VE475 Intro to Cryptography Homework 6

Taoyue Xia, 518370910087

2021/06/29

Ex1 — Application of the DLP

1. a) Since α is a generator of $\mathbb{Z}/p\mathbb{Z}$, we know that:

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

If Bob replies $\delta \equiv r \ mod \ (p-1)$ or $\delta \equiv x + r \ mod \ (p-1)$, Alice can calculate:

$$\alpha^{\delta} \equiv \alpha^{r \ mod \ (p-1)} \equiv \gamma \ mod \ p \qquad \text{or} \qquad \alpha^{\delta} \equiv \alpha^{x+r \ mod \ (p-1)} \equiv \beta\gamma \ mod \ p$$

With these two values, Alice can simply calculate α^{δ} to get a value, compare it with γ or $\beta\gamma$, and finally verify Bob's identity of knowing $\log_{\alpha} \beta$.

b) If Bob does not know how to calculate $\log_{\alpha} \beta$, since it is very hard to solve DLP problems, it is quite impossible for Bob to know the exact value of x, thus the reply $x + r$ would be wrong answer. Then Alice will know that Bob's identity is false. Therefore, Bob can prove his identity.
For Alice, if she doesn't know the protocol, she will never figure out what the two values Bob replies mean. Therefore, Alice cannot cheat too.

2. (a) 128

   (b) 256

3. It's Diffie-Hellman key exchange protocol.

Ex2 — Pohlig-Hellman

For a cyclic group G of order n with a generator g, we need to compute the logarithm $x = log_g h$, and the order n can be expressed as:

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

Then for each $i \in \{1, \cdots, r\}$, compute $g_i = g^{n/p_i^{e_i}}$. According to Lagrange's Theorem, g_i has order $p_i^{e_i}$.
Then compute $h_i = h^{n/p_i^{e_i}}$, we can obviously see that $h_i \in \langle g_i \rangle$. Then apply the Pohlig-Hellman algorithm for groups of prime-order power, for each group $\langle g_i \rangle$, compute $x_i \in \{0, \cdots, p_i^{e_i} - 1\}$ such that $g_i^{x_i} = h_i$. The complete algorithm is shown below, for each group $\langle g_i \rangle$:

1. Initialize $x_0 = 0$
2. Compute $\gamma = g^{p^{e-1}}$, which has order p.
3. For all $k \in \{0, \cdots, e-1\}$:
   (i) Compute $h_k = (g^{-x_k} h)^{e-1-k}$, it is obvious that the order of this element divides p, hence $h_k \in \langle \gamma \rangle$
   (ii) Compute $d_k \in \{0, \cdots, p-1\}$ such that $\gamma^{d_k} = h_k$.
   (iii) set $x_{k+1} = x_k + p_k^{d_k}$.
4. Finally, x_e is the value we need.

Finally, solve the simultaneous congruence:

$$x \equiv x_i \ mod \ p_i^{e_i} \qquad \forall i \in \{1, \cdots, r\}$$

We can apply Chinese Remainder Theorem to get the $x = \log_g h$.

For the example, which asks us to calculate $x = \log_3 3344$ in $G = U(\mathbb{Z}/24389\mathbb{Z})$, $g = 3$ is the generator, we can first find that $24389 = 29^3$, then according to the proof we have done in

h4 ex1.1, we know that the order of $U(\mathbb{Z}/p^k\mathbb{Z})$ is $p^{k-1}(p-1)$, so the order n can be calculated as:

$$n = 29^{3-1} \cdot (29-1) = 2^2 \cdot 7 \cdot 29^2$$

Knowing that $g = 3$ and $h = 3344$, we can calculate each g_i and h_i, $i = 1, 2, 3$ as following:

$$g_1 = g^{n/2^2} = 3^{7 \cdot 29^2} \equiv 10133 \ mod \ 24389$$

$$h_1 = h^{n/2^2} = 3344^{7 \cdot 29^2} \equiv 24388 \ mod \ 24389$$

$$g_2 = g^{n/7} = g^{2^2 \cdot 29^2} \equiv 7302 \ mod \ 24389$$

$$h_2 = h^{n/7} = h^{2^2 \cdot 29^2} \equiv 4850 \ mod \ 24389$$

$$g_3 = g^{n/29^2} = g^{2^2 \cdot 7} \equiv 11369 \ mod \ 24389$$

$$h_3 = h^{n/29^2} = h^{2^2 \cdot 7} \equiv 23114 \ mod \ 24389$$

Then we can apply the Pohlig-Hellman algorithm for groups of prime-order power for each g_i.

