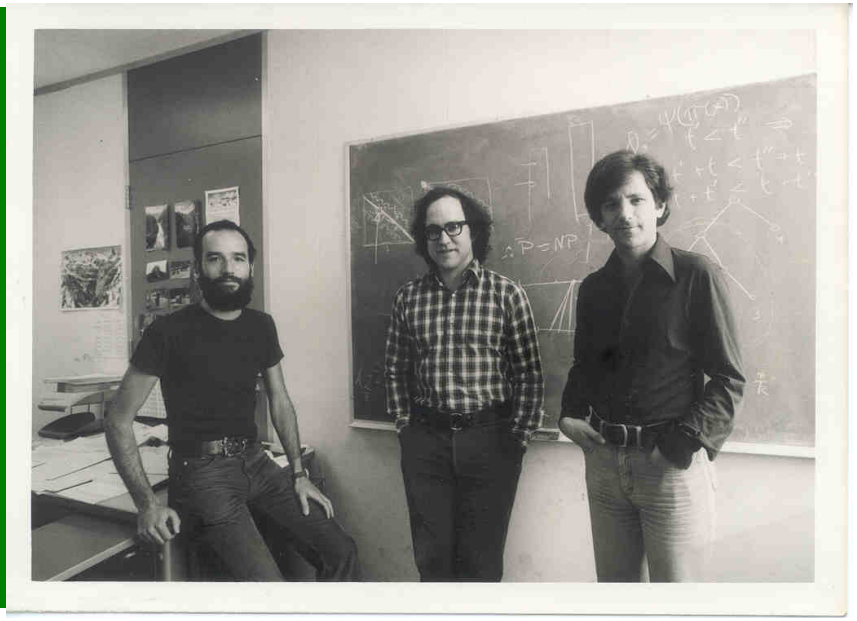
Криптографический алгоритм RSA.

Гимназия N610,
Дарья Дическул,
Апрель 2012.



Оглавление

Термины

- RSA
- Криптографическая система с открытым ключом
- Открытый ключ
- Закрытый ключ
- Электронная подпись

История

Дата	Событие
1976, Ноябрь	Уитфилд Диффи и Мартин Хеллман, «Новые направления в криптографии».
1977, Август	Ronald Linn Rivest, Adi Shamir и Leonard Adleman опубликовали свой алгортим в журнале «Scientific American».
1977	Фраза, за расшифровку которой была обещана награда в 100 долларов США.
1982	Организована компания RSA Data Security.
1983	Выдан патент на RSA (до 2000 г.).
1990	Использование алгоритма министерством обороны США.

НО …

Дата	Событие
1969	Штаб-квартира правительственной связи в Великобритании: Клиффорд Кокс, Малькольм Вильямсон и Джеймс Эллис.
1997	Обнародование информация, согласно которой криптосистема аналогичная RSA была описана в 1973 году.

Односторонние функции:

- Если известно x, то f(x) вычислить относительно просто
- Если известно f(x), то для вычисления x нет простого пути.

