Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

Исследование асимметричных шифров RSA и Эль-Гамаля

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Дубалеко В.В.

Минск 2020

1. **Теоретические сведения**

Асимметричная криптография основана на сложности решения некоторых математических задач. По существу таких задач две:

* разложение больших чисел на простые сомножители (задача факторизации);
* вычисление дискретного логарифма в конечном поле;
* вычислительные операции над точками эллиптической кривой.

Эти задачи объединяет то, что они используют операцию получения остатка от целочисленного деления. В силу этого практически все системы асимметричного зашифрования/расшифрования основаны либо на проблеме факторизации (среди них – RSA), либо на проблеме дискретного логарифмирования (среди них – Эль-Гамаля).

Теорема 1. Основная теорема арифметики. Всякое натуральное число N, кроме 1, можно представить как произведение простых множителей:

N = p1\* p2\* p3\* ... \* pz, z > 1.

Определение 1. Задача дискретного логарифмирования формулируется так: для данных целых чисел а и b, 1 < а, b < n найти логарифм – такое целое число х, что

ax ≡ b (mod n),

если такое число существует. По аналогии с вещественными числами используется обозначение х = logab.

Теорема 2. Китайская теорема об остатках. В общем случае, если разложение числа N на простые множители представляет собой p1\*p2\*…\*pt (некоторые простые числа могут встречаться несколько раз), то система уравнений

(x mod pi) = ai ,

где i= 1,2…, t имеет единственное решение: x, меньшее N.

Иными словами число (меньшее, чем произведение нескольких простых чисел) однозначно определяется своими вычетами по модулю от этих простых чисел. Китайской теоремой об остатках можно воспользоваться для решения полной системы уравнений в том случае, если известно разложение числа N на простые множители

RSA – алгоритм с открытым ключом, который впоследствии стал одним из основных для шифрования и для электронных цифровых подписей. Из всех предложенных алгоритмов с открытыми ключами, RSA проще всего понять и реализовать. Названный в честь трех его создателей: Рона Ривеста (RonRivest), Ади Шамира (Adi Shamir) и Леонарда Эдлемана (Leonard Adleman). Как было отмечено, безопасность RSA основана на трудности разложения на множители больших чисел. Открытый и закрытый ключи являются функциями двух больших простых чисел. Предполагается, что восстановление открытого текста по шифртексту и открытому ключу эквивалентно разложению на множители двух больших чисел.

Для генерации двух ключей: тайного и открытого(а по сути – двух взаимосвязанных частей одного ключа, т. е. ключа, принадлежащего одному физическому лицу (или группе лиц), либо одному юридическому лицу) используются два больших случайных простых числа, p и q. Для максимальной большей криптостойкости нужно выбирать p и q равной длины. Рассчитывается произведение: n = pq. Этой есть один из трех компонент ключа, состоящего из чисел n, e, d..

Наконец расширенный алгоритм Евклида используется для вычисления третьего компонента ключа: ключа расшифрования d, такого, что выполняется условие:

ed = 1 (mod φ(n)).

Другими словами:

d-1 = e(mod φ(n)).

Для зашифрования/расшифрования используется ключ получателя: отправитель шифрует сообщение открытым ключом, а получатель расшифровывает шифртекст своим тайным ключом. Зашифрование. Если шифруется сообщение М, состоящее из r блоков: m1, m2, …, mi, …,mr, то шифртекст С будет состоять из такого же числа (r) блоков, представляемых числами:

ci = (mi)e mod n.

Расшифрование. Для расшифрования каждого зашифрованного блока производится вычисление вида:

mi = (ci)d mod n.

Алгоритм Эль-Гамаля, основан на трудности вычисления дискретных логарифмов. Алгоритм Эль-Гамаля фактически использует схему Диффи-Хеллмана, чтобы сформировать общий секретный ключ для абонентов, передающих друг другу сообщение, и затем сообщение шифруется путем умножения его на этот ключ.

И в случае шифрования, и в случае формирования цифровой подписи каждому пользователю необходимо сгенерировать пару ключей. Рассматриваемый алгоритм отличается от алгоритма RSA несколькими параметрами и особенностями:

1) генерацией ключевой информации и числом компонент, составляющих ключ;

2) каждому блоку (символу) открытого сообщения в шифртексте на основе алгоритма Эль-Гамаля соответствуют 2 блока (в RSA – один-один);

3) в алгоритме Эль-Гамаля при зашифровании используется число (обозначим его k), которое практически никак не связано с ключевой информацией получателя и которое принимает (по определению) различные значения при зашифровании различных блоков сообщения.

Генерация ключевой информации. Выбирается простое число, р. Выбирается число (g, g < p), являющееся первообразным корнем числа р – очень важный элемент с точки зрения безопасности алгоритма (см. ниже).

Далее выбирается число х (х < p) и вычисляется последний компонент ключевой информации:

y =gх mod р.

Первообразный корень (primary (residual) root ) по модулю р является таким числом, что его степени (gi, 1 ≤i≤p-1 ) дают все возможные по модулю р вычеты (остатки), которые взаимно просты с p.

