Частное учреждение образования

Колледж бизнеса и права

|  |
| --- |
| УТВЕРЖДАЮ  Ведущий методист колледжа  \_\_\_\_\_\_\_\_\_\_\_Е.В. Паскал  «\_\_\_» 2023 |
| Специальность: 2-40 01 01 «Программное обеспечение информационных технологий» | Учебная дисциплина: «Защита компьютерной информации» | |

# Лабораторная работа №14-15

Инструкционно-технологическая карта

Тема: ***«***Реализация функции вычисления и проверки ЭЦП Эль-Гамаля***»***

Цель работы: исследовать структуры алгоритма и методики практической реализации криптосистемы шифрования Эль Гамаля.

Время выполнения: 4 часа.

СОДЕРЖАНИЕ РАБОТЫ

1. Теоретические сведения для выполнения работы
2. Практические задания
3. Контрольные вопросы
4. Литература
5. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ ДЛЯ ВЫПОЛНЕНИЯ РАБОТЫ

Схема шифрования Эль Гамаля может быть использована как для формирования цифровых подписей, так и шифрования данных.

Безопасность схемы Эль Гамаля обусловлена сложностью вычисления дискретных логарифмов в конечном поле.

В настоящее время наиболее перспективными системами криптографической защиты являются системы с открытым ключом. В таких системах для шифрования сообщения используется закрытый ключ, а для расшифрования – открытый.

Открытый ключ не является секретным и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифровывание данных с помощью открытого ключа невозможно.

Для расшифрования данных получатель зашифрованной информации использует секретный ключ, который не может быть определён из открытого ключа.

При использовании алгоритма шифрования Эль Гамаля длина шифротекста вдвое больше длины исходного открытого текста ***М***.

В реальных схемах шифрования необходимо использовать в качестве модуля n большое простое число, имеющее в двоичном представлении длину ***512… 1024 бит***.

Следует отметить, что формирование каждой подписи по данному методу требует нового значения ***k***, причём это значение должно выбираться случайным образом. Если нарушитель раскроет значение ***k***, повторно используемое отправителем, то может раскрыть и секретный ключ ***x*** отправителя.

1. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

**Схема алгоритма шифрования данных Эль Гамаля**

**1. Определение открытого «*y*» и секретного «*x*» ключей**

Выбор двух взаимно простых больших чисел ***p*** и ***q***, ***q < p***

Выбор значения секретного ключа ***x, x < p***

Определение значения открытого ключа ***y*** из выражения:

***y = qx (mod p)***

**2.Алгоритм шифрования сообщения M**

1.Выбор случайного числа ***k***, удовлетворяющего условию:

***0 ≤ k < p-1 и НОД***

2. Определение значения ***a*** из выражения: ***a = qk(mod p)***

3. Определение значения ***b*** из выражения: ***b = yk M (mod p)***

4. Криптограмма ***C,*** состоящая из ***a и b,*** отправляется получателю

5. Получатель расшифровывает криптограмму с помощью выражения***:***

**3. Процедуру шифрования данных рассмотрим на следующем примере**

( для удобства расчётов в данном примере использованы числа малой разрядности):

1.Выбираем два взаимно простых числа ***p = 11 и q = 2;***

2.Выбираем значение секретного ключа ***x, (x < p), x = 8;***

3.Вычисляем значение открытого ключа y из выражения

***y = qx (mod p) = 28 (mod 11) = 256 (mod 11) = 3***

4.Выбираем значение открытого сообщения ***M = 5;*** 3.3.5. Выбираем случайное число ***k = 9; НОД (9, 10) = 1***; 3.3.6. Определяем значение a из выражения:

***a = qk (mod p) = 29 (mod 11) = 512 (mod 11) = 6;***

7. Определяем значение ***b*** из выражения:

***b = yk M (mod p) = 39\*5 (mod 11) = 98415 (mod 11) = 9.***

Таким образом, получаем зашифрованное сообщение как ***(a, b) = (6, 9)*** и отправляем получателю.

8. Получатель расшифровает данный шифротекст, используя секретный ключ x и решая следующее сравнение:

***M\*ax ≡ b (mod p) = 5\*68 ≡ 9 (mod 11) = 8398080 ≡ 9 (mod 11)***

Вычисленное значение сообщения ***M = 5*** представляет собой заданное исходное сообщение.

**4.Содержание отчёта**

1.Составить блок-схему и программу алгоритма шифрования Эль Гамаля.

2.Листинг программы шифрования заданного сообщения с использованием алгоритма Эль Гамаля.

1. КОНТРОЛЬНЫЕ ВОПРОСЫ:
2. Что такое хэш-функция, для чего она используется? В чём заключается устойчивость к столкновениям?
3. Как обмануть подписчика, если требование устойчивости к столкновению не выполняется?
4. Схемы хэширования с длиной хэш-значения, равной длине блока.
5. Схемы хэширования с длиной хэш-значения, равной удвоенной длине блока.
6. Для чего нужна цифровая подпись? Основные свойства цифровой подписи.
7. Какие схемы цифровой подписи существуют? Какая схема самая распространенная и почему?
8. Как осуществляется подпись RSA? В чем отличие подписи RSA от алгоритма шифрования RSA?
9. Как осуществляются подпись и проверка на подлинность подписи по алгоритму Эль-Гамаля?

4. ЛИТЕРАТУРА

1. Андресс Д. Защита данных. От авторизации до аудита – Питер, 2021.
2. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 c.
3. Козлов С. Защита информации, устройства несанкционированного съема информации и борьба с ними - Академический проект, 2019.
4. Вострецова Е.В. Основы информационной безопасности – Уральский университет, 2019

Преподаватель Д.А. Бунькевич

Рассмотрено на заседании цикловой комиссии

программного обеспечения информационных технологий

Протокол № \_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2022

Председатель ЦК \_\_\_\_\_\_\_\_\_\_\_ К.О.Якимович