**Лабораторная работа №6**

**Тема:** Изучение асимметричных алгоритмов шифрования

1. **Зашифровывание алгоритмом RSА с ЭЦП**

Порядок создания ключей представлен в таблице 1.1.

Таблица 1.1. Порядок создания ключей для RSA

|  |  |  |
| --- | --- | --- |
| Действия | Абонент А (банкир) | Абонент В (вкладчик) |
| 1. Выбор двух различных простых  чисел P и Q | P = 41,Q = 29 | P = 41, Q = 7 |
| 2. Вычисление произведения  N=P\*Q | N = 41 \* 29 = 1189 | N = 41 \* 7 = 287 |
| 3. Расчет функции Эйлера ϕ(N)=N–p–q+1 | ϕ(N) = 1120 | ϕ(N) = 240 |
| 4. Выбор случайного числа D, взаимно простого с ϕ(N) из интервала 0<D | D = 3 | D = 7 |
| 5. Расчет секретного ключа E с помощью соотношения DE=1(modϕ(N)) | DE=1(mod(1120))  E=747  3\*747=2241  Остаток от деления 2241 на 1120 равняется 1, что удовлетворяет условию DE=1(modϕ(N)) | DE=1(mod(240))  E=103  7\*103=721  Остаток от деления 721 на 240 равняется 1, что удовлетворяет условию DE=1(modϕ(N)) |
| 6. Публикация открытых ключей D, N | D = 3, N = 1189 | D = 7, N = 287 |

1. А передает сообщение В.

Требуется переслать первую букву открытого сообщения, которая предварительно зашифрована методом замены числом 2. Абонент А шифрует число 2 открытым (опубликованным) ключом абонента В. Для шифрования передаваемое число 2 возводится в степень D=7, т. е.

Затем находят остаток от деления числа m на величину N=287, в результате которого получается число 110, то есть:

В линию передается число 128, которое является шифром исходного числа 2. Получив шифрограмму (128), абонент В использует свой секретный ключ E=103. Для дешифрации он возводит полученное число 128 в степень 103 и находит остаток от деления на число 287. Математически это записывается так:

В данном случае остаток от деления равен 2, значит, шифрация и дешифрирование произошли правильно. Было передано число 2, и это же число было принято после всех преобразований.

2. В передает сообщение А с ЭЦП.

Абонент В отсылает сообщение, состоящее из числа 2, абоненту А. Вначале вкладчик шифрует сообщение открытым ключом банкира:

В результате шифрования получено число 8.

Дальше вкладчик повторно шифрует это сообщение своим секретным ключом 103:

Шифрограмма 225 отправляется банкиру.

3. А расшифровывает сообщение В.

Банкир, получив секретное сообщение, использует вначале открытый ключ вкладчика:

Затем банкир использует свой секретный ключ:

В результате абонент А (банкир) получает сообщение, состоящее из числа 2.

1. **Зашифровывание алгоритмом Эль-Гамаля**

Порядок создания ключей для алгоритма Эль-Гамаля представлен в таблице 2.1.

Таблица 2.1. Порядок создания ключей для алгоритма Эль-Гамаля

|  |  |  |
| --- | --- | --- |
| Действия | Абонент А (банкир) | Абонент В (вкладчик) |
| 1. Выбор простого числа p такого, чтобы выполнялось равенство p=2q+1, где q также простое число. | q = 5, p = 11 | q = 11, p = 23 |
| 2. Выбор числа g удовлетворяющее условиям 1<g<p-1и gq(modp)≠1 | g = 2, т.к. 32(mod11)≠1 и 1<2<10 | g = 5, т.к. 48828125 (mod23)≠1 и 1<5<22 |
| 3. Выбор числа x удовлетворяющее условию 1<x<p-1 | x = 4 | x = 3 |
| 4. Вычисляется y=gx(modp). | y = 24(mod11)  y = 5 | y = 53(mod23)  y = 10 |
| 6. Публикация открытых ключей y, g, p | y = 5, g = 2, p = 11 | y = 10, g = 5, p = 23 |
| 7. Закрытый ключ х | x = 4 | x = 3 |

С помощью квадрата Полибия, представленного в таблице 2.2, было зашифровано текстовое сообщение. Результаты представлены ниже.

Таблица 2.2 – Квадрат Полибия

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | А | Б | В | Г | Д | Е/Ё |
| 2 | Ж | З | И/Й | К | Л | М |
| 3 | Н | О | П | Р | С | Т |
| 4 | У | Ф | Х | Ц | Ч | Ш |
| 5 | Щ | Ы | Ь/Ъ | Э | Ю | Я |

Открытый текст: Нос

Шифртекст: 31 32 35

1. А передает сообщение В.

Для шифрования сообщения сначала выбирается случайное число k, удовлетворяющее условию НОД(22,k)=1, k=7.

