Напоминание. Т. Эйлера

$$a^{\varphi(m)} \underset{m}{\equiv} 1, \quad \text{если} \quad (a,m)=1.$$

Пример: $7^{\varphi(11)} \underset{11}{\equiv} 1 \iff 7^{10} \underset{11}{\equiv} 1$

Сл-ие 1 (Т. Ферма, малая) $a \in \mathbb{Z}$

$$a^{p-1} \underset{p}{\equiv} 1 \quad \text{если} \quad a \nmid p \quad p \in \mathbb{P}.$$

Д-во $\varphi(p) = p-1$ если $p \in \mathbb{P}$

$a \nmid p \iff (a,p)=1$

$(a,p)=d>1 \Rightarrow a \vdots d$

$p \vdots d \Rightarrow d=p$ ∎

Сл-ие 2 $a \in \mathbb{Z}$ Если $p \in \mathbb{P}$, то

$$\boxed{a^p \underset{p}{\equiv} a}$$ (неважно, $a \vdots p$ или нет p)

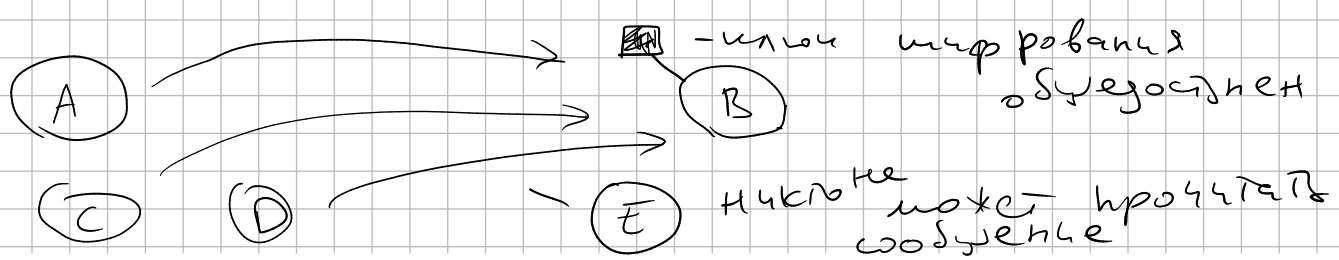
Д-во Если $a \nmid p$, то

$$a^{p-1} \underset{p}{\equiv} 1 \quad (\cdot a)$$

$$a^p \underset{p}{\equiv} a$$

Если $a \vdots p$, то $a \underset{p}{\equiv} 0 \Rightarrow a^p \underset{p}{\equiv} 0$ ∎

Схема шифрования с открытым ключом



Зато кто угодно может его послать.

A, C, D не должны встречаться лично, чтобы обменяться ключами шифрования.

И <u>публичный ключ</u> - данные, которые всем известны, позволяют шифровать.

И <u>приватный ключ</u> - данные, которые известны только получателю, он может с их помощью расшифровать.

Rivest, Shamir, Adelman (RSA)

<u>Схема:</u> B (получатель сообщений)

- придумывает $p, q \overset{\neq}{\in} \mathbb{P}$ (на практике - очень большие числа, ≈ 1000 бит)
- $N = p \cdot q$ (≈ 2000 бит)
- $\varphi(N) = (p-1)(q-1)$
- $e \in \mathbb{N}$ - придумать, $(e, \varphi(N)) = 1$ ← должны быть взаимно просты

{ придумываем e, пока e не станет взаимно просто с $\varphi(N)$.

- вычислив d: $e \cdot d \underset{\varphi(N)}{\equiv} 1$ <u>$(d > 0)$</u>

это возможно, это деление 1 на e по модулю $\varphi(N)$, т.к e и $\varphi(N)$ взаимно просты, деление однозначно.

Публичный / Открытый ключ: (N, e)

Приватный / Закрытый ключ (N, d)

Шифрование. Алиса, имеет сообщение m - число,

$0 \le m < N$ (если $N \approx 2000$ бит, $\Rightarrow m \approx 2000$ бит)

$$E(m) = \bar{m} = m^e \bmod N$$

E - шифрование (encode)

Расшифровка. Боб:

$$D(\bar{m}) = \bar{m}^d \bmod N$$

Утв. $D(E(m)) \overset{?}{=} m$ - декодировав закодированное получим исходное.

Д-во $D(E(m))$

$$D(E(m)) = D(m^e \bmod N) =$$

$$= (m^e \bmod N)^d \bmod N \underset{N}{\equiv} (\underbrace{m^e \bmod N}_{\underset{N}{\equiv} m^e})^d \underset{N}{\equiv}$$

$$(m^e)^d \underset{N}{\equiv} m^{e \cdot d} \overset{1}{\underset{\varphi(N)}{\equiv}} m^{1 + k \cdot \varphi(N)} \underset{N}{\equiv} m \cdot \underbrace{(m^{\varphi(N)})^k}_{\underset{N}{\equiv} 1} \underset{N}{\equiv}$$

$$\underset{N}{\equiv} m \cdot 1^k \underset{N}{\equiv} m$$

Тогда $(m^e)^d \bmod N = m$, т.к. $0 \le m < N$ ■

Пример $p = 7$ $q = 11$ $N = 77$

$\varphi(N) = 6 \cdot 10 = 60.$

~~$e = 3$~~ нельзя $(3, 60) \neq 1$

$e = 13$. Подберем d.

