

# RSA

Кевролетин В.В.

28 декабря 2011 г.

## Задание8.1

### Условие

Доказать, что  $a^{-1} \bmod m$  существует тогда и только тогда, когда  $\text{НОД}(a, m) = 1$ .

### Решение

#### Необходимость

От противного, допустим  $\text{НОД}(a, m) = d > 1$

$$a * a^{-1} = 1(\bmod m)$$

$$a * a^{-1} = q * m$$

$$a * a^{-1} = 1 + q * m$$

$$a * a^{-1} - q * m = 1$$

Левая часть делится на  $d > 1$ , тогда и правая часть должна делиться на  $d$ , но справа стоит 1. Противоречие.

#### Достаточность

Запишем линейное представление НОД:

$$\text{GCD}(a, m) = a * x + m * y$$

$$a * x + m * y = 1$$

$$a * x = 1 - m * y$$

$$a * x = 1(\bmod m)$$

т.е.  $x = a^{-1}(\bmod m)$

## Задание8.2

### Условие

Кольцо классов вычетов по  $\bmod m$  ( $Z_m$ ) является полем тогда и только тогда, когда  $m$  - простое.

### Решение

#### Необходимость

Пусть поле содержит  $m$  элементов. Тогда каждый ненулевой элемент  $x_i$  имеет обратный, т.е. (по результатам предыдущего упражнения)  $GCD(x_i, m) = 1$ . Таким образом, функция Эйлера  $\phi(m) = m - 1 \Rightarrow m$  - простое

#### Достаточность

Коммутативное и ассоциативное кольцо  $R$  с единицей называется полем, если каждый ненулевой элемент  $a \in R$  обладает обратным, то есть существует такой элемент  $a^{-1}$ , что  $a^{-1}a = aa^{-1} = 1$ .

Выполнение этого условия вытекает из результата предыдущего упражнения -  $\text{НОД}(x_i, m) = 1 \Rightarrow$  существует обратный элемент.  $\text{НОД}(x_i, m) = 1$  для любого ненулевого  $x_i$  по определению т.к.  $m$  - простое.

### Задание 8.3

#### Условие

Предположим, что найден эффективный способ решения задачи нахождения  $d$  по  $e$ . Означает ли это, что можно решать эффективно задачу факторизации (нахождения  $p$  и  $q$  по  $n$ ).

#### Решение

$$Ed = 1 \pmod{(p-1)(q-1)}$$

$$Ed - 1 = s(p-1)(q-1)$$

Возьмём произвольное целое число  $X \neq 0$ , тогда по малой теореме Ферма:

$$X^{Ed-1} = 1 \pmod{N}$$

$Ed - 1$  (т.к.  $(p-1)(q-1)$  чётно) значит можем взять квадратный корень:

$$Y_1 = X^{(Ed-1)/2} = 1 \pmod{N}$$

$$Y_1^2 = 1 \pmod{N}$$

$$Y_1^2 - 1 = k * N$$

$$(Y_1 - 1)(Y_1 + 1) = k * N$$

Посчитаем  $\text{НОД}(Y_1 - 1, N)$ ,  $\text{НОД}(Y_1 + 1, N)$  - если получили число отличное от 1 - задача решена. Если же не повезло возьмём квадратный корень еще раз  $Y_2 = X^{(Ed-1)/4}$ . И повторим процедуру. Если не повезло второй раз - выберем другое число  $X$

### Задание 8.4

#### Условие

Показать, что заданный алгоритм осуществляет возведение в степень с использованием метода последовательного возведения в квадрат.

## Решение

Рассмотрим 2-ичное разложение числа  $n$ :

$$n = m_k \cdot 2^k + m_{k-1} \cdot 2^{k-1} + \dots + m_1 \cdot 2 + m_0$$

Подставим в  $x^n$ :

$$x^n = x^{((\dots((m_k \cdot 2 + m_{k-1}) \cdot 2 + m_{k-2}) \cdot 2 + \dots) \cdot 2 + m_1) \cdot 2 + m_0} = (((\dots(((x^{m_k})^2 \cdot x^{m_{k-1}})^2 \dots)^2 \cdot x^{m_1})^2 \cdot x^{m_0})$$

Основываясь на полученном выражении, можно последовательно возводить в степень:

$$\begin{aligned} (1) & x^{m_k \cdot 2} \\ (2) & x^{m_k \cdot 2 + m_{k-1}} \\ (3) & x^{(m_k \cdot 2 + m_{k-1}) \cdot 2} \\ (4) & x^{(m_k \cdot 2 + m_{k-1}) \cdot 2 + m_{k-2}} \\ & \dots \end{aligned}$$

