Практическое занятие №6

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

С ПОМОЩЬЮ АЛГОРИТМОВ АСИММЕТРИЧНОГО

ШИФРОВАНИЯ

Дисциплина: Основы информационной безопасности

Выполнил: Студент 2 курса 1 группы Васильев В. В.

Проверил: Ст. преп. Ржеуцкая Н. В.

**Цель занятия**

Изучение принципов работы алгоритмов асимметричного шифрования, включая алгоритм RSA, алгоритм Диффи – Хеллмана и алгоритм Эль-Гамаля.

**Теоретические сведения**

Асимметричное шифрование – это метод криптографической защиты, при котором используются два ключа: открытый (публичный) и закрытый (приватный). Открытый ключ применяется для шифрования данных, а закрытый – для их расшифровки. Такие алгоритмы широко применяются в безопасном обмене данными, цифровых подписях и аутентификации пользователей.

**Условие задания**

1. Объяснить процесс работы алгоритма RSA.
2. Объяснить процесс работы алгоритма Диффи – Хеллмана.
3. Объяснить процесс работы алгоритма Эль-Гамаля.

**Исполнительская часть**

**1. Процесс работы алгоритма RSA**

Алгоритм RSA основан на сложности факторизации больших чисел. Он включает следующие этапы:

1. Генерация ключей:
   * Выбираются два больших простых числа ***p*** и ***q*** .
   * Вычисляется их произведение ***n = p \* q***, которое используется в открытом и закрытом ключах.
   * Вычисляется значение функции Эйлера



* + Выбирается открытая экспонента ***e***, которая является взаимно простым числом с  .
  + Вычисляется закрытая экспонента ***d*** как модульное обратное ***e*** по модулю .

1. Шифрование:
   * Сообщение ***M*** преобразуется в числовой формат.
   * Вычисляется зашифрованное сообщение:  .
2. Расшифрование:
   * Вычисляется исходное сообщение: .

**2. Процесс работы алгоритма Диффи – Хеллмана**

Алгоритм Диффи – Хеллмана позволяет двум сторонам создать общий секретный ключ через незащищённый канал связи:

1. Договорённость о параметрах:
   * Выбирается большое простое число ***p*** и первообразный корень ***g*** по модулю ***p***.
2. Генерация закрытых ключей:
   * Сторона A выбирает случайное число ***a*** и вычисляет

.

* + Сторона B выбирает случайное число ***b*** и вычисляет

.

1. Обмен данными:
   * A отправляет ***A*** стороне B.
   * B отправляет ***B*** стороне A.
2. Вычисление общего ключа:
   * A вычисляет

.

* + B вычисляет

.

* + Оба значения совпадают, так как

.

**3. Процесс работы алгоритма Эль-Гамаля**

Алгоритм Эль-Гамаля основан на сложности задачи дискретного логарифмирования:

1. Генерация ключей:
   * Выбирается большое простое число ***p*** и первообразный корень ***g***.
   * Выбирается случайное число ***x*** (закрытый ключ).
   * Вычисляется  (открытый ключ).
2. Шифрование:
   * Выбирается случайное число ***k***.
   * Вычисляются два значения:
     + 
     + 
   * Пара ***(C1, C2)*** передаётся получателю.
3. Расшифрование:
   * Получатель вычисляет

, используя закрытый ключ .

**Использованные источники**

1. Уильям Ста́ллингс. "Криптография и защита сетей".
2. Ривест Р., Шамир А., Адлеман Л. "Методы шифрования на основе сложности факторизации".
3. Учебные материалы курса.
4. Веб-ресурсы .