(a) For $p = 2$, $e = 2$, $g = 10133$ and $h = 24388$, we can first calculate γ as:

$$\gamma = g^{p^{e-1}} \equiv 10133^2 \equiv 24388 \equiv -1 \ mod \ 24389$$

Then for $k = 0, 1$, calculate h_k, d_k, x_{k+1} as:

$$h_0 = (10133^0 \cdot 24388)^{2^1} \equiv 1 \ mod \ 24389 \quad d_0 = 0 \quad x_1 = 0$$

$$h_1 = (10133^0 \cdot 24388)^{2^0} \equiv -1 \ mod \ 24389 \quad d_1 = 1 \quad x_2 = 2$$

So for $p = 2$, $e = 2$, $x = 2 \ mod \ 4$

(b) For $p = 7$, $e = 1$, $g = 7302$, $h = 4850$, we can first calculate γ as:

$$\gamma = 7302^{7^0} \equiv 7302 \ mod \ 24389$$

Then for $k = 0$, calculate $h_0,\ d_0,\ x_1$ as:

$$h_0 = (7302^0 \cdot 4850)^{7^0} = 4850 \ mod \ 24389 \quad d_0 = 2 \quad x_1 = 2$$

So for $p = 7$, $e = 1$, $x = 2 \ mod \ 7$.

(c) For $p = 29$, $e = 2$, $g = 11369$, $h = 23114$, we can first calculate γ as:

$$\gamma = 11369^{29} \equiv 12616 \ mod \ 24389$$

Then for $k = 0, 1$, calculate h_k, d_k, x_{k+1} as:

$$h_0 = (11369^0 \cdot 23114)^{29^1} \equiv 11775 \ mod \ 24389 \qquad d_0 = 28 \quad x_1 = 28$$

$$h_1 = (11369^{-28} \cdot 23114)^{29^0} \equiv (7135^{28} \cdot 23114) \equiv 3365 \quad d_1 = 8 \quad x_2 = 260$$

So for $p = 29$, $e = 2$, $x = 260 \ mod \ 841$.

Finally, we can apply the Chinese Remainder Theorem to

$$\begin{cases} x_1 \equiv 2 \ mod \ 4 \\ x_2 \equiv 2 \ mod \ 7 \\ x_3 \equiv 260 \ mod \ 841 \end{cases}$$

Firstly, for each $m_i = 4, \ 7, \ 841$, calculate the corresponding $M_i = 5887, \ 3364, \ 28$, Then calculate the corresponding t_i which satisfies $M_i t_i \equiv 1 \ mod \ m_i$. We can get $t_i = 3, \ 2, \ 811$. So the exact x can be calculated as:

$$x = 2 \cdot 3 \cdot 5887 + 2 \cdot 2 \cdot 3364 + 260 \cdot 28 \cdot 811 \equiv 18762 \ mod \ 23548$$

Therefore, $\log_3 3344 = 18762 \ mod \ 23548$.

Ex3 — Elgamal

1. We can prove this by contradiction. Suppose $X^3 + 2X^2 + 1$ is reducible, so it can have factorization as:

   $X^3+2X^2+1 \equiv (AX+B)(CX^2+DX+E) \equiv (AC)X^3+(AD+BC)X^2+(AE+BD)X+BE$

   Then AC are both 1 or 2, and so does BE pair.

   (a) When $A, C = 1$ and $B, E = 1$, since $AD + BC = 2$, $D = 1$. However, $AD + BC = 0$ indicates that $D = 2$, which raises a contradiction.

(b) When $A, C = 1$ and $B, E = 2$, since $AD + BC = 2$, $D = 0$. However, $AE + BD = 0$ indicates that $D = 2$, which raises a contradiction.

(c) When $A, C = 2$ and $B, E = 1$, since $AD + BC = 2$, $D = 0$. However, $AE + BD = 0$ indicates that $D = 1$, which raises a contradiction.

(d) When $A, C = 2$ and $B, E = 2$, since $AD + BC = 2$, $D = 2$. However, $AE + BD = 0$ indicates that $D = 1$, which raises a contradiction.