Запишем этот алгоритм в виде процедуры на языке программирования Перл:

```
1  sub fast_pow {
2      my ($a, $b, $m) = @_ ;
3      my $x = 1;
4      my $i = length(sprintf("%b", $b));
5      while (--$i >= 0 ) {
6          $x = ($x * $x);
7          $x = ($x * $a) if ($b >> $i) & 1;
8      }
9      $x
10 }
```

Строки 4,5 задают цикл от самого значимого бита числа  $n$  до менее значимого. В цикле выбирается соответствующая цифра двоичного разложения числа  $n$  и производится последовательное возведение в степень. Шагам 1,3 приведённого выше примера соответствует 6-я строка в коде. Шагам 2,4 - 7-я строка.

## Задание 8.5

### Условие

Исполнить WITNESS при  $a=7$ ,  $p=561$ .

### Решение

$7^{561} =$   
1258926710444010346040811055571922352586996256959051397931288  
4530107726283868706896588439519692285292566768381347082887948  
2180768646778503348838717973418979614170849967957673857542754  
2032971340819910096785140243971960661565521618577157286771524  
8415652974420284636170565645107253002715340489762118126124207

4945632975657389418376887366978217840940043289483339781564980  
5005956208316004132717850784019511788620727027104603147026941  
914248546139189929207719822537564097221755952007

## Задание8.6

### Условие

Найти количество составных натуральных чисел  $a$ , не превосходящих 561 таких, что  $a^{560} = 1 \pmod{561}$ .

### Решение

$561 = 3 \cdot 11 \cdot 17 \Rightarrow$  вместо проверки равенства  $a^{560} = 1 \pmod{561}$  можно проверить, выполняются ли одновременно

$$\begin{aligned} a^{560} &= 1 \pmod{3} \\ a^{560} &= 1 \pmod{11} \\ a^{560} &= 1 \pmod{17} \end{aligned}$$

Малая теорема Ферма: Если  $p$  — простое число, и целое  $a$  не делится на  $p$ , то  $a^{p-1} \equiv 1 \pmod{p}$ , т.е.

$$\begin{aligned} a^2 &= 1 \pmod{3} \\ a^{10} &= 1 \pmod{11} \\ a^{16} &= 1 \pmod{17} \end{aligned}$$

Тогда, т.к.  $2|560$ ,  $10|560$ ,  $16|560$ , получается, что первая система равенств выполняется для всех чисел, не кратных 3, 11 или 17. Перебором получим результат: 320

```
my $a=0;
for (1..560) { ++$a if $_%3 && $_%11 && $_%17 }
print $a
```

## Задание8.7

### Условие

Инвариант цикла в EXTENDED EUCLID.

### Решение

На каждой итерации цикла  $x$  и  $y$  получают значения такие, что

$$a \cdot x + b \cdot y = g$$

Мы нашли решение  $(x_1, y_1)$  задачи для пары  $(b \% a, a)$ , такое что

$$(b \% a) \cdot x_1 + a \cdot y_1 = g,$$

на предыдущей итерации цикла. Покажем, что решение  $(x, y)$  для нашей пары  $(a, b)$  вычисляются корректно:

$$b \% a = b - \left\lfloor \frac{b}{a} \right\rfloor \cdot a$$

Подставим это в приведённое выше выражение с  $x_1$  и  $y_1$  и получим:

$$g = (b \% a) \cdot x_1 + a \cdot y_1 =$$

$$\left( b - \left\lfloor \frac{b}{a} \right\rfloor \cdot a \right) x_1 + a \cdot y_1$$

$$g = b \cdot x_1 + a \cdot \left\lfloor \frac{b}{a} \right\rfloor \cdot x_1$$

Сравнивая это с исходным выражением над неизвестными  $x$  и  $y$ , получаем требуемые выражения:

$$\begin{cases} x = y_1 - \left\lfloor \frac{b}{a} \right\rfloor x_1 \\ x = x_1 \end{cases}$$

## Задание 8.8

### Условие

Найти  $\text{нод}(560, 1769)$  с использованием расширенного алгоритма Евклида.

### Решение

$$1 = 477 \cdot 560 + (-151) \cdot 1769$$

```
sub ext_gcd {
    my ($a, $b) = @_ ;

    if ($a == 0) {
        return ($b, 0, 1)
    }
    my ($d, $x1, $y1) = ext_gcd($b % $a, $a);
    ($d, $y1 - int($b / $a) * $x1, $x1)
}
```

```
my ($a, $b) = (560, 1769);
printf "%d = %d*$a + %d*$b", ext_gcd($a, $b);
```

## Задание 8.9

### Условие

Доказать, что если  $p$  - простое ( $> 2$ ), то  $p$  делит  $2^p - 2$ . Доказать, что составное число 341 делит  $2^{341} - 2$ .

