Домашнее задание на десятую неделю

Бельденова Камила, 675

18 апреля 2017

1	2	3	6	Σ

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.

$N = p \cdot q = 17 \cdot 23, e = 3$
$gcd(e,(p-1)(q-1)) = gcd(3, 16 \cdot 22) = \underline{1}$
Euclid:

$$\begin{array}{cc} 16 \cdot 22 & 3 \\ 1 & 3 \\ \underline{1} & 0 \end{array}$$

Extended Euclid:
$1 = 16 \cdot 22 + \mathbf{(-117)} \cdot 3$

$d = e^{-1} \pmod{16 \cdot 22}$
$3d = 1 \pmod{16 \cdot 22}$
$\mathbf{-177} = 3^{-1} \equiv 235 \pmod{16 \cdot 22}$
Шифровка: $\boxed{y = x^e \pmod N} = 41^3 \equiv 105 \pmod{391}$
Дешифровка: $\boxed{x = y^d \pmod N} = 105^{235} = 41 \pmod{16 \cdot 22}$

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.

Т. к. (N,e), $e = 3$ — ключ открытый (передаётся по незащищенному каналу), то можем сказать, что злоумышленник его знает. Пусть он узнал и d, посмотрим, что это даст ему при попытке расшифровки сообщения.
$\boxed{d = e^{-1} \pmod{(p-1)(q-1)}} \Rightarrow d \cdot e = (p-1)(q-1) \cdot y + 1$
$3d = (p-1)(q-1) \cdot y + 1$

$$\begin{cases} d = e^{-1} & (\mathrm{mod}\ 16 \cdot 22) \\ e = d^{-1} & (\mathrm{mod}\ 16 \cdot 22) \end{cases}$$

$\Rightarrow$ d — остаток по модулю $(p-1)(q-1) \Rightarrow d < (p-1)(q-1)$
$3d < 3(p-1)(q-1) \Rightarrow 3d < 3(p-1)(q-1) + 1 \Rightarrow$ равенство может выполниться при $y < 3$, т. е., учитывая, что $y \in \mathbb{Z}$, y равен либо 1, либо 2.

(a) Пусть $y = 1$, тогда:
$3d - 1 = (p-1)(q-1)$
d известно $\Rightarrow$ решив систему:

$$\begin{cases} p \cdot q = N \\ (p-1)(q-1) = 3d - 1 \end{cases} \tag{1}$$

найдем p и q.
Обозначим за $M = 3d - 1$

$$\begin{cases} p = \dfrac{N}{q} \\ \left(\dfrac{N}{q} - 1\right)(q-1) = M \end{cases} \Rightarrow \begin{cases} p = \dfrac{N}{q} \\ q^2 + q(M - N - 1) + N = 0 \end{cases} \Rightarrow \begin{cases} p = \dfrac{N}{q} \\ q_{1/2} = \dfrac{-M + N + 1 \pm \sqrt{(M-N-1)^2 - 4Nq^2}}{2} \end{cases}$$

(b) Пусть $y = 2$, тогда:

$$\begin{cases} p \cdot q = N \\ (p-1)(q-1) = \frac{M}{2} \end{cases} \tag{2}$$

Система 2 имеет решение, аналогичное решению системы 1

Ответ: зная d, злоумышленник может найти разложение N на простые множители.

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?

$$\boxed{x = y^d \pmod N}$$

$N = 2021 = 43 \cdot 47$
$e = 25$
$d = e^{-1} \pmod{42 \cdot 46}$
$d = 25^{-1} \pmod{42 \cdot 46}$
$25d = 1 \pmod{42 \cdot 46}$ Euclid:

$42 \cdot 46$	25
7	25
7	4
3	4
3	1
0	1

Extended Euclid: $1 = 4 - 3 = 2 \cdot 4 - 7 = 2 \cdot (25 - 3 \cdot 7) - 7 = 2 \cdot 25 - 7 \cdot 7 = 2 \cdot 25 - 7 \cdot (42 \cdot 46 - 77 \cdot 25) = \underline{541} \cdot 25 - 7 \cdot 42 \cdot 46$
$d = 541$
Ответ: сообщение нужно возвести в 541 степень.

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

$$\boxed{\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)}$$

Пусть d — результат деления n на произведение всех простых делителей числа n, тогда:

$$\boxed{\varphi(n) = d\prod_{p|n}(p-1)}$$

Т.к. $\varphi(n) \in \mathbb{Z}$, то $d \in \mathbb{N} \Rightarrow d$ есть делитель 6.
Теперь рассмотрим всевозможные делители 6.

(a) $d = 1$
Тогда $(p_i - 1)$, где p_i — простые делители числа n, могут быть равны:

i. $p_1 - 1 = 1, p_2 - 1 = 2, p_3 - 1 = 3 \Rightarrow p_1 = 2, p_2 = 3, p_3 = 4$, но 4 не есть простое число $\Rightarrow$ этот вариант не подходит;

ii. $p_1 - 1 = 2, p_2 - 1 = 3 \Rightarrow p_1 = 3, p_2 = 4$, не подходит аналогично предыдущему пункту;

iii. $p_1 - 1 = 1, p_2 - 1 = 6 \Rightarrow p_1 = 2, p_2 = 7 \Rightarrow \boxed{n_1 = d \cdot p_1 \cdot p_2 = 14}$;

iv. $p - 1 = 6 \Rightarrow p = 7 \Rightarrow \boxed{n_2 = 7}$.

(b) $d = 2$

i. $p_1 - 1 = 1, p_2 - 1 = 3 \Rightarrow p_1 = 2, p_2 = 4$, не подходит, т. к. 4 — не простое число;

ii. $p - 1 = 3 \Rightarrow p = 4$, не подходит аналогично предыдущему пункту.

(c) $d = 3$

i. $p_1 - 1 = 1, p_2 - 1 = 2 \Rightarrow p_1 = 2, p_2 = 3 \Rightarrow \boxed{n_3 = 18}$;

ii. $p - 1 = 2 \Rightarrow p = 3 \Rightarrow \boxed{n_4 = 9}$.

(d) $d = 6$, тогда:

i. $p-1 = 1 \Rightarrow p = 2$, т. е. при делении n на 2 мы получили $6 \Rightarrow n$ изначально было кратно 3, следовательно одним из простых делителей должен быть $p = 3$, но мы его не получили $\Rightarrow$ противоречие;

ii. Допустим, простых делителей нет. $d = 6 \Rightarrow n \vdots 2, n \vdots 3$, значит среди простых делителей должны быть числа 2 и 3, но мы их не получили $\Rightarrow$ противоречие.

Ответ: $n \in \{7; 9; 14; 18\}$.