названием «Совершенно новый код, на решение которого уйдет миллион лет». Показывая метод шифрования, он также указал значение n для открытого ключа: n = 114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706 935 2 4 5 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541. Он пообещал денежное вознаграждение людям, которые разделят число n на простые числа. С дополнительными вопросами могут обращаться сотрудники Массачусетского технологического института Р. Ривест, А. Шамир и Л. Адельман. n опубликовал и ключ, и зашифрованный текст. 600 человек должны были работать вместе в течение 17 лет, чтобы решить эту проблему. В результате p = 32 769 132 993 266 709 549 961 988 190 834 461 413 177 642 967 992 942 539 798 288 533 q = 3 490 529 510 847 650 949 147 849 619 903 898 133 417 764 638 493 387 843 990 820 Было определено 577 номеров и раскрыт код. Таким образом, было доказано, что метод RSA обладает беспрецедентной криптографической целостностью. Выше использовались 64- и 65-значные простые числа. Поэтому только при работе с очень большими числами приоритет метода RSA при создании электронной цифровой подписи высок.

Электронная цифровая подпись (ЭЦП) создается в результате специального изменения информации электронного документа в электронном документе с использованием закрытого ключа ЭДО и заключается в определении отсутствия ошибок в информации электронного документа с использованием открытый ключ ЭДО.

[Электронная цифровая подпись (ЭОД) — это подпись, которая позволяет идентифицировать владельца закрытого ключа.

Бумажная подпись имеет такое же значение, как и личная подпись на бумажном документе, при соблюдении условий, требуемых Законом о ERI. Данные ERI представляют собой упорядоченную последовательность символов, сгенерированную в результате криптографического преобразования. Любой документ, циркулирующий в интернет-системе ERI, может иметь возможность нарушить целостность изображения или изменить его содержание. В настоящее время такой риск особенно опасен для уведомления о финансовых платежах в банковской системе. Потому что изменение адреса или суммы денег на счете носит временный характер noxush voqealarga olib kelishi muqarrarДля получения ЭРИ необходимо обратиться в орган государственной службы при Министерстве юстиции Республики Узбекистан, заполнить заявление в установленном порядке и зарегистрировать его. Выдается сроком на один год с момента регистрации и срок действия продлевается по договоренности.

В методе асимметричного ключа отправитель шифрует данные с помощью открытого ключа, а получатель шифрует файл с помощью закрытого ключа.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. В.П. Базы данных. Книга 2 распределенные и удаленные базы данных: учебник.// Москва ИД «ФОРУМ» - ИНФРА- М. -2018. - С 261.

2. Голицына О.Л. Базы данных: учеб. Пособие // - 4-е изд., иерераб. И доп. — М.: ФОРУМ: ИНФРА-М, 2018. —400 с.

3. Мартишин С.А. Базы данных. Практическое применение СУБД SQL -и NoSQL — типа для проектирования информационных систем: учеб. Пособие // - Москва: ИД «ФОРУМ» - ИНФРА-М, 2019, - 368 с.

4. Rahul Batra. SQL Primer An Accelerated introduction to SQL Basics. '/ Gurgaon, India. 2019. -P 194.

5. Ноликов А.М. Безопасность Oracle глазами аудитория: нападение и чатцита. -Москва. 2017. -336 с.

6. Usmonov J.T., Xujaqulov T. A. Ma'lumotlar bazasini boshqarish tizimi/ o'quv qo'llanma. - T. : Aloqachi, 20! 8. - 96 b.

7. Usmonov J. T., Xujaqulov T. A. Ma'lumotlar bazasini boshqarish tizimi fanidan labomloriya ishlarini bajarish bo'yicha uslubiy ko'rsatma - T. : TATU. 2016. - 55 b.

8. Eric Redmond, Jim R. Wilson. A Guide to Modern Databases and the NoSQL Movemen AQSH, 2015. - 347 c.