Домашняя работа №10

Бредихин Александр

18 мая 2020 г.

Задача 1

Задача: 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.

Передаём сообщение $m = 41$ (не надо разбивать на блоки). Найдём закрытый ключ: по алгоритму RSA: $d = e^{-1} \mod (p-1)(q-1)$. Находим обратный элемент с помощью алгоритма Евклида, как в предыдущем семинаре: $d = 3^{-1} \mod 352 = 235$.

Отправка сообщения: $y = m^e \mod N = 41^3 \mod 391 = 105$ (считаем с помощью КТО аналогично прошлому семинару задаче 3).

К получателю приходит зашифрованное сообщение y. Он знает закрытый ключ d. Для расшифровки делает следующее: $y^d \mod N = 105^{235} \mod 391 = 41$. Получили то сообщение, которое было зашифровано, что и требовалось показать.

Задача 2

Задача: 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.

По определению: $d = e^{-1} \mod (p-1)(q-1)$, следовательно, $de = 1 \mod (p-1)(q-1)$. Решаем диофантово уравнение $de + 1 \cdot (p-1)(q-1) = 1$ относительно e и $(p-1)(q-1)$. Находим $(p-1)(q-1)$ (за полиномиальное время). Делаем следующее:

$$de = 1 \mod (p-1)(q-1)$$
$$de + (p-1)(q-1) = 1 \mod (p-1)(q-1)$$
$$de + N - p - q = 0 \mod (p-1)(q-1)$$

Так как мы знаем $(p-1)(q-1)$, d, e, то из этого сравнения мы сможем найти $p+q = E$. Также мы знаем, что $pq = N$ (значение открытого ключа мы тоже знаем). Получается p, q - корни квадратного уравнения с коэффициентам $a = 1$, $b = -E$, $c = N$. Его решение мы находим за полиномиальное время (решение через дискриминант). Поэтому за полиномиальное время, мы можем получить разложение N на множители.

Задача 3

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

Поэтапно пройдём по действиям алгоритма шифрования и убедимся в этом (использую обозначения, как в семинаре):

1) А → Б: $M^{c_A} \mod p$

2) Б → А: $(M^{c_A})^{c_B} \mod p$.
Для следующего пункта учитываем, что $c_A d_A = 1 \mod p-1 \Rightarrow c_A d_A = 1 + n(p-1)$, где n- натуральное число.

3) А → Б: $(M^{c_A c_B})^{d_A} = M^{c_B(1+n(p-1))} = M^{c_B} \cdot M^{n(p-1))c_B} \Rightarrow$ по Малой теореме Ферма $M^{p-1} = 1 \mod p \Rightarrow (M^{c_A c_B})^{d_A} = M^{c_B} (M^{n c_B})^{p-1} \mod p = M^{c_B} \mod p$

4) Б: $(M^{c_B})^{d_B} \mod p$. Так как по Малой теореме Ферма $M^{p-1} = 1 \mod p$, то показатель можно брать по модулю $p-1$, учитывая, что $c_B d_B = 1 \mod p-1$ (по алгоритму шифрования), получаем: $(M^{c_B})^{d_B} \mod p = M \mod p$. Получили то сообщение, которое и было зашифровано, что и требовалось показать.

Задача 4

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

Используем все те же обозначения, что и в семинаре.
Из семинара получаем $m' = ed_A^{p-1-c_B}$. Покажем, что полученное сообщение совпадает с отправленным.
Так как по малой теореме Ферма $d_A^{p-1} = 1 \mod p$ и из алгоритма шифрования $e = md_B^{c_A}$, получаем, что $m' = md_B^{c_A}\left(d_A^{c_B}\right)^{-1} \mod p$.

Из алгоритма шифрования следует:
$\left(d_A^{c_B}\right)^{-1} \mod p = \left(g^{c_A c_B}\right)^{-1} \mod p$
$d_B^{c_A} \mod p = g^{c_B c_A} \mod p$

В итоге получаем:

$$m' = md_B^{c_A}\left(d_A^{c_B}\right)^{-1} \mod p = mg^{c_B c_A}\left(g^{c_A c_B}\right)^{-1} \mod p = m$$

Получили зашифрованное сообщение, что и требовалось показать.