$ed \equiv 1 \pmod{60}$ $\quad 13d \equiv 1 \pmod{60}$ – решаем. $1-13d \vdots 60 \Rightarrow \exists z$:

$1-13d = 60z \Leftrightarrow 13d + 60z = 1$

60 mod 13

(1) $60 = 13 \cdot 0 + 60 \cdot 1$

(2) $13 = 13 \cdot 1 + 60 \cdot 0$

$60 - 4 \cdot 13 =$ (3) $8 = 13(-4) + 60 \cdot 1$

(1) -4 (2)

$5 = 13 \cdot 5 + 60(-1)$

$3 = 13 \cdot (-9) + 60 \cdot 2$

$2 = 13 \cdot 14 + 60 \cdot (-3)$

$1 = 13(-23) + 60 \cdot 5$

60	13	8	5	3	2	1
0	1	-4	5	-9	14	-23
1	0	1	-1	2	-3	5

Итого: $13(-23) + 60 \cdot 5 = 1$.

(если бы было $13d - 60z = 1$, $13(-2) - 60(-5) = 1$)

т.е. $\begin{cases} d = -23 + 60k \\ z = 5 - 13k \end{cases}$ $\quad k = 1$ $\quad \boxed{d = 37}$

итого $\quad N = 77 \quad e = 13$

$\varphi(N) = 60 \quad d = 37$

Берем сообщение $m = 42$. $\quad 0 \le m < 77$

$E(m) = 42^{13=e} \bmod 77 = 14$ – быстрое возв. в степень. (калькулятор)

$D(14) = 14^{37} \bmod 77 = 42$ – узнали, что было.

Обсуждение, почему 1) не подобрать приватный ключ, 2) почему не расшифровать без него

1). $e \cdot d \equiv 1 \pmod{\varphi(N)}$ – Боб знал $\varphi(N)$, а

другие знают только N, e.

Чтобы посчитать $\varphi(N) = (p-1)(q-1)$, нужно знать p и q.
Но для задачи разложить N на множители не известно эффективного решения.

Вывод: подобрать $d \Longleftrightarrow$ разложить N на p и q

не известно эфф. алг.

2) $\overline{m} = m^e \bmod N$

$\overline{m} \equiv m^e \pmod N$

Если сообщение перехватили, то известно $\overline{m}$, $\underline{e, N}$ открытый ключ.

$m = ?$

$m = \sqrt[e]{\overline{m}} \bmod N$ - для этой задачи тоже не известно эфф. алгоритма

Найти m по $\overline{m}, e, N \Longleftrightarrow$ подобрать $d \Longleftrightarrow$ разложить N на множители

Подбор простых чисел p и q

Проблема, проверить число на простоту - нет эфф. алгоритмов. Генерировать простое - тоже нет алгоритма.

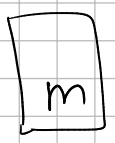
Зато есть вероятностный алгоритм проверки на простоту. Алгоритм дает p, выдается да/нет если нет, не простое, значит p - 100% действительно не простое. Если да, простое, то скорее всего действительно простое, вероятность ошибки мала.

Идея: Берем случайное a и проверяем

$a^p \underset{p}{\equiv} a$ должно быть справедливо

Схема электронной подписи

Alice
C
D



Bob → публичный ключ
→ приватный

документ

подпись $S(m) = m^d \bmod N$

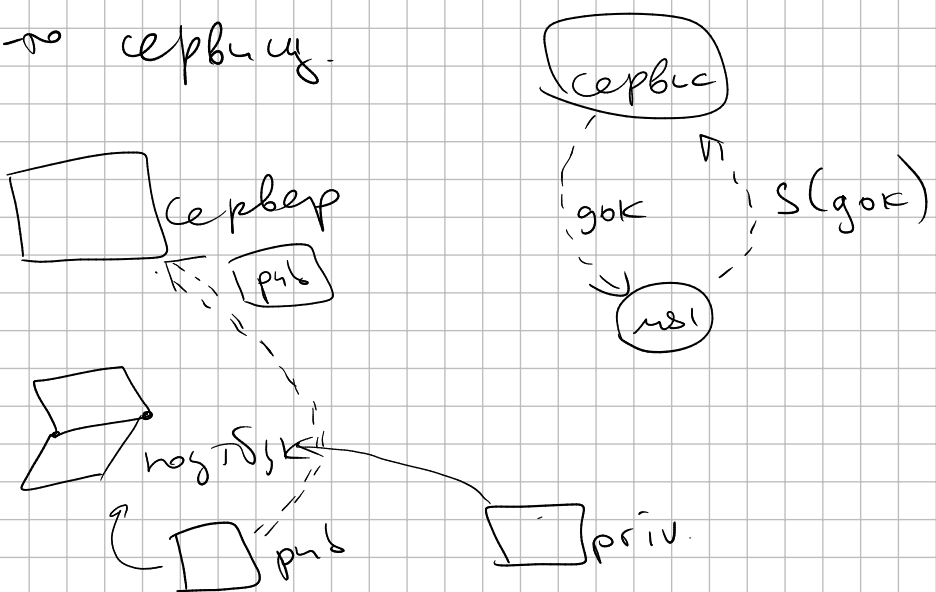
A, C, D видят m, $S(m) = \overline{m}$
и понимают, что никто кроме B не мог создать документ m с подписью $S(m)$.
Подпись можно проверить открытым ключом:

$$Check(\overline{m}) = \overline{m}^e \bmod N \overset{?}{=} m$$

Если $Check(\overline{m}) = m$, значит $\overline{m}$ - правильная подпись

$$Check(S(m)) \equiv (m^d)^e \underset{N}{\equiv} m$$

Практика: - настоящие подписи настоящих документов
- аутентификация. доказываем, что мы это мы
каким-то сервисам.



практика