Зашифрование сообщения. Как ранее, предположим, что сообщение М = {mi}, где – mi – i-й блок сообщения.

Зашифрование отправителем (каждого отдельного блокаmi исходного сообщения) предусматривает использование, как это особо подчеркивалось выше, некоторого случайного числа k (1 < k <p – 1).

В силу использования случайной величины k шифр Эль-Гамаля называют также шифром многозначной замены, а также схемой вероятностного шифрования.

Вероятностный характер шифрования является преимуществом для схемы Эль-Гамаля по сравнению, например, с алгоритмом RSA.

Блок шифртекста (ci) состоит из двух чисел: аi и bi:

ai = gk mod p,

bi = (yk \*mi) mod p.

Расшифрование ci выполняется по следующей формуле:

mi = (bi \*(ai)x)-1) mod p

или

mi = (bi \*(ai)р-x-1) mod p

где (ax)-1 – обратное значение числа ax по модулю p. Нетрудно проверить, что (ai)x)-1) = gkх mod p.

Если для зашифрования двух разных блоков (m1 и m2) некоторого сообщения использовать одинаковые k, то для соответствующих шифртекстов c1 = (a1, b1) и c2 = (a2, b2) выполняется соотношение b1(b2)-1 = m1(m2)-1. Из этого выражения можно легко вычислить m2, если известно m1.

1. **Практическая часть**

В данной лабораторной работе необходимо разработать приложения, которые должны реализовывать следующие операции:

• Приложение 1 зашифрование и расшифрование текстовых документов на основе алгоритмов RSA;

• Приложение 2 зашифрование и расшифрование текстовых документов на основе алгоритмов Эль-Гамаля;

В связи с поставленными требованиями было разработано приложение реализующее алгоритм RSA на основе встроенного пакета javax.crypto.Cipher в языке Java.

Пример шифрации:

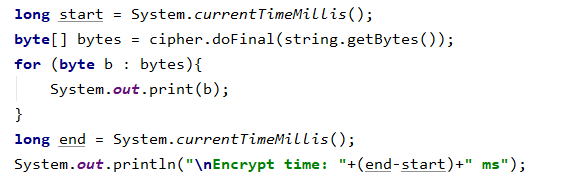


Рисунок 2.1 – Листинг шифрования RSA

Пример дешифрации:

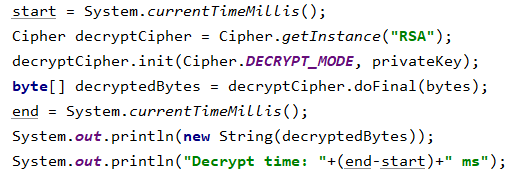


Рисунок 2.2– Листинг дешифрования

В приложении 2 было реализовано шифрование/расшифрование алгоритмом Эль-Гамаля. Ниже показан пример шифрования этим алгоритмом.

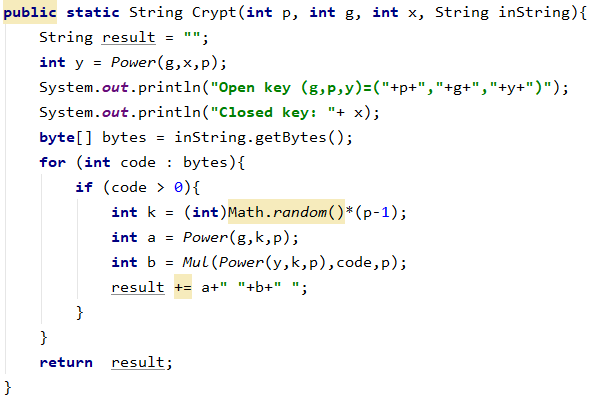
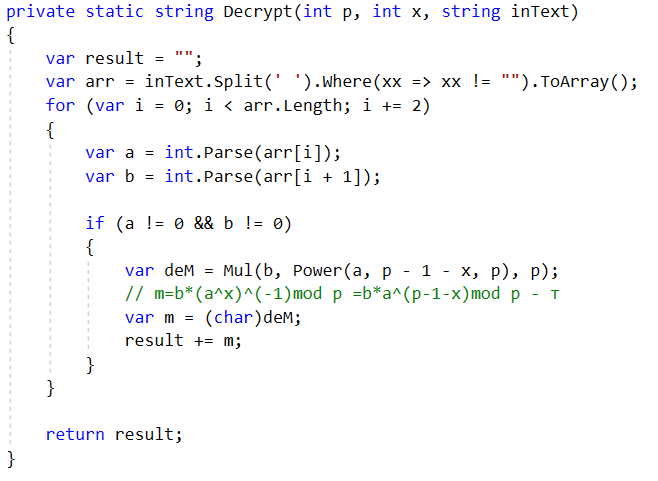


Рисунок 2.3 – Листинг шифрования

Пример дешифрации для алгоритма Эль-Гамаля:



**Вывод**

В данной лабораторной работе я закрепил теоретические знания по асимметричным шифрам. А также разработал приложения для шифрации/дешифрации по алгоритмам RSA и Эль-Гамаль.