**Практическое занятие №6**

**Тема «Криптографическая защита информации»**

**Цель:** Овладение основными криптографическими алгоритмами асимметричного шифрования .

**Теоретическое введение**

# Реализация элементов криптосистемы RSA

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и других.

Весь алгоритм расписан в таблице:

Таблица 8.1 – Алгоритм RSA

|  |  |  |
| --- | --- | --- |
| Этап | Описание операции | Результат операции |
| Генерация ключей | Выбрать два простых различных числа | p=3557,  q=2579 |
| Вычислить модуль (произведение) | n = p \cdot q = 3557 \cdot 2579 = 9173503 |
| Вычислить функцию Эйлера | \varphi(n) = (p-1) (q-1) = 9167368 |
| Выбрать открытую экспоненту | e = 3 |
| Вычислить секретную экспоненту | d = e^{-1} \mod \varphi(n)  d = 6111579 |
| Опубликовать открытый ключ | \{e, n\} = \{3,9173503 \} |
| Сохранить закрытый ключ | \{d, n\} = \{6111579, 9173503 \} |
| Шифрование | Выбрать текст для зашифровки | m = 111111 |
| Вычислить шифротекст | \begin{align} c &= E(m) \\  &= m^e \mod n \\  &= 111111^3   \mod 9173503 \\  &= 4051753 \end{align} |
| Расшифрование | Вычислить исходное сообщение | \begin{align} m &= D(c) = \\   &= c^d \mod n \\   &= 4051753^{6111579} \mod 9173503 \\   &= 111111 \end{align} |

# Реализация элементов схемы шифрования Эль-Гамаля

# ****Генерация ключей****

1. Генерируется случайное простое число ~p длины ~n [битов](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82).
2. Выбирается случайный примитивный элемент ~g.
3. Выбирается случайное целое число ~x такое, что ~1 < x < p-1.
4. Вычисляется ~y = g^x\,\bmod\,p.
5. Открытым ключом является тройка \left( p,g,y \right), закрытым ключом — число ~x.

**Шифрование**

Сообщение ~M шифруется следующим образом:

1. Выбирается сессионный [ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) — случайное целое число ~k такое, что ~1 < k < p - 1
2. Вычисляются числа a = g^k\,\bmod\,p и b = y^k M\,\bmod\,p.
3. Пара чисел \left( a, b \right) является [шифротекстом](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82).

Нетрудно видеть, что длина шифротекста в схеме Эль-Гамаля длиннее исходного сообщения M вдвое.

**Расшифрование**

Зная закрытый ключ ~x, исходное сообщение можно вычислить из шифротекста \left( a, b \right) по формуле:

M = b(a^x)^{-1}\,\bmod\,p.

При этом нетрудно проверить, что

~(a^x)^{-1}\equiv g^{-kx}\pmod{p}

и поэтому

~b(a^x)^{-1}\equiv (y^kM)g^{-xk}\equiv (g^{xk}M) g^{-xk}\equiv M \pmod{p}.

Для практических вычислений больше подходит следующая формула:

M = b(a^x)^{-1}\,\bmod\,p = b \cdot a^{(p-1-x)}\,\bmod\,p **.**

**Пример**

**Шифрование**

Допустим, что нужно зашифровать сообщение ~M=5.

Произведем генерацию ключей :

пусть ~p=11, g=2. Выберем ~x=8 - случайное целое число ~x такое, что ~1 < x < p.

Вычислим ~y= g^x\bmod{p}=2^8\bmod{11}=3.

Итак, открытым является тройка ~(p,g,y)=(11,2,3), а закрытым ключом является число ~x=8.

Выбираем случайное целое число ~k такое, что 1 < k < (p − 1). Пусть ~k=9.

Вычисляем число ~a=g^k\bmod{p}=2^9 \bmod{11}=512 \bmod{11}=6.

Вычисляем число ~b=y^k M\bmod{p}=3^9 5 \bmod{11}=19683 \cdot 5 \bmod{11}=9.

