**Лабораторная работа № 8**

**Тема:** «Открытое распределение ключей с использованием криптосистемы RSA».

**Цель:** изучить принципы функционирования криптосистемы RSA.

**Контрольные вопросы.**

1. Охарактеризовать достоинства и недостатки асимметричных криптосистем.

Достоинства:

- Безопасность ключей: Каждый пользователь имеет пару ключей — открытый и закрытый. Закрытый ключ хранится конфиденциально, обеспечивая безопасность.

- Распределение открытых ключей: Открытые ключи могут быть распределены открыто, что облегчает процесс установления безопасного канала связи.

- Эффективность ключевого обмена: Упрощение процесса обмена ключами, так как не требуется секретного обмена.

Недостатки:

- Вычислительная сложность: Асимметричные операции более затратны с точки зрения вычислительных ресурсов, чем симметричные, что может быть проблемой при работе с большими объемами данных.

- Проблемы с производительностью: Сравнительно медленные скорости работы, особенно в сравнении с симметричными криптосистемами.

- Опасности от атак с открытым текстом и выбором открытого текста (Chosen-plaintext attack): Существует угроза, что злоумышленник может сравнивать результаты шифрования для разных открытых текстов и анализировать полученные шифры.

2. Перечислить основные требования, обеспечивающие безопасность асимметричных криптосистем.

- Длина ключа: Ключи должны быть достаточно длинными, чтобы предотвратить атаки перебора. Чем длиннее ключ, тем более безопасна криптосистема.

- Качественный генератор случайных чисел: Надежность ключей зависит от случайности их генерации.

- Безопасность открытого текста (Chosen-plaintext attack): Криптосистема должна быть стойкой к атакам, где злоумышленник имеет доступ к открытым текстам и их шифрам.

- Устойчивость к атакам с выбором открытого текста (Chosen-ciphertext attack): Система должна быть устойчивой к атакам, при которых злоумышленник может выбирать открытые тексты и получать соответствующие шифры.

- Стойкость к факторизации больших чисел: Безопасность асимметричных систем, основанных на факторизации больших чисел, зависит от сложности разложения на простые множители.

**Практическая часть**

Таблица 1 – Процедура создания ключей

|  |  |  |
| --- | --- | --- |
| № п/п | Описание операции | Пример |
| 1 | Выбираются два простых числа p и q. | p = 7  q = 13 |
| 2 | Вычисляется произведение n = p \* q. | n = 91 |
| 3 | Вычисляется функция Эйлера ϕ(n). | ϕ(n) = (7-1)(13-1) =  91 – 7 – 13 + 1 = 72 |
| 4 | Выбиарется произвольное число e (0 < e < n), взаимно простое с результатом функции Эйлера (e ⊥ ϕ(n)). Число e называется открытой экспонентой. | e = 5 |
| 5 | Вычисляется секретный ключ d из соотношения (d \* e) mod ϕ(n) = 1. Число d называется закрытой экспонентой. Обычно пользуются выражением de = 1 + kϕ(n), где k – некоторое целое число. | (d \* 5) mod 72 = 1  d = 29 |
| 6 | Публикуются открытые ключи e и n в специальном хранилище, где исключается возможность его подмены (общедоступном сертифицированном справочнике). |  |

Таблица 2 – Пример шифрования по алгоритму RSA

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Открытое сообщение, T | Символ | А | Б | Р | А | М | О | В |
| Код | 1 | 2 | 18 | 1 | 14 | 16 | 3 |
| Шифрограмма, C = T5 mod 91 | | 1 | 32 | 44 | 1 | 14 | 74 | 61 |
| Открытое сообщение, T = C29 mod 91 | | 1 | 2 | 18 | 1 | 14 | 16 | 3 |

Таблица 3 – Кодировка русского алфавита

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |

Таблица 4 – Вариант задания

|  |  |  |  |
| --- | --- | --- | --- |
| № варианта | p | q | Открытый ключ e |
| 17 | 19 | 13 | 11 |

Задание 1. Пользуясь алгоритмом RSA, рассчитать сеансовый ключ, используя данные своего варианта. зашифруйте свою фамилию, предварительно закодировав его согласно прилагаемым таблицам 1, 2 (Приложение А) и расшифруйте его. Параметры алгоритма указаны в таблице вариантов (таблица 3 Приложения А).

