VE475 Introduction to Cryptography
Homework 6

Jiang, Sifan
jasperrice@sjtu.edu.cn
515370910040

June 30, 2019

Ex. 1 - Application of the DLP

1. a) Bob sends $\gamma \equiv \alpha^r \mod p$ to Alice. If Bob replies with $b \equiv r \mod (p-1)$ or $b \equiv x + r \mod (p-1)$, then according to Fermat's little theorem, we have $\alpha^{p-1} \equiv 1 \mod p$. We would then have

$$\alpha^b \equiv \alpha^r \equiv \gamma \mod p$$

or

$$\alpha^b \equiv \alpha^{x+r} \equiv \beta\gamma \mod p$$

So, Alice can get γ or $\beta\gamma$ and since she has got γ and known β, she can prove Bob's identity.

   b) Bob cannot compute $x + r \mod (p-1)$ if he doesn't know x. And it would be a DLP problem to solve $\alpha^{x+r} \equiv \beta\gamma \mod p$. So, Bob can prove his identity.

2. a) 128 times should be repeated for a 128 bits security level.

   b) 256 times should be repeated for a 256 bits security level.

3. It's a Digital Signature Protocol.

Ex. 2 - Pohlig-Hellman

Assume α is a generator of the group. Let $x = \log_\alpha \beta$, let the order of the group

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

where $r \in \mathbb{N}$. Then compute $\alpha_i = \alpha^{n/p_i^{e_i}}$ and compute $\beta_i = \beta^{n/p_i^{e_i}}$ in the group G.

Let $x_i = \log_{\alpha_i} \beta_i$, where $\alpha_i = p_i^{e_i}$ and $x_{i,0} = 0$. For each $k \in \{0, \cdots, e_i - 1\}$, calculate $\beta_{i,k} = (\alpha_i^{-x_{i,k}} \beta_i)^{p_i^{e_i-1-k}}$. Have $\gamma = \alpha_i^{p_i^{e_i-1}}$ and then compute d_k such that $\gamma^{d_k} = \beta_{i,k}$ and let $x_{k+1} = x_k + p_i^k d_k$. And finally obtain $x_i = x_{i,e_i}$. We can then have $x_i = x \mod p_i^{e_i}$ for $1 \leq i \leq r$ and use Chinese remainder theorem to solve x.

As an example, we are going to calculate $\log_3 3344$ in $\mathbb{Z}/24389\mathbb{Z}$. Since $24389 = 29^3$, the order of the group is $28 \cdot 29^2 = 2^2 \cdot 7 \cdot 29^2$. And since 3 is a generator of the group, we would have

$$\begin{aligned}
\alpha_1 &\equiv 3^{n/2^2} \equiv 3^{7\cdot 29^2} \equiv 10133 \mod 24389 \\
\alpha_2 &\equiv 3^{n/7} \equiv 3^{2^2\cdot 29^2} \equiv 7302 \mod 24389 \\
\alpha_3 &\equiv 3^{n/29^2} \equiv 3^{2^2\cdot 7} \equiv 11369 \mod 24389 \\
\beta_1 &\equiv 3344^{n/2^2} \equiv 3344^{7\cdot 29^2} \equiv 24388 \mod 24389 \\
\beta_2 &\equiv 3344^{n/7} \equiv 3344^{2^2\cdot 29^2} \equiv 4850 \mod 24389 \\
\beta_3 &\equiv 3344^{n/29^2} \equiv 3344^{2^2\cdot 7} \equiv 23114 \mod 24389
\end{aligned}$$

For $p_1 = 2$, $e_1 = 2$, $\alpha_1 = 10133$, and $\beta_1 = 24388$, we have $\gamma \equiv \alpha_1^{p_1^{e_1-1}} \equiv 10133^2 \equiv -1 \mod 24389$. Then we can calculate

$$\beta_{1,0} \equiv (10133^0 \cdot 24388)^{2^{2-1-0}} \equiv [1\cdot(-1)]^2 \equiv 1 \mod 24389$$

and $d_0 = 0$, $x_{1,1} \equiv x_{1,0} + p_1^0 d_0 \equiv 0 \mod 4$. Then by iteration, we have $\beta_{1,1} = -1$, $d_1 = 1$, and $x_{1,2} = 2$. So $x_1 = x_{1,2} = 2 \mod 4$.