Полученная пара ~(a,b)=(6,9) является шифротекстом.

Расшифрование

Необходимо получить сообщение ~M=5 по известному шифротексту ~(a,b)=(6,9) и закрытому ключу ~x=8.

Вычисляем M по формуле : ~M=b(a^x)^{-1}\bmod{p}=9(6^8)^{-1}\mod{11}=5

Получили исходное сообщение ~M=5.

# Реализация элементов схемы шифрования Дифи-Хеллмана

# ****Генерация ключей****

В 1976 году после публичной критики алгоритма DES и указания на сложность обработки секретных ключей Уитфилд Диффи (Whitfield Diffie) и Мартин Хеллман (Martin Hellman) опубликовали свой алгоритм обмена ключами. Это была первая публикация на тему криптографии с открытым ключом и, возможно, самый большой шаг вперед в области криптографии, сделанный когда‑либо.

Из‑за невысокого быстродействия, свойственного асимметричным алгоритмам, алгоритм Диффи‑Хеллмана не предназначен для шифрования данных. Он был ориентирован на передачу секретных ключей DES, ARS или других подобных алгоритмов через небезопасную среду. В большинстве случаев алгоритм Диффи‑Хеллмана не используется для шифрования сообщений, потому что он, в зависимости от реализации, от 10 до 1000 раз медленнее алгоритма DES.

До алгоритма Диффи‑Хеллмана было сложно совместно использовать зашифрованные данные из‑за проблем хранения ключей и передачи информации. В большинстве случаев передача информации по каналам связи небезопасна, потому что сообщение может пройти десятки систем, прежде чем оно достигнет потенциального адресата, и нет никаких гарантий, что по пути никто не сможет взломать секретный ключ. Уитфилд Диффи и Мартин Хеллман предложили зашифровывать секретный ключ DES по алгоритму Диффи‑Хеллмана на передающей стороне и пересылать его вместе с сообщением, зашифрованным с использованием DES. Тогда на другом конце его сможет расшифровать только получатель сообщения.

На практике обмен ключами по алгоритму Диффи‑Хеллмана происходит по следующей схеме.

1. Два участника обмена договариваются о двух числах. Один выбирает большое простое число, а другой – целое число, меньшее числа первого участника. Переговоры они могут вести открыто, и это никак не отразится на безопасности.
2. Каждый из двух участников, независимо друг от друга, генерирует другое число, которое они будут хранить в тайне. Эти числа выполняют роль секретного ключа. Далее в вычислениях используются секретный ключ и два предыдущих целых числа. Результат вычислений посылается участнику обмена, и он играет роль открытого ключа.
3. Участники обмена обмениваются открытыми ключами. Далее они, используя собственный секретный ключ и открытый ключ партнера, конфиденциально вычисляют ключ сессии. Каждый партер вычисляет один и тот же ключ сессии.
4. 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.

## **Пример**

Ева — криптоаналитик. Она читает пересылку Боба и Алисы, но не изменяет содержимого их сообщений.

* s = секретный ключ. s = 2
* g = простое число меньшее p. g = 5
* p = открытое простое число. p = 23
* a = секретный ключ Алисы. a = 6
* A = открытый ключ Алисы. A = ga mod p = 8
* b = секретный ключ Боба. b = 15
* B = открытый ключ Боба. B = gb mod p = 19

Таблица 8.2 – Алгоритм Дифи-Хеллмана



**Задание для выполнения**

1. Написать программу, которая получит общий секретный ключ из доступных публичных ключей с помощью алгоритма Диффи-Хеллмана.

Генерируйте секретный ключ Алисы и Боба, и высчитайте секретный ключ, удостоверьтесь что его одинаково смогут получить и Алиса и Боб.