Передача первой буквы Н:

Передача второй буквы О:

Передача третьей буквы С:

2. В расшифровывает сообщения А.

Первая буква:

Результат: 31 => Н

Вторая буква:

Результат: 32 => О

Третья буква:

Результат: 35 => С

3. В передает сообщение А.

Зашифруем с помощью таблицы Полибия слово «Сон».

Результатом будет: 35 32 31.

Выберем случайное число k, удовлетворяющее условию НОД(10,k)=1, k=3.

Передача первой буквы С:

Передача второй буквы О:

Передача третьей буквы Н:

2. В расшифровывает сообщения А.

Первая буква:

Результат: 35 => С

Вторая буква:

Результат: 32 => О

Третья буква:

Результат: 31 => Н

1. **Эллиптические кривые в криптографии**

В криптографии рассматривается два вида эллиптических кривых: над конечным полем Zp  — кольцо вычетов по модулю простого числа. И над полем GF(2m) — бинарное конечное поле.

У эллиптических кривых над полем GF(2m) есть одно важное преимущество, элементы поля GF(2m)  могут быть легко представленны в виде n-битных кодовых слов, это позволяет увеличить скорость аппаратной реализации эллиптических алгоритмов.

Все математические операции на эллиптических кривых над конечным полем производятся по законам конечного поля над которым построена эллиптическая кривая. Т.е. для вычисления, например, суммы двух точек кривой E над кольцом вычетов Zp все операции производятся по модулю числа p.

Однако здесь есть свои подводные камни. Если мы сложим два одинаковых элемента из бинарного конечного поля, то получим в результате 0, т.к. сложение происходит по модулю 2. Это означает что характеристика такого поля равна 2. Но эллиптическая кривая видаописанная над полем характеристики 2 или 3 становится сингулярной, а как уже замечалось выше это неудачная идея использовать сингулярные кривые в криптографии.

Поэтому над бинарным конечным полем используются кривые вида:

Еще одним важным понятие эллиптической криптографии является порядок эллиптической кривой, который показывает количество точек кривой над конечным полем.

Теорема Хассе утверждает, что если N — количество точек кривой, определенной над полем Zq с q элементами тогда справедливо равенство:

Т.к. бинарное конечное поле GF(2n)  состоит из 2n элементов мы можем сказать, что порядок кривой E2n(a,b) равен  где.

С числом t связано следующее определение:  
эллиптическая кривая над бинарным конечным полем называется суперсингулярной, если t делится на характеристику поле (в случае бинарного поля характеристика равна 2) без остатка.  
Разумеется все это я к тому, что нельзя использовать в схемах ЭЦП суперсингулярные кривые.

Точки эллиптической кривой над конечным полем представляют собой группу. И как отмечено выше для этой группы определена операция сложения. Соответственно мы можем представить умножение числа k на точку G как G+G+..+G с k слагаемыми.

Теперь представим, что у нас имеется сообщение M представленное в виде целого числа. Мы можем зашифровать его используя выражение  
C=M\*G.

Вопрос в том, насколько сложно восстановить M зная параметры кривой E(a,b), шифротекст С и точку G.

Данная задача называется дискретным логарифмом на эллиптической кривой и не имеет быстрого решения. Более того, считается, что задача дискретного логарифма на эллиптической кривой является более трудной для решения, чем задача дискретного логарифмирования в конечных полях.

Наиболее быстрые методы, разработанные для конечных полей оказываются бесполезны в случае эллиптических кривых.

Так для решения дискретного логарифма существуют достаточно быстрые алгоритмы имеющие сложность , где c и d — некоторые константы, а p — размер поля. Такие алгоритмы называются субэкспоненциальными и позволяют сравнительно легко вскрывать дискретный логарифм в конечном поле, если размер поля не выбран очень большим, порядка 21024.

В тоже время наиболее быстрые методы решения дискретного логарифма на эллиптической кривой имеют сложность , где q — количество точек эллиптической кривой.

Таким образом, для обеспечения уровня стойкости в 280 операций необходимо чтобы q=2160. Напомню, для того, чтобы получить аналогичный уровень сложности при вычислении дискретного логарифма в конечном поле необходимо поле порядка q=21024.

Следует, однако, заметить, что поскольку мощность вычислительной техники постоянно повышается, значение q будет постоянно увеличиваться. Но так как графики функций и резко отличаются друг от друга, в группе точек эллиптической кривой q будет расти намного медленнее, чем в произвольном конечном поле.

**Выводы**

В ходе данной лабораторной работы были рассмотрены асимметричные алгоритмы шифрования. В частности, было зашифровано и расшифровано сообщение с использованием алгоритмов RSA, ЭЦП и Эль-Гамаля. Также была рассмотрена криптография на эллиптических кривых.