(23) ЛЫГАНЕНКО ЕЛИЗАВЕТА
419 группа

Протокол Хейса - Переклена.

$p=167,\ q=83$

$N=9,\ g=2,\ h=-15,\ x_1=18,\ x_2=13,\ x_3=69$

$x_4=54,\ M=61.$

1) $g=2,\ h=-15,\ p=167$

$\left(\frac{2}{167}\right)=(-1)^{\frac{167^2-1}{8}}=(-1)$

$\left(\frac{h}{p}\right)=\left(\frac{3}{167}\right)\left(\frac{5}{167}\right)\left(-\frac{1}{167}\right)=(-1)$

$\left(\frac{3}{167}\right)=\left(\frac{167}{3}\right)(-1)^{\frac{167-1}{2}\cdot\frac{3-1}{2}}=\left(\frac{2}{3}\right)(-1)=(-1)(-1)^{\frac{9-1}{8}}=1.$

$\left(\frac{5}{167}\right)=\left(\frac{167}{5}\right)(-1)^{\frac{167-1}{2}\cdot\frac{5-1}{2}}=\left(\frac{2}{5}\right)=(-1)^{\frac{5-1}{2}}=1.$

$\left(\frac{-1}{167}\right)=-1$

2) $x=(x_1,x_2,x_3,x_4)=(18,13,69,54)$

$y_1=g^{x_1}\cdot h^{x_2}\pmod p=2^{18}(-15)^{13}\pmod{167}=21.$

$y_2=g^{x_3}\cdot h^{x_4}\pmod p=2^{69}(-15)^{54}\pmod{167}=48$

$y=(y_1,y_2)=(21,48)$

$s_1=x_1+Mx_3\pmod q=18+61\cdot 69\pmod{83}=77$

$s_2=x_2+Mx_4\pmod q=13+61\cdot 54\pmod{83}=70$

$s(M,x)=(s_1,s_2)=(77,70)$

3) $y_1y_2^M\overset{?}{=}g^{s_1}h^{s_2}\pmod p$

$\left.\begin{array}{l}21\cdot 48^{61}\pmod{167}=36\\ 2^{77}\cdot(-15)^{70}\pmod{167}=36\end{array}\right\}\Rightarrow$ верно.

Упражнение 5.58 $a^x = b \pmod p$

⑦, $p = 811$, $a = 3$, $b = 137$

1) $q \mid p-1$ $q \in \{2,3,5\}$

$3^{\frac{810}{2}} \pmod{811} = -1 \neq 1$

$3^{\frac{810}{3}} \pmod{811} = 680 \neq 1$

$3^{\frac{810}{5}} \pmod{811} = 212 \neq 1$

$\Rightarrow g = 3$ - обр.

$810 = 2 \cdot 5 \cdot 3^4$

2) $c(2,0) = 1$

$c(2,1) = 3^{\frac{810}{2}} = 3^{405} = -1$

$c(3,0) = 1$

$c(3,1) = 3^{\frac{810}{3}} = 680$

$c(3,2) = 3^{\frac{810}{3} \cdot 2} = 130$

$c(5,0) = 1$

$c(5,1) = 212$

$c(5,2) = 3^{\frac{810}{5} \cdot 2} = 339$

$c(5,3) = 3^{\frac{810}{5} \cdot 3} = 380$

$c(5,4) = 3^{\frac{810}{5} \cdot 4} = 570$

3) $p = 2$, $k = 1$

$x = x_1 \pmod 2$, $x_1 = j_0$

$137^{405} \pmod{811} = 1 \Rightarrow \underline{x_1 = j_0 = 0}$

4) $p = 5$ $k = 1$

$x = x_2 \pmod 5$, $x_2 = j_0$

$137^{\frac{810}{5}} = 137^{162} \pmod{811} = 1 \Rightarrow \underline{x_2 = j_0 = 0}$

5) $p = 3$, $k = 4$

$x = x_3 \pmod{81} \Rightarrow x_3 = j_0 + 3j_1 + 9j_2 + 27j_3$

2)

$137^{270} \pmod{811} = 1 \Rightarrow j_0 = 0$

$(137 \cdot 3^{-9})^{30} \pmod{811} = 680 \Rightarrow j_1 = 1$

$(137 \cdot 3^{-3})^{30} \pmod{811} = 130 \Rightarrow j_2 = 2$

$(137 \cdot \underbrace{3^{-3-18}}_{18})^{10} \pmod{811} = 680 \Rightarrow j_3 = 1$

$\Rightarrow \underline{x_3 = 3 + 18 + 27 = 48.}$

К.Т.О. $N = 810$

$N_1 = \frac{810}{2} = 405$ | $x_1 = 0 \pmod 2$

$N_2 = \frac{810}{5} = 162$ | $x_2 = 0 \pmod 5$

$N_3 = \frac{810}{81} = 10$ | $x_3 = 48 \pmod{81}$

$M_1 = N_1^{-1} \pmod{n_1} = 405^{-1} \pmod 2 = 1$

$M_2 = N_2^{-1} \pmod{n_2} = 162^{-1} \pmod 5 = 3$

$M_3 = N_3^{-1} \pmod{n_3} = 10^{-1} \pmod{81} = 73$

$x = \underbrace{0 \cdot 405 \cdot 1}_{0} + \underbrace{0 \cdot 162 \cdot 3}_{0} + 48 \cdot 73 \cdot 10 \pmod{810} =$

$= 210 \pmod{810}$

Проверка $3^x = 3^{210} = 137 \pmod{811} \Rightarrow$ верно.

Ответ: 210