### Решение

$$2^n - 2 = x(mod\ n)$$

$$2^n = 2 + x(mod\ n)$$

$$2^{n-1} = \frac{2+x}{2}(mod\ n)$$

Основываясь, на малой теореме Ферма(т.к. n - простое):

$$\frac{2+x}{2} = 1(mod\ n)$$

$$x/2 = 0(mod\ n)$$

$$x = 0(mod\ n)$$

ч.т.д

В уравнении  $2^{341} - 2 = x(mod\ 341)$  найдём x. Т.к.  $341 = 11*31$ , то вместо  $2^{341} = x + 2(mod\ 341)$  мы можем решать

$$2^{341} = x + 2(mod\ 11)$$

$$2^{341} = x + 2(mod\ 31)$$

По малой теореме Ферма:

$$2^{10} = 1(mod\ 11) \mid * 43$$

$$2^{340} = 1(mod\ 11) \mid * 2$$

$$2^{341} = 2(mod\ 11)$$

$$2^{341} = 0 + 2(mod\ 11)$$

Для 2го уравнения:

$$2^{30} = 1(mod\ 31) \mid * 11$$

$$2^{330} = 1(mod\ 31) \mid * 2$$

$$\text{т.к. } 2^{11} = 2048 = 2(mod\ 31)$$

$$2^{341} = 2(mod\ 31)$$

$$2^{341} = 0 + 2(mod\ 31)$$

Таким образом  $x = 0$ , т.е.  $2^{341} - 2 = 0(mod\ 341)$  ч.т.д.

### Задание8.10

#### Условие

Уравнение  $ax \equiv b \pmod m$ ,  $\text{НОД}(a, m) = d > 1$ , имеет решение тогда и только тогда, когда  $d \mid b$ . Если условие выполняется, то имеется ровно  $d$  решений по  $\pmod m$ .

### Решение

#### Необходимость

$$a * x = b(mod\ m)$$

$$a * x = b + q * m$$

$$a * x - q * m = b$$

Левая часть делится на d, правая так же должна делиться на d.

#### Достаточность

$$a * x - q * m = b|/d$$

$$a' * x - q' * m = b'|/d$$

$$a' * x = b'(mod\ m')$$

т.к. НОД(a', m') = 1  $\Rightarrow$  существует  $a'^{-1} mod\ m'$

$$x = b' * a'^{-1}(mod\ m')$$

Покажем, что таких решений будет d штук.  $m = m'd \Rightarrow x = a'^{-1}b' + m' * q, q = 0, ..., d - 1$  - разные значения по mod m

### Задание8.11

#### Условие

Решить систему  $x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5}, x \equiv 2 \pmod{7}$ .

#### Решение

$$x = 23$$

### Задание8.12

#### Условие

Шесть профессоров начинают читать лекции по своим курсам в ПН, ВТ, СР, ЧТ, ПТ, СБ и читают их далее через 2, 3, 4, 1, 6, 5 дней соответственно. Лекции не читаются по ВС (отменяются). Когда в первый раз все лекции выпадут на ВС и будут отменены.

#### Решение

Пусть x - количество прошедших дней с первого воскресенья

$$\begin{cases} x &= 0 \pmod{7} \\ x - 1 &= 0 \pmod{2} \\ x - 2 &= 0 \pmod{3} \\ x - 3 &= 0 \pmod{4} \\ x - 4 &= 0 \pmod{1} \\ x - 5 &= 0 \pmod{6} \\ x - 6 &= 0 \pmod{5} \end{cases}$$

5-е сравнение можно выбросить, т.к.  $x \neq 0$

$$\begin{cases} x = 0 & (mod\ 7) \\ x = 1 & (mod\ 2) \\ x = 2 & (mod\ 3) \\ x = 3 & (mod\ 4) \\ x = 5 & (mod\ 6) \\ x = 1 & (mod\ 5) \end{cases}$$

2е сравнение избыточно, т.к. оно включено в 4е. Аналогично 3е учтено в 6м.

$$\begin{cases} x = 0 & (mod\ 7) \\ x = 3 & (mod\ 4) \\ x = 5 & (mod\ 6) \\ x = 1 & (mod\ 5) \end{cases}$$