Задача 5

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

Используем все обозначения, как в семинаре.
Применяем КТО к зашифрованному сообщению: $M = pq$, $m_1 = p$, $m_2 = q$. Обозначим, что $m^2 = x_1 \mod p$, $m^2 = x_2 \mod q$, тогда

$$y = m^2 = x_1 q \left(q^{-1} \mod p\right) + x_2 p \left(p^{-1} \mod q\right) \mod pq$$

Заметим, что обратные элементы к q по модулю p и к p по модулю q, находятся из решения диофантового уравнения: $ap + bq = 1$. В итоге получаем такое сравнение:

$$y = m^2 = x_1 qb + x_2 pa \mod pq$$

Для нахождения ответа нам нужно извлечь корень из полученного выражения. Заметим, что число pq – число Блюма (по определению) для него $x = y^{\frac{p+1}{4}} \mod p, q$ - корень из k по модулю p, q (так как $y^{\frac{p+1}{2}} = 1 \mod p, q$). Также (аналогично) $-y^{\frac{p+1}{4}} \mod p, q$ – тоже корень. Поэтому мы получаем 4 разных варианта $\pm apy^{\frac{q+1}{4}} \pm bqy^{\frac{p+1}{4}} \mod pq$. По принципу кодирования, один из этих решений и будет являться первоначальным сообщением.

Задача 6

Задача: Докажите формулу обращения: $(M_n(\omega))^{-1} = \dfrac{1}{n}M_n(\omega^{-1})$. Вычислите также матрицу $(M_n(\omega))^4$.

Для доказательства утверждения и для нахождения $(M_n(\omega))^4$ докажем такую лемму «о суммировании»:

Формулировка: для любого целого $n \geqslant 1$ и ненулевого k не кратного n выполнено:

$$\sum_{j=0}^{n-1} \left(\omega_n^k\right)^j = 0$$

Доказательство: используя формулу геометрической прогрессии, получаем:

$$\sum_{j=0}^{n-1} \left(\omega_n^k\right)^j = \frac{\left(\omega_n^k\right)^n - 1}{\omega_n^k - 1} = \frac{\left(\omega_n^n\right)^k - 1}{\omega_n^k - 1} = \frac{(1)^k - 1}{\omega_n^k - 1} = 0$$

Так как k не делит n, то знаменатель в ходе доказательства не равен 0 ($\omega_n^k = 1$ тогда и только тогда, когда k делится на n).

Для доказательства, что $(M_n(\omega))^{-1} = \dfrac{1}{n}M_n(\omega^{-1})$, покажем, что $M_n^{-1} \cdot M_n = E$ (единичной матрице). Рассмотрим (j, j') элемент матрицы $M_n^{-1} \cdot M_n$

$$\left[M_n^{-1}M_n\right]_{jj\prime} = \sum_{k=0}^{n-1} \left(\omega_n^{-kj}/n\right)\left(\omega_n^{kj\prime}\right) = \sum_{k=0}^{n-1} \omega_n^{k(j'-j)}/n$$

Согласно доказанной ранее лемме, полученная сумма равна 1, если $j' = j$ и 0 иначе. Так как $-(n-1) \leq j' - j \leq n-1, j' - j$, то условие леммы выполняется и k не делит n. Получили единичную матрицу, следовательно, $(M_n(\omega))^{-1} = \dfrac{1}{n}M_n(\omega^{-1})$

Найдём $(M_n(\omega))^4$.

Возьмём iую строчку (индексируем с нуля для удобства). iая строчка состоит из таких элементов:
$1 \quad w^i \quad w^{2i} \dots \quad w^{i(n-1)}$
Аналогично рассматриваем j столбец:
$1 \quad w^j \quad w^{2j} \dots \quad w^{j(n-1)}$

При возведении матрицы в квадрат: при перемножении iой строчки и jго столбца получаем элемент:
$1 + w^{i+j} + w^{2(i+j)} + \ldots + \quad w^{(i+j)(n-1)}$
По лемме о суммировании он равен 0 если $i+j \neq n+1$, если $i+j = n+1$, то получаем сумму из n единиц. Получается, что при возведении такой матрицы в квадрат получим такую матрицу:

$$\begin{pmatrix} n & 0 & 0 & & 0 \\ 0 & 0 & 0 & & n \\ & & & & \\ 0 & 0 & n & & 0 \\ 0 & n & 0 & & 0 \end{pmatrix} \tag{1}$$

При перемножении двух таких матриц получаем диагональную с n^2 в диагонале (перемножаем по определению замечаем закономерность).

Ответ: диагональная с n^2 в диагонале.