VE475 Homework 6

Liu Yihao 515370910207

Ex. 1 — Application of the DLP

1. (a) For Alice, she knows that

$$\gamma \equiv \alpha^r \bmod p$$

If Bob replies

$$b \equiv r \bmod p-1 \text{ or } b \equiv x+r \bmod p-1$$

She can get

$$\alpha^{p-1} \equiv 1 \bmod p$$

$$\alpha^r \equiv \alpha^b \equiv \gamma \bmod p \text{ or } \alpha^r \equiv \alpha^{b-x} \equiv \gamma \bmod p$$

So after calculating $\alpha^b \bmod p$ or $\alpha^{b-x} \bmod p$ and compare it with γ, she can prove Bob's identity if he replies the correct b.

   (b) For Bob, he doesn't know r, but he can compute $b = \log_\alpha \gamma$ or $b = \log_\alpha \gamma + x$ so that $b \equiv r \bmod p-1$. If he can't do so, it becomes a DLP problem which is very difficult to solve, so he can prove his identity.

2. (a)

   (b)

3. It is Digital Signature Protocol.

Ex. 2 — Pohlig-Hellman

First, let g be a generator of the group, let $x = \log_g h$, let n be the order of the group, obtain a prime factorization so that

$$n = \prod_{i=1}^{r} p_i^{e_i}$$

Then, for each $i \in \{1, \ldots, r\}$, compute $g_i = g^{n/p_i^{e_i}}$, which has order $p_i^{e_i}$, and compute $h_i = h^{n/p_i^{e_i}}$. Then we can use the Pohlig-Hellman algorithm for prime-power order to compute $x_i \in \{0, \ldots, p_i^{e_1} - 1\}$, which is described as follow:

1. Let $x = \log_g h$ ($x = x_i$, $g = g_i$, $h = h_i$ from previous part), where $g = p^e$, and first initialize $x_0 = 0$.
2. Set $\gamma = g^{p^{e-1}}$.
3. For each $k \in \{0, \ldots, e-1\}$, compute $h_k = (g^{-x_k} h)^{p^{e-1-k}}$, By construction, the order of this element must divide p, hence $h_k \in \langle\gamma\rangle$. Then compute d_k such that $\gamma^{d_k} = h_k$ and set $x_{k+1} = x_k + p^k d_k$.

4. Obtain $x = x_e$.

After get all x_i, solve the simultaneous congruence

$$x \equiv x_i \bmod p_i^{e_i}, i \in \{1, \dots, r\}$$

according to Chinese reminder theorem to get $x = \log_g h$.

As an example, we try to find $\log_3 3344$ in $G = U(Z/24389Z)$. Note that $24389 = 29^3$, so the order $n = 28^3 = 2^6 \cdot 7^3$.

$$\varphi(85) = 2^6$$

$$\varphi() = 7^3$$

And 3 is a generator of G, so we can get

$$g_1 \equiv 3^{7^3} \equiv 62 \bmod 85$$
$$h_1 \equiv 3344^{7^3} \equiv 24 \bmod 85$$
$$g_2 \equiv 3^{2^6} \equiv 225 \bmod 342$$
$$h_2 \equiv 3344^{2^6} \equiv 76 \bmod 342$$

First, for $p = 2$, $e = 6$, $g = 62$ and $h = 24$, we should determine $x = \log_g h$ in $G = U(Z/85Z)$. We can get

$$\gamma \equiv 62^{2^5} \equiv 1 \bmod 85$$

$$h_0 \equiv (62^0 \cdot 24)^{2^5} \equiv 1 \bmod 85, \quad d_0 = 1, \quad x_1 \equiv 1 \bmod 85$$