Федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет аэрокосмического приборостроения»

КАФЕДРА № 51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

| ст. преп. | | А.М. Буланов |
|---|---|---|
| должность, уч. степень, звание | подпись, дата | инициалы, фамилия |

# Контрольная работа № 3

по курсу: **Криптографические методы защиты информации**

РАБОТУ ВЫПОЛНИЛА

| СТУДЕНТ ГР. № 5721 | | А.Е. Ковалева |
|---|---|---|
| | подпись, дата | инициалы, фамилия |

Санкт-Петербург 2020

Ковалева 5721
вариант 35.

№1.

1) $\varphi(53)$. , 53 - число, взаимнопростое со всеми числами, кроме себя и 1 =>

$\varphi(53) = 53^1 - 53^{1-1} = 53^1 - 53^0 = 53 - 1 = 52$.

2) $\varphi(43^2)$, число 43 - аналогично числу 53 (пункт 1) =>

$\varphi(43) = 43^2 - 43^{2-1} = 43^2 - 43^1 = 1806$.

(ф-ла Эйлера: $\varphi(p^n) = p^n - p^{n-1}$, где p - простое число)

3) $\varphi(97 \cdot 79) = (97^1 - 97^{1-1}) \cdot (79^1 - 79^{1-1}) = (97-1)(79-1) = 96 \cdot 78 = 7488$

№2.

Вычислим $22^{4513} \bmod 83$

Имеем $a = 22$, $m = 83$, $X = 4513$

$X = 4513_{10} = 0001.0001.1010.0001_2$; $n = 15$

В общем случае $a_j = a^{2^j} \bmod m$, $j = \overline{0, n-1}$

Вычислим $a_j$. Все действия вычисляются по модулю 83. Запись $(\bmod 83)$ опускаем.

0. $a_0 = 22$
1. $a_1 = 22^1 = 69$
2. $a_2 = 69^2 = 30$
3. $a_3 = 30^2 = 70$
4. $a_4 = 70^2 = 3$
5. $a_5 = 3^2 = 9$
6. $a_6 = 9^2 = 81$
7. $a_7 = 81^2 = 4$
8. $a_8 = 4^2 = 16$
9. $a_9 = 16^2 = 7$
10. $a_{10} = 7^2 = 49$
11. $a_{11} = 49^2 = 77$
12. $a_{12} = 77^2 = 36$
13. $a_{13} = 36^2 = 51$
14. $a_{14} = 51^2 = 28$
15. $a_{15} = 28^2 = 37$

Запишем вычисления в таблицу.

| j | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $x_j$ | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| $a_j$ | 22 | 69 | 30 | 70 | 3 | 9 | 81 | 4 | 16 | 7 | 49 | 77 | 36 | 51 | 28 | 37 |

$\Rightarrow 22^{4513} = 22 \cdot 9 \cdot 4 \cdot 16 \cdot 36 = 456192 \pmod{83} = 24$

Ответ: 24

№3.

$2^{-1} \bmod 23$ , 23 - прост. число $\Rightarrow \varphi(23) = 22$

$2^{\varphi(23)-1} \bmod 23 = 2^{22-1} \bmod 23 = 2^{21} \bmod 23 = 2^5 \cdot 2^5 \cdot 2^5 \cdot 2^5 \cdot 2 =$

$= 32 \cdot 32 \cdot 32 \cdot 32 \cdot 2 \pmod{23} = 9 \cdot 9 \cdot 9 \cdot 9 \cdot 2 \pmod{23} = 81 \cdot 81 \cdot 2 =$

$= 12 \cdot 2 \cdot 12 \pmod{23} = 12 \cdot 24 \pmod{23} = 12 \bmod 23$

проверка: $2 \cdot 12 \bmod 23 = 1 \Rightarrow$ верно

№4.

