Рябых Владислав, Б05-905

Алгоритмы и модели вычислений.
Домашнее задание № 12

Задача 1. В протоколе RSA выбраны $p = 17$, $q = 23$, $N = 391$, $e = 3$. Выберите ключ d и зашифруйте сообщение 41. Затем расшифруйте полученное сообщение и убедитесь, что получится исходное 41.

Решение. Зашифрованное сообщение: $y = m^e \mod N = 41^3 \mod 391 = 68921 \mod 391 = 105$
Для того, чтобы расшифровать сообщение, сначала необходимо вычислить значение d:
$d = e^{-1} \mod (p-1)(q-1) = 3^{-1} \mod 352 = 235$, так как $3 \cdot 235 = 705 \underset{352}{\equiv} 1$
Теперь расшифровываем: $y^d \mod N = 105^{235} \mod 391$
Долго думал, как посчитать остаток сразу по модулю 391, но ни одна идея сильно подсчёт не облегчает, так что посчитаем остаток по модулям $p = 17$ и $q = 23$, а потом воспользуемся КТО.

- $105^{235} = (105^{16})^{14} \cdot 105^{11} \overset{\text{по МТФ}}{\underset{17}{\equiv}} 1 \cdot 105^{11} \underset{17}{\equiv} 3^{11} = 27^3 \cdot 9 \underset{17}{\equiv} 10^3 \cdot 9 \underset{17}{\equiv} -3 \cdot 9 \underset{17}{\equiv} 7$
- $105^{235} = (105^{22})^{10} \cdot 105^{15} \overset{\text{по МТФ}}{\underset{23}{\equiv}} 1 \cdot 105^{15} \underset{23}{\equiv} 13^{15} = 169^7 \cdot 13 \underset{23}{\equiv} 8^7 \cdot 13 = 2^{22} \cdot 2^{-1} \cdot 13 \overset{\text{по МТФ}}{\underset{23}{\equiv}}$ $\overset{\text{по МТФ}}{\underset{23}{\equiv}} 2^{-1} \cdot 13 = 12 \cdot 13 \underset{23}{\equiv} 18$

  Воспользуемся КТО: $\begin{cases} x \underset{17}{\equiv} 7 \\ x \underset{23}{\equiv} 18 \end{cases}$

Сначала найдём обратные элементы:

- по модулю 17: $23^{-1} = 6^{-1} = 3$, так как $6 \cdot 3 = 18 \underset{17}{\equiv} 1$
- по модулю 23: $17^{-1} = 19$, так как $17 \cdot 19 = 323 \underset{23}{\equiv} 1$

Тогда $x \underset{391}{\equiv} 7 \cdot 3 \cdot 23 + 18 \cdot 19 \cdot 17 = 483 + 5814 = 6297 \underset{391}{\equiv} 41$
Таким образом $y^d \mod N = 105^{235} \mod 391 = 41$ — сообщение успешно расшифровано

Задача 2. Пусть в протоколе RSA открытый ключ (N, e), $e = 3$. Покажите, что если злоумышленник узнаёт закрытый ключ d, то он может легко найти разложение N на множители.

Решение. Так как $d = e^{-1} \mod (p-1)(q-1)$, то $d \cdot e \underset{(p-1)(q-1)}{\equiv} 1 \Rightarrow d \cdot e - 1 = k \cdot (p-1)(q-1), k \in \mathbb{Z}$
$e = 3$ по условию, так что $3d - 1 = k \cdot (p-1)(q-1), k \in \mathbb{Z}$.
$k \cdot (p-1)(q-1) \underset{3}{\equiv} 2; (p-1) \underset{3}{\equiv} 2 (q-1) \underset{3}{\equiv} 1 \Rightarrow k \underset{3}{\equiv} 2$
$d = e^{-1} \mod (p-1)(q-1) \Rightarrow d < (p-1)(q-1) \Rightarrow k = 2$ — единственный вариант.
Таким образом $3d - 1 = 2 \cdot (p-1)(q-1) = 2 \cdot (pq - p - q + 1)$
$p = -q + N + \dfrac{3}{2}(1-d)$
$N = pq \Rightarrow N = -q^2 + Nq + \dfrac{3}{2}(1-d)q$, откуда находим $q \Rightarrow$ находим p.

***Задача* 3.** Схема RSA позволяет также создавать защищенные электронные подписи. Если открытый ключ (N, e), то автор сообщения, обладающий закрытым ключом d, отправляет сообщение A^d, где A — незашифрованное сообщение. После этого идентификация подписи - это возведение в степень e. Пусть открытый ключ $(2021, 25)$. В какую степень автору нужно возвести сообщение, чтобы отправить его за своей электронной подписью?

***Решение*.** $N = 2021 = 43 \cdot 47 = p \cdot q$.
Тогда степень, в которую автору нужно возвести сообщение, есть $d = e^{-1} \mod (p-1)(q-1) = 25^{-1} \mod 42 \cdot 46 = 25^{-1} \mod 1932$.
$25 \cdot d \underset{1932}{\equiv} 1 \Rightarrow 25d + 1932k = 1$, где $d, k \in \mathbb{Z}$ — диофантово уравнение, которое мы решим с помощью расширенного алгоритма Евклида (учтём, что $(25, 1932) = 1$, так что решение в целых числах существует).

d	1	0	-77	232	-1391
k	0	1	1	-3	18
$25d + 1932k$	25	1932	7	4	1

Таким образом, $d = -1391 + 1932m, m \in \mathbb{Z}$. Тогда берём $d = -1391 + 1932 \cdot 1 = 541$
Это и есть искомая степень.