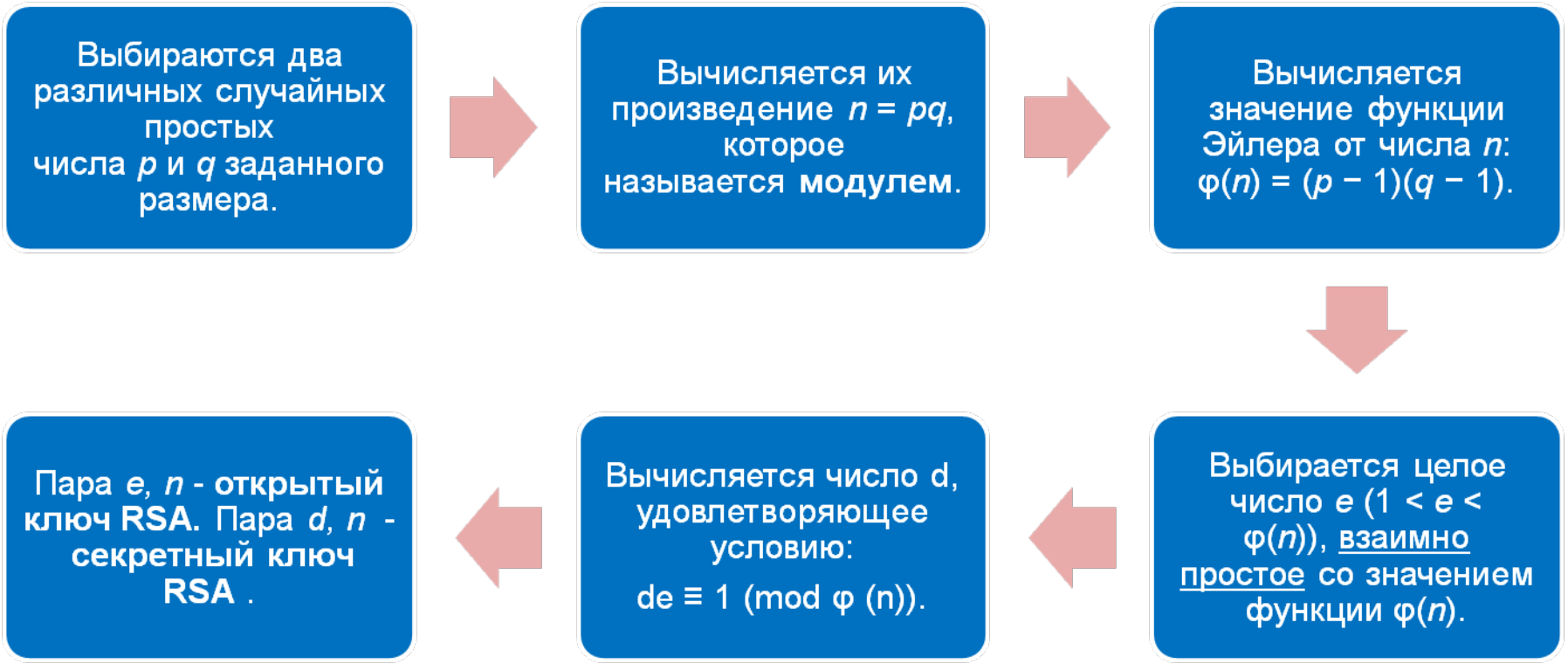
Открытый и закрытый ключи являются **взаимно обратными**, т.е:
ڍ قفطظلعفع معفع MڬW, عظظ W ᾳ غفعفعقظقف ظفقفقعقعلك
غعفعلظفطفق;

□ открытого и секретного ключа P и S;

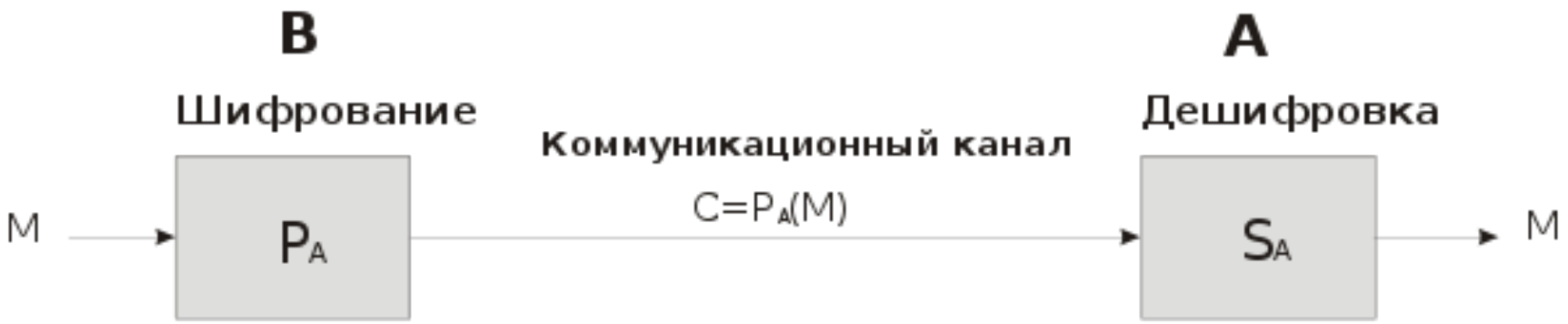
□ соответствующие функции шифрования E_p и расшифрования D_s:

$$M = D_s(E_p(M))$$
$$M = E_s(D_p(M))$$

Описание алгоритма. Создание открытого и секретного ключей.