Приложение 8.1 – Код рабочей программы на С++

std::cout << "\n-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-";

std::cout << "\n| Алгоритм Диффи-Хеллмана |";

std::cout << "\n-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-";

std::cout << "\nUser 1: \t\tUser 2:\nPublic key:" << pub\_1 << " \t\tPublic key:" << pub\_2;

std::cout << "\nPrivate Key:" << pri\_1 << " \tPrivate Key:" << pri\_2;

int part\_1 = (int)pow(pub\_1, pri\_1) % pub\_2;

int part\_2 = (int)pow(pub\_2, pri\_2) % (pub\_1);

std::cout << "\nPartial Key:" << part\_1 << " \tPartial Key:" << part\_2;

int full\_2 = (int)pow(part\_1, pri\_2) % (pub\_1);

int full\_1 = (int)pow(part\_2, pri\_1) % (pub\_2);

std::cout << "\nFull Key:" << full\_1 << " \tFull Key:" << full\_2<<std::endl;

1. Написать программу, которая зашифрует и расшифрует текст, введенный с клавиатуры, зашифрует и расшифрует его алгоритмом RSA.

Таблица 8.3 – Ключи для алгоритма RSA

|  |  |  |  |
| --- | --- | --- | --- |
| # | e | n | d |
| 1 | 13 | 1073 | 853 |
| 2 | 7 | 533 | 343 |
| 3 | 17 | 391 | 145 |
| 4 | 11 | 1121 | 95 |
| 5 | 17 | 497 | 173 |
| 6 | 17 | 989 | 761 |
| 7 | 5 | 559 | 101 |
| 8 | 13 | 403 | 277 |
| 9 | 17 | 493 | 369 |
| 10 | 11 | 779 | 131 |

Приложение 8.2 – Код рабочей программы на С++

long long e = 17, n = 391, d = 145; // открытая экспонента, {закрытый ключ}

std::cout << "\n-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-";

std::cout << "\n| Алгоритм RSA |";

std::cout << "\n-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-";

std::cout << "\nИсходный текст:\t" << text;

std::cout << "\nОткрытая экспонента:\t" << e;

std::cout << "\nОткрытый ключ {d,n}:\t{" << d << ", " << n << "} ";

std::cout << "\nЗакрытый ключ {d,n}:\t{" <<d<<", "<<n<<"} " ;

long long newtext = (long long)pow(text, e) % n;

long long prevText = (long long)pow(newtext, d) % n;

std::cout << "Зашифрованный текст:\t" << newtext;

std::cout << "Расшифрованный текст:\t" << prevText<<std::endl;

1. Написать программу, которая сгенерирует ключи, зашифрует и расшифрует текст, введенный с клавиатуры алгоритмом Эль-Гамаля.

Приложение 8.3 – Код рабочей программы на С++

std::cout << "\n-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-";

std::cout << "\n| Алгоритм Эль-Гамаля |";

std::cout << "\n-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-";

srand(time(NULL));

int p =1+3\* rand() % 10;

int n = bitNum(p);

std::cout << "\nСлучайное число: "<<p <<" длиной "<<n<<" бит";

int g=1+rand() % 9;

std::cout << "\nСлучайный примитивный элемент: " << g ;

int x = 2\*rand() % 10;

std::cout << "\nСлучайное целое число x:{1<x<p-1}: " << x;

int y = (int)pow(g, x) % p;

if (y == 0) y = 1;

std::cout << "\nОткрытый ключ (p,g,y): (" << p << ", " << g << ", " << y << ")";

std::cout << "\nЗакрытый ключ: " << x;

int k = 1 + rand() % (p + 1);

std::cout << "\nСессионный ключ: " << k;

int a = (int)pow(g, k) % p;

int b = (int)pow(y, k) \* text % p;

std::cout << "Шифротекст: (" << a << ", " << b << ")";

int text2 = b \* (int)pow(a, p - 1 - x) % p;

std::cout << "Исходный текст: " << text2;

**Вывод:** Были изучены основные криптографические алгоритмы асимметричного шифрования .