With the four conditions above, we cannot find some A, B, C, D, E that can meet the factorization. Therefore, $X^3 + 2X^2 + 1$ is irreducible in $\mathbb{F}_3$.
According to the theorem in c2, p.38, since $X^3 + 2X^2 + 1$ is an irreducible polynomial of degree 3 in $\mathbb{F}_3$, we can define F as the set of all the polynomials of degree less than 3, Then F has $3^3 = 27$ elements, which indicates that $X^3 + 2X^2 + 1$ defines the field $\mathbb{F}_{3^3}$, which has 27 elements.

2. We can transform letters of the alphabet to their corresponding position, namely, $1, \cdots, 26$. After that, we can calculate $X^i \ mod \ P(X)$, where $i \in \{1, \cdots, 26\}$ and $P(X) = X^3 + 2X^2 + 1$ in $\mathbb{F}_{3^3}$. Thus the map can be shown as $\kappa \to f(\kappa)$, for which $\kappa = \{1, \cdots, 26\}$ and $f(\kappa) = \{X^i \ mod \ P(X) : \ i \in \kappa\}$. The corresponding relationship is shown in the table below:

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

What's more, we can find that X is a generator of $\mathbb{F}_{3^3}$ defined by $P(X)$. And the map is $\kappa \to f(\kappa)$

3. From the previous problem, we can conclude that the order of the subgroup generated by X is 26.

4. Given the secret key $x = 11$, the public key is $\alpha^x \equiv X^{11} \equiv X + 2 \ mod \ P(X)$.

5. Firstly, choose a random number k, here I choose $k = 16$. Then, since the generator α is X, calculate $r \equiv \alpha^k \equiv X^{16} \equiv 2X^2 + 1 \ mod \ P(X)$. Then we can transform each letter of the message "goodmorning" into 11 elements in $\mathbb{F}_{3^3}$ as:

$$X^2+1,\ 2X^2,\ 2X^2,\ X^2+2X+2,\ 2,\ 2X^2,\ X+1,\ 2X,\ 2X^2+2X+2,\ 2X,\ X^2+1$$

Then for each letter, compute $t \equiv \beta^k m \ mod \ P(X)$, where $\beta \equiv \alpha^x \equiv X^{11} \equiv X + 2 \ mod \ P(X)$. So $\beta^k \equiv (X+2)^{16} \equiv 2X^2 + 2 \ mod \ P(X)$. All 11 "t"s are shown below:

$$X,\ 2X^2+2X+1,\ 2X^2+2X+1,\ 2X+1,\ X^2+1,\ 2X^2+2X+1,$$

$$X^2+2,\ X^2+X+2,\ X^2+2,\ X^2+X+2,\ X$$

So the encrypted message is "auuxgulhcha".
After that, compute $m \equiv tr^{-x}$. We can first apply extended Euclidean algorithm to calculate the element s, such that $rs \equiv 1 \ mod \ P(X)$. After some calculation, $s \equiv X^2 + 2X + 1 \ mod \ P(X)$. Then we can get m as:

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

$$m \equiv tr^{-x} \equiv t \cdot (X^2+2X+1)^16 \equiv t \cdot (2X^2+2X) \ mod \ P(X)$$

Therefore, each letter is:

$$X^2+1,\ 2X^2,\ 2X^2,\ X^2+2X+2,\ 2,\ 2X^2,\ X+1,\ 2X,\ 2X^2+2X+2,\ 2X,\ X^2+1$$

After transfroming into letters, the message is "goodmorning", which indicates a successful encryption and decryption.
(P.S. all the calculation this part is done by hand.)

Ex4 — Simple questions

1. (i) Yes, h is pre-image resistant. Given a y, if we want to find x so that $x^2 \equiv y \ mod \ n$, we need to calculate $\sqrt{y} \ mod \ n$. However, since n is the product of two large primes p and q, it is very hard to determine the factorization of n, thus making it computationally infeasible to find the corresponding x. Therefore, h is pre-image resistant.

(ii) No, h is not second pre-image resistant. For $h(x) \equiv x^2 \ mod \ n$, we can easily find $x' = -x$ $(x \neq 0)$ so that $h(x') = h(x)$. Therefore, h is not second pre-image resistant.

(iii) No, h is not collision resistant. Same as (ii), we can choose arbitrary x and $-x$ with $x \neq -x$ and $x \neq 0$ but $h(x) = h(x')$. Therefore, h is not collision resistant.

2. (i) The property "Efficiently computed for any input" is verified, because any input message can be ouput as 160 bits by xor efficiently.