Описание алгоритма. Шифрование и дешифрование.



Алгоритм:

1. Взять *открытый ключ* (e, n) стороны A;
2. Взять открытый текст M;
3. Передать шифрованное сообщение:

$$P_a(M)=M^e \bmod n$$

Алгоритм:

1. Принять зашифрованное сообщение C;
2. Применить свой *секретный ключ* (d,n) для расшифровки сообщения:

$$S_a(C)=C^d \bmod n$$

Зашифруем и расшифруем сообщение "CAB" по алгоритму RSA.

Описание алгоритма. Пример.

Выберем p=3 и q=11.

Выбираются два различных случайных простых числа p и q заданного размера.

Определим n= 3*11=33.

Вычисляется их произведение $n = pq$, которое называется **модулем**.

Найдем (p-1)*(q-1)=20.

Вычисляется значение функции Эйлера от числа n: $\varphi(n) = (p - 1)(q - 1)$.

Выбирается целое число e ($1 < e < \varphi(n)$), взаимно простое со значением функции $\varphi(n)$.

e, например, равно, 7: (e=7)

Вычисляется число d, удовлетворяющее условию:

$de \equiv 1 \pmod{\varphi(n)}$.

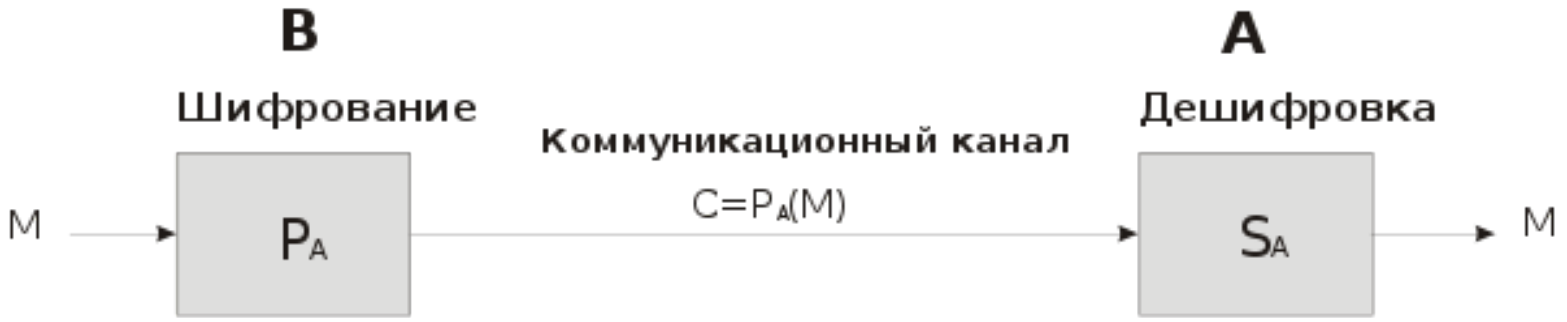
(d*7) mod 20=1. d, например, равно 3: (d=3)

Пара e, n - **открытый ключ RSA.** Пара d, n - **секретный ключ RSA** .

Откр. ключ {7,33}, Закр. ключ {3,33}.

Описание алгоритма. Пример.

Представим шифруемое сообщение как последовательность чисел в диапазоне от 0 до 32. Буква А =1, В=2, С=3.