Similarly, we would have $x_2 = 2 \mod 7$ and $x_3 = 260 \mod 29^2$. Applying Chinese remainder theorem, we would have $x = 18762 \mod 2^2 \cdot 7 \cdot 29^2$.

Ex. 3 - Elgamal

1. Assume X^3+2X^2+1 is reducible over $\mathbb{F}_3[X]$. Then we can find $(X+a)(X^2+bX+C) = X^3+a(b+1)X^2+(b+c)X+ac = X^3+2X^2+1$, where $a, b, c \in \{0, 1, 2\}$. So $a = 1$, $b = -1$, $c = 1$, or $a = 2$, $b = -2$, $c = 2$. But neither of the two cases would lead to $a(b+1) \equiv 2 \mod 3$. So X^3+2X^2+1 is irreducible over $\mathbb{F}_3[X]$. And since the degree is 3, it defines the field $\mathbb{F}_{3^3}$, which has 27 elements.

2. Let $a \leftrightarrow X^1$, $b \leftrightarrow X^2$, $\cdots$, $z \leftrightarrow X^{26}$. We have $P(X) = X^3+2X^2+1$.

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

3. The order of the subgroup generated by X is shown in previous question, which is 26.

4. If we have 11 as the secret key, we would have

$$X^{11} \equiv X + 2 \mod P(X)$$

   Then the public key is $X + 2$.

5. Randomly choose $k = 18$, map "goodmorning" to $\mathbb{F}_{3^3}$, we have

X^2+1	$-X^2$	$-X^2$	X^2-X-1	-1	$-X^2$	$X+1$	$-X$	$-X^2-X-1$	$-X$	X^2+1

Then we would have

$$r \equiv X^{18} \equiv X+1 \mod P(X)$$
$$\beta^k \equiv (X+2)^{18} \mod P(X)$$

Encryption: using equation

$$t \equiv \beta^k m \equiv (X+2)^{18} m \mod P(X)$$

The result is

X^2+X	X	X	$-X^2+1$	$-X^2+X$	X	X^2-X-1	1	$-X^2-X+1$	1	X^2+X

which is "saapyadzuzs" after mapping.

Decryption: using equation

$$tr^{-x} \equiv t(X+1)^{-11} \equiv m \mod P(X)$$

The decryption is successful and get "goodmorning".

Ex. 4 - Simple questions

1. (i) Yes, h is pre-image resistant. Since $h(x) \equiv x^2 \mod pq$, we can find x by using Chinese remainder theorem with $\sqrt{h(x)} \mod p$ and $\sqrt{h(x)} \mod q$. However, it is infeasible to factorize n.
   (ii) No, h is not second pre-image resistant. Let $x' = -x$, we would have $h(x) = h(x')$.
   (iii) No, h is not collision resistant. Let $x' = -x$, we would have $h(x) = h(x')$.
2. (i) It is efficiently computed for any input since $\oplus$ is fast.
   (ii) Pre-image resistant is not verified. Given y it is feasible to find or design m such that $h(m) = y$.
   (iii) Second pre-image resistant is not verified. There are many combination can lead to same $h(m)$.
   (iv) Collision resistant is not verified. There are many combination can lead to same $h(m)$.

Ex. 5 - Merkle-Damgård construction

1. a) Since $f(0) = 0$ and $f(1) = 01$, $f(x_i)$ is always start with 0. So y can be separated into several segments start from 0, except for the first two digits. Those segments are injective with x_i, so the map s from x to y is injective.
   b) If z is empty, from what previous proved, there's no such x'. If z is not empty, since we have 11 at the beginning of y_{i+1}, so no this no such x' and z such that $s(x) = z \| s(x')$.
2. Because the previous conditions guarantee the mapping is collision resistant.