Homework #5

Student name: *Chengqi Liu (1954148), Maitraiyi Dandekar (1990136), Zakariae Jabbour (2039702)*

Course: *Cryptology (2MMC10)* – Professor: *Tanja Lange*
Due date: *October 10th, 2023*

1.
$p = 1249$. $p - 1 = 2^5 * 3 * 13$. $g = 7$. $h_b = 1195$.
Let

$$\begin{aligned} b =& a_0 + a_1 2 + a_2 2^2 + a_3 2^3 + a_4 2^4 \\ =& \sum_{j=0}^{4} a_j 2^j,\ (a_j \in \mathbb{Z}_2) \mod 2^5 \end{aligned}$$

$\forall r \in \{1, 2, 3, 4, 5\}$:

$$\begin{aligned} & g^b = h_b \mod p \\ \Rightarrow & (g^b)^{\frac{p-1}{2^r}} = h_b^{\frac{p-1}{2^r}} \mod p \\ \Rightarrow & g^{\sum_{j=0}^{4} 2^{j-r}(p-1)a_j} = h_b^{\frac{p-1}{2^r}} \mod p \\ \Rightarrow & \prod_{j=0}^{4} g^{2^{j-r}(p-1)a_j} = h_b^{\frac{p-1}{2^r}} \mod p \\ \Rightarrow & \prod_{j=0}^{r-1} g^{\frac{p-1}{2^{r-j}}a_j} \prod_{j=r}^{4} g^{2^{j-r}(p-1)a_j} = h_b^{\frac{p-1}{2^r}} \mod p \end{aligned}$$

When $j \geq r$, because $g^{p-1} = 1 \mod p$,

$$g^{2^{j-r}(p-1)a_j} = 1 \mod p$$

So,

$$\prod_{j=r}^{4} g^{2^{j-r}(p-1)a_j} = 1 \mod p$$

So,

$$\prod_{j=0}^{r-1} g^{\frac{p-1}{2^{r-j}}a_j} = h_b^{\frac{p-1}{2^r}} \mod p \tag{1}$$

$$\Rightarrow (g^{\frac{p-1}{2}})^{a_{r-1}} = \frac{h_b^{\frac{n-1}{2^r}}}{\prod_{j=0}^{r-2} g^{\frac{p-1}{2^{r-j}}a_j}} \mod p \tag{2}$$

Formula (2) is the recursive formula of a_j. We can just solve this DLP (using BSGS) and get a_{r-1} from $a_0, a_1, ..., a_{r-2}$. The order of $g^{\frac{p-1}{2}}$ is 2.
Let $r = 1$ in formula (1), we have

$$(g^{\frac{p-1}{2}})^{a_0} = h_b^{\frac{p-1}{2}} \mod 2$$

Solve this DLP using BSGS and we can get the initial value a_0. Run the program "Pohlig-Hellman.py" and the first part of output is:

a0 is 0

a1 is 1

a2 is 0

a3 is 0

a4 is 1

So,

$$b = 0 + 2 + 0 + 0 + 2^4 = 18 \mod 2^5$$

For 3 and 13, we have:

$$\begin{aligned}
&(g^{\frac{p-1}{3}})^b = h_b^{\frac{p-1}{3}} \mod p \\
\Rightarrow &(7^{416})^b = 1195^{416} \mod p \\
\Rightarrow &1155^b = 1155 \mod p \\
&(g^{\frac{p-1}{13}})^b = h_b^{\frac{p-1}{13}} \mod p \\
\Rightarrow &(7^{96})^b = 1195^{96} \mod p \\
\Rightarrow &994^b = 240 \mod p
\end{aligned}$$

Run the program "Pohlig-Hellman.py" and the second part of output is:

log_1155(1155) is 1

log_994(240) is 12

So,

$$\begin{aligned}
b &= 18 \mod 2^5 \\
b &= 1 \mod 3 \\
b &= 12 \mod 13
\end{aligned}$$

Using CRT to solve this equation set. Run the program "Pohlig-Hellman.py".

```
ans=Pohlig_Hellman(g,hb,p-1,p_l,e_l,p)[0]
print("The answer is",ans)
if pow(g,ans,p)==hb:
print("The answer is correct.")
```

```
else:
print("The answer is wrong!")
```

The third part of output is:
The answer is 1234
The answer is correct.
So, $b = 1234$ and $g^b = 1195 = h_b$. You can find all the codes in file "Pohlig-Hellman.py".

2.(a)

$n = 396553$. $e = 17$. $p = 541$. $q = 733$.

$$\begin{aligned} \phi(n) =& (p-1)(q-1) = 395280 \\ d =& e^{-1} \mod \phi(n) = 302273 \\ d_p =& d \mod p-1 = 413 \\ d_q =& d \mod q-1 = 689 \\ u =& p^{-1} \mod q = 691 \end{aligned}$$

So, $(n, p, q, d_p, d_q, u) = (396553, 541, 733, 413, 689, 691)$.

(b)

$a = 2$. $1 \leq a < p$.

$$a^p \mod p = 2^{541} \mod 541 = 2 = a$$

So, p passes the one-round Fermat test. It's probably a prime.

(c)

$c = 234040$. Using CRT method, we have

$$\begin{aligned} c_p =& c \mod p = 328 \\ c_q =& c \mod q = 213 \\ m_p =& c_p^{d_p} \mod p = 37 \\ m_q =& c_q^{d_q} \mod q = 162 \\ m =& m_p + pu(m_q - m_p) \mod n \\ =& 37 + 541 * 691 * (162 - 37) \mod 396553 \\ =& 332211 \end{aligned}$$

Verify it:

$$c' = m^e \mod n = 234040 = c$$

So, the answer is correct.