VE475 Homework 6

Yiwen Yang

Ex. 1 - Application of the DLP

1. (a) With r, Alice can calculate α^r, which should be the same as $\gamma \bmod p$.

   With $x + r \bmod (p-1)$, since $\alpha^{p-1} \equiv 1 \bmod p$, then $\alpha^{x+r \bmod (p-1)} \equiv \alpha^{x+r} \equiv \alpha^x \alpha^r \bmod p$, which should be the same as $\beta \cdot \gamma$.

   So r and $x + r \bmod (p-1)$ are considered so that Alice can operate on it to verify the results.

   (b) If Alice requests r, she will never know x; If Alice requests $x+r$, she cannot know x either without knowing r, because she only knows $\beta = \alpha^x$ and $\gamma = \alpha^r$ separately both of which is hard to solve. So Alice cannot cheat to get x by requesting r or $x + r$.

   If Bob does not know the true x, there is no way to answer $x+r$, thus Bob cannot cheat either. On the other hand, if Bob can correctly answer both r and $x + r$, then he definitely knows x, so he can prove his identity.

2. (a) 128 times.

   (b) 256 times.

3. Digital Signature.

Ex. 2 - Pohlig-Hellman

Let g be a generator of a cyclic group G with order n, for h in G, find $x \in \{0, \dots, n-1\}$ such that $g^x = h$.

1. Factorize $n = \Pi_{i=1}^{r} {p_i}^{e_i}$.

2. Repeat Step 3 to 5 for all $i \in \{1, \dots, r\}$.

3. Compute $g_i = g^{n/{p_i}^{e_i}}$.

4. Compute $h_i = h^{n/{p_i}^{e_i}}$.

5. Find $x_i \in \{0, \dots, {p_i}^{e_i} - 1\}$ such that ${g_i}^{x_i} = h_i$.

6. Use Chinese Remainder Theorem to solve $x \equiv x_i \bmod {p_i}^{e_i}$.

In this example, $n = 28 \times 29^2 = 2^2 \times 7 \times 29^2$, $g = 3$, $h = 3344$.

1. $p_0 = 2$, $e_0 = 2$, $g_0 = 10133$, $h_0 = 24388$, $x_0 = 2$.

2. $p_1 = 7$, $e_1 = 1$, $g_1 = 7032$, $h_1 = 4850$, $x_1 = 2$.

3. $p_2 = 29$, $e_2 = 2$, $g_2 = 11369$, $h_2 = 23114$, $x_2 = 260$.

Then calculate $7 \times 841 \times 3 \equiv 1 \bmod 4$, $4 \times 841 \times 2 \equiv 1 \bmod 7$, $4 \times 7 \times 811 \equiv 1 \bmod 841$, so $x \equiv 7 \times 841 \times 3 \times 2 + 4 \times 841 \times 2 \times 2 + 4 \times 7 \times 811 \times 260 \equiv 18762 \bmod 23548$.

Ex. 3 - Elgamal

1. Suppose that $X^3 + 2X^2 + 1$ is irreducible in $F_3[x]$, then

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

$$AC = 1$$

   If $A = C = 1$, then $B + 1 = 2$, $B + 1 = 0$ contradicts.

   If $A = C = 2$, then $B + 2 = 2$, $2B + 2 = 0$ also contradicts.

   So $X^3 + 2X^2 + 1$ is irreducible in $F_3[x]$ with degree 3, and we can conclude that F_{3^3} is a finite field with $3^3 = 27$ elements.

2. X is a generator of F_{3^3}. First let $a = 1, b = 2, \ldots, z = 26$, then the map can be defined as $c \to f(c) : f(c) = X^c \bmod (X^3 + 2X^2 + 1)$.

3. The order is 26.

4. $X^{11} \equiv X + 2 \bmod (X^3 + 2X^2 + 1)$, then public key is $X + 2$.

5. First convert "goodmorning" into F_{3^3}, yielding $\{1+X^2, 2X^2, 2X^2, 2+2X+X^2, 2, 2X^2, 1+X, 2X, 2+2X+2X^2, 2X, 1+X^2\}$.

   Randomly pick $k = 23$, $r \equiv X^{23} \equiv (2+X+2X^2) \bmod (X^3+2X^2+1)$, $t \equiv (X+2)^{23}m \equiv (X + X^2)m \bmod (X^3 + 2X^2 + 1)$. Then the cipher text is $\{1, 2 + X + X^2, 2 + X + X^2, 2 + X + 2X^2, 2X + 2X^2, 2 + X + X^2, 2 + X, 1 + X^2, X^2, 1 + X^2, 1\}$, mapping to "zhhwfhkgbgz".

   To decrypt, calculate $r^{-1} = 2 + X^2$, $tr^{-x} \equiv t(2 + X^2)^{11} \equiv 1 + X^2 \bmod (X^3 + 2X^2 + 1)$. The result plain text is $\{1 + X^2, 2X^2, 2X^2, 2 + 2X + X^2, 2, 2X^2, 1 + X, 2X, 2 + 2X + 2X^2, 2X, 1 + X^2\}$, mapping to "goodmorning", which is correct.

Ex. 4 - Simple Questions

1. (a) h is pre-image resistant. To reversely find x is to solve Quadratic Residuosity Problem, which is very difficult with large primes p and q.
   (b) h is not second pre-image resistant. Given x, $h(-x) = h(x)$.
   (c) h is not collision resistant. For every x, $h(-x) = h(x)$.
2. (a) h can be efficiently computed for any input.
   (b) h is not pre-image resistant. To reversely find m, simply calculate $h(h(m))$.
   (c) h is not second pre-image resistant. Given m, let $n = m \parallel \{160'b0\}$, then $h(m) = h(n)$.
   (d) h is not collision resistant. For every m, let $n = m \parallel \{160'b0\}$, then $h(m) = h(n)$.

Ex. 5 - Merkle-Damgård Construction

See in **H7**.

Ex. 6 - Programming

See in folder **ex6**.