



Криптография: алгоритм RSA

Выполнила:
Ученица 8а класса.
Семёнова Екатерина Вадимовна

Научный руководитель:
Князькина Татьяна Викторовна

Цели и задачи

Цель проекта : изучение системы шифрования с открытым ключом RSA.

Задачи проекта:

- Ознакомиться с основными понятиями криптографии.
- Изучение основных принципов симметрических криптосистем.
- Изучение основных принципов асимметрических криптосистем.
- Ознакомиться с методами теории чисел, используемых в RSA.
- Изучение алгоритма RSA.
- Продемонстрировать на примерах шифрование и дешифрование различных сообщений по алгоритму RSA.



Основные понятия

Криптология (kryptos - тайный, logos - наука) - наука, изучающая математические методы защиты информации путем ее преобразования.

Криптография - занимается поиском и исследованием математических методов преобразования информации.

Криптоанализ - занимается исследованием возможности расшифровывания информации без знания ключей.

Шифрование - преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом (называемый также криптограммой) .

Дешифрование - обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Симметричные системы

В них, как связаться друг с другом, должны заранее договориться между собой об



Алгоритм создания открытого и секретного ключей Шифрование и дешифрование: схема RSA

RSA

Сообщением являются целые числа лежащие от 0 до $m-1$.

1. Выберем два простых числа p и q .

Алгоритм шифрования

1. Взять *открытый* ключ

(e, m) .

2. Взять *открытый* текст

$0 \leq a \leq m-1$

3. Получить

криптограмму b :

$$b = a^e \bmod m$$

4. Передать зашифрованное

сообщение b .

Алгоритм дешифрования

1. Принять зашифрованное

сообщение b .

2. Применить свой *секретный* ключ

(d, m) для расшифровки сообщения:

представление $\text{НОД}(e, \phi(m))$

равно 1 , то $a = b^{d^{-1}}$

Эвклида.)

секретного ключа RSA

ли p и q можно ли

уничтожить либо сохранить вместе с секретным



Алгоритм RSA: пример

пример

Алгоритм шифрования

1. Возьмем открытый ключ $(e, m) = (5, 85)$.
2. Возьмем открытый текст $a = 7$.
3. Получить криптограмму b :

$$b = a^e \bmod m = 7^5 \bmod 85 = 16807$$

4. Передать зашифрованное сообщение $b = 62$.

$$\text{НОД}(5, 84) = 1 \quad | \quad \text{НОЛ}(5, 64) = 1 = d * 5 + c * 64 = 13 * 5 + (-1) * 64 \quad |$$



Алгоритм дешифрования

1. Принять зашифрованное сообщение $b = 62$.
2. Применить свой секретный ключ $(d, m) = (13, 85)$ для расшифровки сообщения:

$$a = b^d \bmod m = 62^{13} \bmod 85 = 200028539268669788905472 \bmod 85 = 7$$

RSA.

Криптоанализ

RSA

Почему же систему RSA трудно

взломать?

Ловушка в системе RSA заключается в том, что умножение чисел p и q для получения числа m — простая операция, тогда как обратная задача — разложение числа m на множители для получения p и q — практически неразрешима.



Основные результаты работы

- Изучены основные виды симметрических криптосистем: шифры замены и шифры перестановки.
- Изучены основные принципы асимметрических криптосистем.
- Изучены понятия и методы теории чисел, используемых в RSA: алгоритм Евклида нахождения НОД, расширенный алгоритм Евклида, функция Эйлера и ее свойства.
- Изучен алгоритма RSA.
- Разобрано 5 примеров шифрования и дешифрования различных высказываний великих математиков по алгоритму RSA