1. Взять *открытый ключ* (e, n) стороны А;
2. Взять открытый текст М;
3. Передать шифрованное сообщение:

$$P_a(M)=M^e \bmod n$$

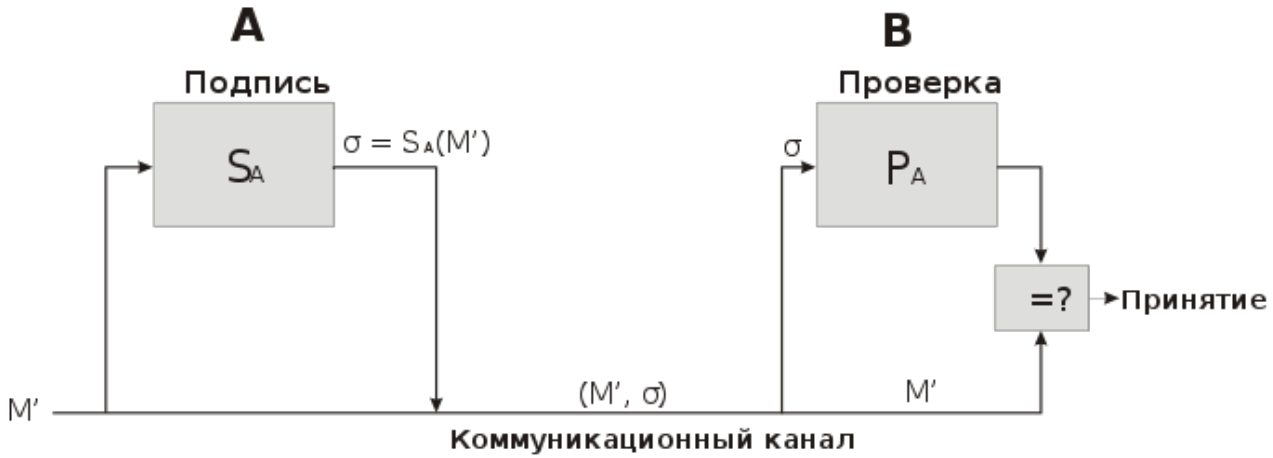
C1 = (3^7) mod 33 = 2 187 mod 33 = 9;
C2 = (1^7) mod 33 = 1 mod 33 = 1;
C3 = (2^7) mod 33 = 128 mod 33 = 29;

1. Принять зашифрованное сообщение С;
2. Применить свой *секретный ключ* (d,n) для расшифровки сообщения:

$$S_a(C)=C^d \bmod n$$

M1=(9^3) mod 33 =729 mod 33 = 3 (C);
M2=(1^3) mod 33 =1 mod 33 = 1(A);
M3=(29^3) mod 33 = 24 389 mod 33 = 2(B);

Описание алгоритма. Цифровая подпись.



Алгоритм:

1. Взять *открытый текст* M';
2. Создать цифровую подпись б с помощью своего секретного ключа (d, n):

$$б = S_a(M') = M'^{d} \bmod n$$

3. Передать пару (M' , б).

Алгоритм:

1. Принять пару (M' , б).
2. Взять открытый ключ (e, n) стороны A.
3. Проверить подлинность подписи:

$$P_a(б) = б^{e} \bmod n \equiv M' \rightarrow$$ подпись верная

P и Q не должны быть слишком близки друг к другу, иначе можно будет их найти, используя метод факторизации Ферма.

Криптоанализ RSA. Схема с общим модулем.

Начальные данные: Защищённый сервер использует единый n для шифрования всех сообщений. Сторона A использует этот сервер для получения сообщения M.

Задача: противник хочет расшифровать сообщение стороны A.

Защита: для каждого пользователя должен использоваться свой модуль n.

Криптоанализ RSA. Атака на подпись RSA в схеме с нотариусом.

Начальные данные: (n, e) - открытый ключ нотариуса. Противник получает отказ при попытке подписания нотариусом сообщения M.

Задача: противник хочет получить подпись нотариуса на сообщении M.

Защита: при подписи добавлять в сообщение некоторое случайное число (например, время).

С помощью квантового компьютера можно будет взломать RSA, применив алгоритм Шора.

СПАСИБО!

Первое описание криптосистемы

9686	9613	7546	2206
1477	1409	2225	4355
8829	0575	9991	1245
7431	9874	6951	2093
0816	2982	2514	5708
3569	3147	6622	8839
8962	8013	3919	9055
1829	9451	5781	5154

«THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE»

НАЗАД