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

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

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

Ex. 3 — Elgamal

(a) If the polynomial $X^3 + 2X^2 + 1$ is reducible in $F_3[x]$, it can be factored as

$$X^3 + 2X^2 + 1 = (X + A)(X^2 + BX + C) = X^3 + A(B + 1)X^2 + (B + C)X + AC$$

There are two possible pairs of (A, C), which are $(1, 1)$ and $(2, 2)$ so that $AC = 1$.

First, if $A = C = 1$, then $B = 2$, but $A(B + 1) = 0 \neq 2$, so it is wrong.

Second, if $A = C = 2$, then $B = 1$, but $A(B + 1) = 1 \neq 2$, so it is also wrong.

Then we can conclude that $X^3 + 2X^2 + 1$ is irreducible in $F_3[x]$.

According to Theorem 2.38, $X^3 + 2X^2 + 1$ is an irreducible polynomial of degree 3 in $F_3[x]$, let F_{3^3} be the set of all the polynomial of degree less than 3 in $F_3[x]$, then F_{3^3} is a finite field with $3^3 = 27$ elements.

(b) We can use 26 lower-case letters and define a map $\xi \leftrightarrow f(\xi)$, where ξ is one of 26 letters. That is, $a \leftrightarrow 1$, $b \leftrightarrow 2$, $\ldots$, $z \leftrightarrow 26$. Then we can define three variables α, β, γ so that

$$\begin{aligned}
\alpha &= f(\xi) \text{ div } 9 \\
\beta &= (f(\xi) \bmod 9) \text{ div } 3 \\
\gamma &= f(\xi) \bmod 3
\end{aligned}$$

And now we can define the map as

$$\xi \to g(\xi) : g(\xi) = \alpha X^2 + \beta X + \gamma$$

(c) Let $P(x) = X^3 + 2X^2 + 1$,

$$\begin{array}{ccc}
x^1 \equiv x \bmod P(x) & x^2 \equiv x^2 \bmod P(x) & x^3 \equiv x^2 - 1 \bmod P(x) \\
x^4 \equiv x^2 - x - 1 \bmod P(x) & x^5 \equiv -x - 1 \bmod P(x) & x^6 \equiv -x^2 - x \bmod P(x) \\
x^7 \equiv x^2 + 1 \bmod P(x) & x^8 \equiv x^2 + x - 1 \bmod P(x) & x^9 \equiv -x^2 - x - 1 \bmod P(x) \\
x^{10} \equiv x^2 - x + 1 \bmod P(x) & x^{11} \equiv x - 1 \bmod P(x) & x^{12} \equiv x^2 - x \bmod P(x) \\
x^{13} \equiv -1 \bmod P(x) & x^{14} \equiv -x \bmod P(x) & x^{15} \equiv -x^2 \bmod P(x) \\
x^{16} \equiv -x^2 + 1 \bmod P(x) & x^{17} \equiv -x^2 + x + 1 \bmod P(x) & x^{18} \equiv x + 1 \bmod P(x) \\
x^{19} \equiv x^2 + x \bmod P(x) & x^{20} \equiv -x^2 - 1 \bmod P(x) & x^{21} \equiv -x^2 - x + 1 \bmod P(x) \\
x^{22} \equiv x^2 + x + 1 \bmod P(x) & x^{23} \equiv -x^2 + x - 1 \bmod P(x) & x^{24} \equiv -x + 1 \bmod P(x) \\
x^{25} \equiv -x^2 + x \bmod P(x) & x^{26} \equiv 1 \bmod P(x) &
\end{array}$$

So the order of the subgroup generated by X is 26, and X is a generator of F_{3^3}.

(d) Use X as the generator and 11 as the secret key,

$$X^{11} \equiv x - 1 \equiv x + 2 \bmod P(x)$$

So $x + 2$ is the public key.

(e) Choose $k = 18$, we can get

$$r \equiv X^{18} \equiv x + 1 \bmod P(x)$$