Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Практическое задание №6

«Криптографическая защита информации»

Подготовил: студент ФИТ 2 курса 5 группы Древотень Е.В.

Проверил: асс. Берников В.О.

Цель: Овладение основными криптографическими алгоритмами асимметричного шифрования.

1. Рассказать процесс работы алгоритма RSA.

Сначала генерируются ключи.

Для этого выбираются два различных больших числа p и q. Пусть p = 3313, а q = 2039.

Вычисляется произведение (модуль) n: n = p \* q = 6 755 207.

Вычисляется функция Эйлера: φ(n) = (p-1)\*(q-1) = 6 749 856.

Выбирается открытую экспоненту: *e* = 4.

Вычисляется закрытая экспонента: *d* = ; *d* = 1 687 464.

Публикуется открытый ключ: {*e, n*} = {4, 6 755 207}.

Сохраняется закрытый ключ: {*d, n*} = {1 687 464, 6 755 207}.

Далее идёт процесс шифрования.

Принимается открытый ключ {*e, n*}: {4, 6 755 207}.

Выбирается текст для расшифровки: *m* = 123456.

Вычисляется шифротекст:

*c* = E(*m*) = = = 4453653.

Теперь расшифровывается сообщение *c*.

Принимается закрытый ключ {*d, n*}: {1 687 464, 6 755 207}.

Принимается шифротекст: *c* = 4453653.

Вычисляется исходное сообщение:

*m* = D(*c*) = = = 123456.

1. Рассказать процесс работы алгоритма Диффи-Хеллмана.

Генерация ключей:

1. Генерируется случайное простое число *p*.
2. Выбирается случайный примитивный элемент *g*.
3. Выбирается случайное целое число *x* такое, что 1 < *x* < *p* – 1.
4. Вычисляется *y* = .
5. Открытым ключом является тройка {*p, g, y*}, закрытым ключом — число *x*.

Шифрование сообщения M:

1. Выбирается сессионный ключ — случайное целое число *k* такое, что 1 < *k* < *p* – 1.
2. Вычисляются числа *a* = и *b =*  .
3. Пара чисел {*a, b*} является шифротекстом.

Расшифрование

Зная закрытый ключ *x*, исходное сообщение можно вычислить из шифротекста {*a, b*} по формуле: M = .

Для практических вычислений больше подходит следующая формула:

M = .

1. Рассказать процесс работы алгоритма Эль-Гамаля.
2. Выбирается два числа. Одно – большое простое число, а другое – целое число, меньшее первого числа. Выбор чисел может быть открытым.
3. Генерируется другое число каждым участником, которое будет храниться в тайне. Это число выполняют роль секретного ключа. Далее в вычислениях используются секретный ключ и два предыдущих целых числа. Результат вычислений посылается участниками обмена друг другу, и он играет роль открытого ключа.
4. Обмен открытыми ключами. Далее, используя собственный секретный ключ и открытый ключ партнера, конфиденциально вычисляется ключ сессии. Каждый партер вычисляет один и тот же ключ сессии.
5. Ключ сессии может использоваться как секретный ключ для другого алгоритма шифрования, например DES. Никакое третье лицо, контролирующее обмен, не сможет вычислить ключ сессии, не зная один из секретных ключей.

Вывод. Овладел основными криптографическими алгоритмами асимметричного шифрования: шифры PSA, Диффи-Хеллмана, Эль-Гамаля.