Создадим ключи. по алгоритму таблицы 1.

Таблица 5 – Процедура создания ключей

|  |  |  |
| --- | --- | --- |
| № п/п | Описание операции | Пример |
| 1 | Выбираются два простых числа p и q. | p = 19  q = 13 |
| 2 | Вычисляется произведение n = p \* q. | n = 247 |
| 3 | Вычисляется функция Эйлера ϕ(n). | ϕ(n) = (19-1)(13-1) = 216 |
| 4 | Выбиарется произвольное число e (0 < e < n), взаимно простое с результатом функции Эйлера (e ⊥ ϕ(n)). Число e называется открытой экспонентой. | e = 11 |
| 5 | Вычисляется секретный ключ d из соотношения (d \* e) mod ϕ(n) = 1. Число d называется закрытой экспонентой. Обычно пользуются выражением de = 1 + kϕ(n), где k – некоторое целое число. | k = 3  d = (1 + k \* ϕ(n)) / e =  = (1 + 3 \* 216) / 11 = 59 |
| 6 | Публикуются открытые ключи e и n в специальном хранилище, где исключается возможность его подмены (общедоступном сертифицированном справочнике). | Публикуем открытый ключ:  {e, n} = {11, 247}  Сохраняем закрытый ключ:  {d, n} = {59, 247} |

Зашифруем фамилию в соответствии с таблицей 2.

Таблица 6 – Пример шифрования по алгоритму RSA

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Открытое сообщение, T | Символ | М | И | К | У | Ц | Е | В | И | Ч |
| Код | 14 | 10 | 12 | 21 | 25 | 6 | 3 | 10 | 25 |
| Шифрограмма, C = T11 mod 247 | | 222 | 147 | 103 | 148 | 207 | 245 | 48 | 147 | 207 |
| Открытое сообщение, T = C59 mod 247 | | 14 | 10 | 12 | 21 | 25 | 6 | 3 | 10 | 25 |

Получаем шифр: 222 147 103 148 207 245 48 147 207.

Задание 2. По примеру необходимо зашифровать свою фамилию. Открытый текст: «Фамилия». Ключ «КЛЮЧ».

Таблица 7 – Пример шифрования

|  |  |  |  |
| --- | --- | --- | --- |
| Открытый текст | Ключ | Преобразование | Шифр |
| З | К | y1=8+11(mod33)=19 | Т |
| А | Л | y2=1+12(mod33)=13 | М |
| М | Ю | y3=13+31(mod33)=11 | К |
| Е | Ч | y4=6+24(mod33)=30 | Э |
| Н | К | y5=14+11(mod33)=25 | Ш |
| А | Л | y6=1+12(mod33)=13 | М |

Зашифруем наше сообщение в соответствии с примером задания.

Таблица 8 – Шифрование

|  |  |  |  |
| --- | --- | --- | --- |
| Открытый текст | Ключ | Преобразование | Шифр |
| М | К | y1=13+11(mod33)=24 | Ч |
| И | Л | y2=9+12(mod33)=21 | Ф |
| К | Ю | y3=11+31(mod33)=9 | И |
| У | Ч | y4=20+24(mod33)=11 | К |
| Ц | К | y5=23+11(mod33)=1 | Б |
| Е | Л | y6=5+12(mod33)=17 | Р |
| В | Ю | y7=2+31(mod33)=0 | А |
| И | Ч | y8=9+24(mod33)=0 | А |
| Ч | К | y9=24+11(mod33)=2 | В |

Получаем шифр: «ЧФИКБРААВ».