$14^9 \bmod 29$

$9_{10}' = 1001_2$ ; $a = 14$, $m = 29$, $X = 9$, $n = 3$

$a_0 = 14^1 \bmod 29 = 22$ ; $a_1 = 22^2 \bmod 29 = 20$;
$a_2 = 20^2 \bmod 29 = 23$ ; $a_3 = 23^2 \bmod 29 = 7$

| j: | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $x_j$ | 1 | 0 | 0 | 1 |
| $n_j$ | 22 | 20 | 23 | 7 |

$14^9 = 22 \cdot 7 = 154 \pmod{29} = 9$

№5.

сообщ: 47253

откр-ключ: $b_i$ = [3078, 12172, 8208, 8348, 12662, 4128, 3709, 4923, 6325, 14119]

множитель: 12615, модуль: 16649.

$r = 12615$, $q = 16649$

$\begin{cases} r_{-1} = 16649 \\ x_{-1} = 0 \\ y_{-1} = 1 \end{cases}$ $\begin{cases} r_0 = 12615 \\ x_0 = 1 \\ y_0 = 0 \end{cases}$ $\begin{cases} r_1 = 16649 - 1 \cdot 12615 = 4034 \\ x_1 = 0 - 1 \cdot 1 = -1 \\ y_1 = 1 - 1 \cdot 0 = 1 \end{cases}$

$\begin{cases} r_2 = 12615 - 3 \cdot 4034 = 513 \\ x_2 = 1 - 3 \cdot (-1) = 1 + 3 = 4 \\ y_2 = 0 - 3 \cdot 1 = -3 \end{cases}$ $\begin{cases} r_3 = 4034 - 7 \cdot 513 = 443 \\ x_3 = -1 - 7 \cdot 4 = -29 \\ y_3 = +1 - 7(-3) = 22 \end{cases}$

$\begin{cases} r_4 = 513 - 1 \cdot 443 = 70 \\ x_4 = 4 - 1 \cdot (-29) = 33 \\ y_4 = -3 - 22 = -25 \end{cases}$ $\begin{cases} r_5 = 443 - 6 \cdot 70 = 23 \\ x_5 = -29 - 6 \cdot 33 = -227 \\ y_5 = 22 - 6 \cdot (-25) = 172 \end{cases}$ $\begin{cases} r_6 = 70 - 3 \cdot 23 = 1 \\ x_6 = 33 - 3 \cdot (-227) = 714 \\ y_6 = -25 - 3 \cdot 172 = 541 \end{cases}$

$16649 \cdot 541 + 714 \cdot 12615 = 1$

$r \cdot r^{-1} \equiv 1 \mod q \Rightarrow r^{-1} = 714$

$B_i = r \cdot w_i \mod q \Rightarrow w_i = b_i \cdot r^{-1} \mod q$

$w_1 = 3078 \cdot 714 \pmod{16649} = 24$
$w_2 = 12172 \cdot 714 \ (-\text{''}-) = 30$
$w_3 = 8208 \cdot 714 \ (-\text{''}-) = 64$
$w_4 = 8348 \cdot 714 \ (-\text{''}-) = 130$
$w_5 = 12662 \cdot 714 \ (-\text{''}-) = 261$
$w_6 = 4128 \cdot 714 \ (-\text{''}-) = 512$
$w_7 = 3709 \cdot 714 \ (-\text{''}-) = 1035$
$w_8 = 4223 \cdot 714 \ (-\text{''}-) = 2083$
$w_9 = 6325 \cdot 714 \ (-\text{''}-) = 4171$
$w_{10} = 14119 \cdot 714 \pmod{16649} = 8321$

| | |
|---|---|
| 1 | $0111011101_2 =$ |
| 0 | $= 477_{10}$ |
| 1 | |
| 1 | Ответ: |
| 1 | 477,0 |
| 0 | |
| 1 | |
| 1 | |
| 1 | |
| 0 | |

$s' = s \cdot r \mod q \Rightarrow s' = 47253 \cdot 714 \mod 16649 = 7768$

$7768 - 4171 = 3597 - 2083 = 1514 - 1035 = 479 - 261 = 218 - 130 = 88 - 64 = 24 - 24 = 0$