Рассмотрим 2е и 3е сравнения:

$$\begin{cases} x = 3 & (mod\ 4) \\ x = 5 & (mod\ 6) \end{cases}$$

$$\begin{cases} x = -1 & (mod\ 4) \\ x = -1 & (mod\ 6) \end{cases}$$

Тогда их можно заменить одним:

$$\{ x = -1 \quad (mod\ 12)$$

В итоге имеем:

$$\begin{cases} x = 0 & (mod\ 7) \\ x = 11 & (mod\ 12) \\ x = 1 & (mod\ 5) \end{cases}$$

Решим полученную систему сравнений, используя греко-китайскую теорему:

$$M_1 = 5 * 7 = 35, M_1^{-1}(mod\ 12) = 11 \quad (mod\ 12)$$

$$M_2 = 12 * 7 = 84, M_2^{-1}(mod\ 5) = 4 \quad (mod\ 5)$$

$$M_3 = 12 * 5 = 60, M_3^{-1}(mod\ 7) = 2 \quad (mod\ 7)$$

$$M = 12 * 5 * 7 = 420$$

$$x = 35 * 11 * 11 + 84 * 4 * 1 + 60 * 2 * 0 (mod\ 420) = 371 (mod\ 420)$$

Т.е. через 371 день после первого воскресенья

### Задание 8.13

#### Условие

Найти  $(678 * 973) \bmod 1813$  (с использованием греко-китайской теоремы).



### Решение

$$\begin{aligned}1813 &= 7^2 * 37, 678 = 2 * 3 * 113, 973 = 7 * 139 \\678 * 973(mod\ 1813) &= 2 * 3 * 113 * 7 * 139(mod\ 7^2 * 37) \\&= 94242(mod\ 7^2 * 37)\end{aligned}$$

Вычислим:

$$\begin{aligned}94242 &= 1 \quad (mod\ 7) \\94242 &= 11 \quad (mod\ 37)\end{aligned}$$

$$37^{-1} = 4(mod\ 7)$$

Используем формулу для решения:

$$\begin{aligned}x &= (m_2^{-1} mod\ m_1)(a_1 - a_2)m_2 + a_2 mod(m_1 * m_2) \\x &= 4 * (1 - 3) * 37 + 3 = -293 = 225(mod\ 259) \\7 * 225 &= 1575(mod\ 1813)\end{aligned}$$

Ответ:

$$678 * 973 = 1575(mod\ 1813)$$

### Задание8.14

#### Условие

Вычислить первые 20 простых чисел Мерсенна.

### Задание8.15

#### Условие

Как повлияет на работу RSA тот факт, что одно из чисел (например,  $p$ ) не является простым, а представляется в виде произведения двух простых:  $p = p_1 * p_2$ .

### Решение

Используя каноническое разложение  $n = \prod_{i=1}^k p_i^{\alpha_i}$  числа  $n$ , функция Эйлера может быть вычислена по формуле

$$\varphi(n) = \prod_{i=1}^k p_i^{\alpha_i-1} (p_i - 1)$$

Таким образом, мы можем посчитать функцию Эйлера, если в каноническом разложении  $n$  присутствуют 3 числа. В алгоритме, кроме как в вычислении функции Эйлера делители числа  $n$  участия не принимают, так что всё остаётся, как и прежде. Единственно что изменится - чем больше делителей имеет число  $n$ , тем, потенциально, проще его факторизовать, значит криптостойкость снижается.

### Задание8.16

#### Условие

Как повлияет на работу RSA тот факт, что шифруемое число не является взаимно простым, например, с  $p$ .

#### Решение

Значит шифруемое число не взаимно простое с  $N$ , а значит мы не получим взаимно однозначного отображение при шифровании (по результатам предыдущих заданий) и потом не сможем расшифровать криптотекст.

### Задание8.17

#### Условие

Сгенерировать RSA и провести шифрование/дешифрование (Mathematica, Scheme, Sage).

### Задание8.18

#### Условие

Пусть  $n(=pq)$  и  $\phi(n)$  известны, а  $p$  и  $q$  – неизвестны. Выразить  $p$  и  $q$  через  $n$  и  $\phi(n)$ . Рассмотреть случай  $n=2993$  и  $\phi(n) = 2880$ .

### Задание8.19

#### Условие

$p, q, e, d, n$  – параметры RSA. Доказать, что имеется  $r + s + rs$  неподвижных точек  $x$ ,  $1 \leq x \leq n - 1$ , где  $r = \gcd(p - 1, e - 1)$ ,  $s = \gcd(q - 1, e - 1)$ . (Из-за этого выбираются  $p$  и  $q$ , для которых  $r$  и  $s$  малы.)