(ii) The property "pre-image resistant" is not verified by h, because given an output y which is 160 bits, we can easily find some input x, break it into blocks of 160 bits, and after xor, $h(x) \equiv y$. Therefore, h doesn't verify "pre-image resistant".

(iii) The property "second pre-image resistant" is not verified by h. For message m, we can find some m' which only swap the positions of each blocks m_i of m. After doing xor, $h(m) \equiv h(m')$. Therefore, h doesn't verify "second pre-image resistant".

(iv) The property "collision resistant" is not verified by h. We can just choose some arbitrary message m, after breaking it into blocks of 160 bits, we can reform the m_i, swap them into different order, get a different message m'. However, after doing xor, $h(m) \equiv h(m')$. Therefore, h doesn't verify "collision resistant".

Ex5 — Merkle-Dåmgard construction

1. (a) We can prove this by contradiction. Suppose that the map s is not injective, namely, There exists some $x \neq x'$ but $y = y'$.
From $y = y'$ we know that $\forall i \in \{1, \cdots, k\}$, $y_i = y'_i$. Then if $y_k = y'_k = 0$, $x_{|x|} = x'_{|x'|} = 0$. After that, delete the last bit of y and y'. If $y_{k-1}||y_k = 01$, we know that $x_{|x|} = x'_{|x'|} = 1$. After that verification, delete the last two bits of y and y'. Iterate this method until $y = y' = 11$, we can find that $\forall i \in \{1, \cdots, |x|\}$, $x_i = x'_i$. Therefore, If $y = y'$, $x = x'$, which raises a contradiction. So the map $\mathbf{s}$ from x to y is injective.

(b) If z is null, according to the former question, we have proved that s is an injection, thus if $x \neq x'$, $s(x) \neq s(x')$.
If z contains some bits, then for $w = z||s(x') = w_1|| \cdots ||w_{|w|}$, there exists the i_{th} and $i + 1_{th}$ bits, for which i is other than 1, that $w_i||w_{i+1} = 11$. However, for $y = s(x)$,

only the first two bits can be 11, so $s(x) \neq z||s(x')$.

Therefore, according to the two conditions above, we can determine that there is no strings $x \neq x'$ and z such that $s(x) = z||s(x')$.

2. For the former condition, if the map s from x to y is not injective, there exists some $x \neq x'$ that makes $y = y'$, then this method doesn't meet the requirement for collision resistant.

   For the second condition, if we can find some $x \neq x'$ and z such that $s(x) = z||s(x')$, the method also doesn't meet the requirement of collision resistant.

   Therefore, the two previous conditions are of a major importance.

3. Assuming we have a collision on h, i.e. $x \neq x'$ and $h(x) = h(x')$, we will prove that a collision on the compression function g can be efficiently found.

   First note that if $|x| \neq |x'|$, then they are padded with different values d and d', respectively. Similarly, $k+1$ and $d'+1$ denote the number of blocks of x and x'.

   Since in this problem $t = 1$ and $t - 1 = 0$, then we don't need to consider the case $|x| \neq |x'|$ mod $(t-1)$. Thus we just need to determine the cases $k = k'$ and $k \neq k'$.

   Case 1: $k = k'$, this implies $y_{k+1} = y'_{k+1}$, and we have:

$$g(z_{k-1}||y_k) = z_k = h(x) = h(x') = z'_k = g(z_{k-1}||y'_k)$$

   If $z_k \neq z'_k$, then a collision is found. Otherwise, we repeat the process and get:

$$g(z_{k-2}||y_{k-1}) = z_{k-1} = z'_{k-1} = g(z_{k-2}||y'_{k-1})$$

   Then either we found a collision or we continue backward until one is obtained. If none is found then we get:

$$z_1 = z'_1, \cdots, z_k = z'_k$$

   which raises a contradiction with $x \neq x'$.

   Case 2: consider $k \neq k'$. Without loss of generality we imply that $k' > k$ and proceed as in case 1. If no collision is found before $k = 1$ then we have:

$$g(0^m||y_1) = z_1 = z'_{k'-k-1} = g(z'_{k'-k-2}||y'_{k'-k-1})$$

   By construction the m_{th} bit on the left is 0 while on the right is 1. Hence we found a collision.

   All the cases being covered this complete the proof.

Ex6 — Programming

Please refer to folder *ex6* to check the codes, and there is also a readme file in it.