**Лабораторная работа № 9**

**Тема:** «Реализация элементов схемы шифрования Эль-Гамаля».

**Цель:** изучить схему шифрования Эль-Гамаля

**Контрольные вопросы.**

1. Реализация алгоритма шифрования данных Эль Гамаля:

- Выбор параметров: генерируются два больших простых числа, p и g. Число p используется для создания конечного поля, а g - для генерации генератора подгруппы.

- Генерация ключей: выбирается случайное число x (закрытый ключ), и вычисляется y (открытый ключ) по формуле y = g^x mod p.

- Шифрование: для каждого сообщения m генерируется случайное число k, и вычисляются два значения: a = g^k mod p и b = (y^k \* m) mod p. Зашифрованный текст - пара (a, b).

2. Расшифрование в алгоритме Эль Гамаля:

- Полученная пара (a, b) передается владельцу закрытого ключа.

- Вычисляется общий секретный ключ s по формуле s = a^x mod p.

- Инвертированием s находится обратный элемент s^(-1) в конечном поле по модулю p.

- Исходное сообщение восстанавливается умножением b на обратный элемент s^(-1) mod p.

3. Выбор открытого ключа в криптосистеме Эль Гамаля:

- Открытый ключ состоит из чисел p, g и y, где p и g выбираются как описано выше, а y вычисляется по формуле y = g^x mod p, где x - закрытый ключ.

4. Информационная безопасность криптосистемы Эль Гамаля:

- Безопасность основана на сложности задачи вычисления дискретного логарифма в конечных полях.

- Криптосистема обеспечивает конфиденциальность сообщений и может использоваться для обмена ключами для симметричного шифрования.

5. Преимущества криптосистемы Эль Гамаля:

- Ключевое преимущество - отсутствие прямого вычисления закрытого ключа из открытого ключа без решения сложной математической задачи.

- Эль Гамаль также поддерживает протоколы аутентификации и обмена ключами.

- Отсутствие необходимости в цифровой подписи для обеспечения аутентичности сообщений.

**Практическая часть**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Буква | Dec-код | Bin-код | Буква | Dec-код | Bin-код | Буква | Dec-код | Bin-код |
| А | 192 | 1100 000 | Л | 203 | 1100 1011 | Ц | 214 | 1101 0110 |
| Б | 193 | 1100 0001 | М | 204 | 1100 1100 | Ч | 215 | 1101 0111 |
| В | 194 | 1100 0010 | Н | 205 | 1100 1101 | Ш | 216 | 1101 1000 |
| Г | 195 | 1100 0011 | О | 206 | 1100 1110 | Щ | 217 | 1101 1001 |
| Д | 196 | 1100 0100 | П | 207 | 1100 1111 | Ь | 218 | 1101 1010 |
| Е | 197 | 1100 0101 | Р | 208 | 1101 0000 | Ы | 219 | 1101 1011 |
| Д | 198 | 1100 0110 | С | 209 | 1101 0001 | Ь | 220 | 1101 1100 |
| З | 199 | 1100 0111 | Т | 210 | 1101 0010 | Э | 221 | 1101 1101 |
| И | 200 | 1100 1000 | У | 211 | 1101 0011 | Ю | 222 | 1101 1110 |
| Й | 201 | 1100 1001 | Ф | 212 | 1101 0100 | Я | 223 | 1101 1111 |
| К | 202 | 1100 1010 | Х | 213 | 1101 0101 |  |  |  |

При оформлении отчета необходимо привести исходное сообщение (фамилию) и таблицы генерации ключей, шифрования и расшифрования. Для первого и второго способов принять, что код символа соответствует его положению в алфавите, для второго – в соответствии с кодировкой Windows 1251 (табл.3).

Исходное сообщение: «СТАНКЕВИЧ».

Задание 1. Зашифровать свою фамилию с помощью шифров гаммирования по модулю N и модулю 2.

Исходное сообщение: СТАНКЕВИЧ.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Открытое сообщение | Буква | С | Т | А | Н | К | Е | В | И | Ч |
| Dec-код | 209 | 210 | 192 | 205 | 202 | 197 | 194 | 200 | 215 |
| Bin-код | 1101  0001 | 1101 0010 | 1100 0000 | 1100 1101 | 1100 1010 | 1100 0101 | 1100 0010 | 1100 1000 | 1101 0111 |
| Гамма | Буква | К | Л | Ю | Ч | К | Л | Ю | Ч | К |
| Dec-код | 202 | 203 | 222 | 215 | 202 | 203 | 222 | 215 | 202 |
|  | Bin-код | 1100 1010 | 1100 1011 | 1101 1110 | 1101 0111 | 1100 1010 | 1100 1011 | 1101 1110 | 1101 0111 | 1100 1010 |
| Шифрограмма | Dec-код | 27 | 25 | 30 | 26 | 0 | 14 | 28 | 31 | 29 |
| Bin-код | 0001 1011 | 0001 1001 | 0001 1110 | 0001 1010 | 0000 0000 | 0000 1110 | 0001 1100 | 0001 1111 | 0001 1101 |

Зашифруем сообщение по модулю 33.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Символ | открытого сообщения, Pi | С | Т | А | Н | К | Е | В | И | Ч |
| 18 | 19 | 0 | 14 | 11 | 5 | 2 | 9 | 24 |
| гаммы, Ki | К | Л | Ю | Ч | К | Л | Ю | Ч | К |
| 11 | 12 | 31 | 24 | 11 | 12 | 31 | 24 | 11 |
| шифрограммы, Ci | Ч | Ф | Й | Л | В | Р | Б | Б | Г |
| 29 | 31 | 31 | 6 | 22 | 17 | 1 | 1 | 3 |

Задание 2. Зашифровать свою фамилию с помощью алгоритма шифрования Эль-Гамаля.

Исходное сообщение: «СТАНКЕВИЧ».

Для шифрования по алгоритму Эль-Гамаля необходимо сначала сгенерировать ключи по примеру таблицы 1.

|  |  |  |
| --- | --- | --- |
| № п/п | Описание операции | Пример |
| 1 | Выбирается простое число p. | p = 17 |
| 2 | Выбирается число g, являющееся первообразным корнем по модулю p и меньшее p. | g = 3 |
| 3 | Выбирается произвольное число x, меньшее p. | x = 2 |
| 4 | Вычисляется y = gx mod p | y = 32 mod 17 = = 9 mod 17 = 9 |
| 5 | Открытый ключ – y, g и p. Причем g и p можно сделать общими для группы пользователей.  Закрытый ключ – x. |  |

Допустим k = 15. Тогда:

a = gk mod p = 315 mod 17 = 6,

b = (yk \* T) mod p = (915 \* T) mod 17,

T = (b \* ap-1-x) mod p = (b \* 614) mod 17.

Теперь зашифруем сообщение по примеру таблицы 2.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Открытое сообщение, T | Символ | C | Т | А | Н | К | Е | В | И | Ч |
| Код | 18 | 19 | 0 | 14 | 11 | 5 | 2 | 9 | 24 |
| Вторая часть шифрограммы,  b = (915 \* T) mod 17 | | 2 | 4 | 0 | 11 | 5 | 10 | 4 | 1 | 14 |
| Открытое сообщение,  T = (b \* 6­14) mod 37 | | 18 | 19 | 0 | 14 | 11 | 5 | 2 | 9 | 24 |