***Задача* 4.** Решите уравнение $\varphi(n) = 6$, где $\varphi(n)$ — функция Эйлера (количество чисел, не превосходящих n и взаимно простых с ним).

***Решение*.** Сразу заметим, что $n \geqslant 7$, причём $n = 7$ подходит, так как 7 — простое число, а для простых чисел справедливо $\varphi(p) = p - 1$.

$$2 \cdot 3 = 6 = \varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_m}\right)$$

Отсюда можно сказать, что простых делителей в разложении числа n не больше двух.
Допустим, что простой делитель только один. Тогда $n = p_1^k \Rightarrow 2 \cdot 3 = \varphi(n) = p_1^{k-1} \cdot (p_1 - 1) \Rightarrow p_1 = 7, k = 1$ и $p_1 = 3, k = 2$ — единственно возможные варианты. То есть ещё добавляем к множеству решений $n = 9$.
Смотрим теперь ситуацию, когда простых делителей два:

$$2 \cdot 3 = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) = n \cdot \frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} = p_1^{k_1 - 1} \cdot p_2^{k_2 - 1} \cdot (p_1 - 1) \cdot (p_2 - 1)$$

Таким образом, чтобы в правой части было 2 делителя есть всего 2 возможных случая:

- $k_1 = k_2 = 1 \Rightarrow 2 \cdot 3 = (p_1 - 1) \cdot (p_2 - 1)$. Существует всего 2 варианта: $2 \cdot 3$ и $1 \cdot 6$. Первый даёт нам ничего не даёт, так как $p_2 = 3 + 1 = 4$ на самом деле не является простым, а второй даёт $n = 2 \cdot 7 = 14$.

- $p_1 = 2$. Тогда $2 \cdot 3 = 2^{k_1 - 1} \cdot p_2^{k_2 - 1} \cdot (p_2 - 1)$. Сразу заметим, что $1 \leqslant k_1 \leqslant 2$. Опять делим на 2 случая:

  - $k_1 = 1 \Rightarrow 2 \cdot 3 = p_2^{k_2 - 1} \cdot (p_2 - 1) \Rightarrow k_2 = 2 \Rightarrow 2 \cdot 3 = p_2 \cdot (p_2 - 1) \Rightarrow p_2 = 3$. То есть добавляем к множеству решений $n = 2 \cdot 3^2 = 18$.

– $k_2 = 2 \Rightarrow 2 \cdot 3 = 2 \cdot p_2^{k_2-1} \cdot (p_2 - 1) \Rightarrow k_2 = 1 \Rightarrow p_2 - 1 = 3$ — отбрасываем этот вариант, так как $p_2 = 3 + 1 = 4$ на самом деле не является простым.

Таким образом, все решения уравнения $\varphi(n) = 6$ — множество $\{7, 9, 14, 18\}$.

Задача 5. Докажите, что в шифре Шамира в итоге у B в действительности оказывается то сообщение, которое A планировал передать.

Решение. По условиям шифра мы знаем, что $c_a d_a \underset{p-1}{\equiv} c_b d_b \underset{p-1}{\equiv} 1$.
Тогда $c_a d_a = u \cdot (p-1) + 1 = r + 1$, $c_b d_b = v \cdot (p-1) + 1 = s + 1$, где $u, v \in \mathbb{Z}$. Заметим также, что $r = u \cdot (p-1)$ и $s = v \cdot (p-1)$ делятся на $p - 1$
B считает $x_4 = x_3^{d_b} = x_2^{d_a d_b} = x_1^{c_b d_a d_b} = m^{c_a c_b d_a d_b} = m^{(c_a d_a) \cdot (c_b d_b)} = m^{(r+1) \cdot (s+1)} = m^{rs+r+s+1} = m \cdot m^{rs+r+s} \overset{\text{по МТФ}}{\underset{p}{\equiv}} m \cdot 1 = m$, то есть $x_4 \underset{p}{\equiv} m$, что и требовалось доказать.

Задача 6. Докажите, что в шифре Эль-Гамаля в итоге у B в действительности оказывается то сообщение, которое A планировал передать.

Решение. B считает $e \cdot r^{p-1-c_b} \mod p$, где $r = g^k \mod p; e = m \cdot d_b^k \mod p; d_b = g^{c_b} \mod p$.
Таким образом B считает $m \cdot d_b^k \cdot (g^k)^{p-1-c_b} = m \cdot g^{kc_b} \cdot g^{kp-k-kc_b} = m \cdot g^{k(p-1)} \overset{\text{по МТФ}}{\underset{p}{\equiv}} m \cdot 1 = m$, что и требовалось доказать.

Задача 7. Докажите, что в алгоритме шифрования Рабина B в итоге сможет найти исходное передаваемое сообщение среди $(\pm apm_q \pm bqm_p)$.

Решение. A передаёт $y = m^2 \mod pq$
B вычисляет $ap + bq \underset{pq}{\equiv} 1$, а также $m_p = y^{\frac{p+1}{2}}, m_q = y^{\frac{q+1}{2}}$
$m_p = m^{\frac{p+1}{2}} = m \cdot \left(\dfrac{m}{p}\right); m_q = m^{\frac{q+1}{2}} = m \cdot \left(\dfrac{m}{q}\right)$, так как $p, q \underset{4}{\equiv} 3$ по условию алгоритма.
Таким образом $\pm apm_q \pm bqm_p = \pm apm \cdot \left(\dfrac{m}{q}\right) \pm bqm \cdot \left(\dfrac{m}{p}\right) = \pm apm \pm bqm = m(\pm ap \pm bq)$
И тогда существует комбинация из знаков, такая что B в итоге получает $m \cdot (ap + bq) \underset{pq}{\equiv} m \cdot 1 = m$, что и требовалось доказать.