Introduction to Cryptography: Homework #6

Due on June 30, 2019 at 11:59pm

Professor Manuel

ShiHan Chan

Problem 1

1. (a) Since Alice knows that $\gamma \equiv \alpha^r \mod p$, if Bob replies $t \equiv r \mod p-1$ or $t \equiv x+r \mod p-1$, then Alice would get $\alpha^{p-1} \equiv 1 \mod p$, $\alpha^t \equiv \alpha^r \equiv \gamma \mod p$ or $\alpha^t \equiv \alpha^{x+r} \equiv \beta\gamma \mod p$.
After Alice calculate $\alpha^t \mod p$ and compare it with $\beta\gamma$ or γ, she can prove Bob identity if Bob can calculate $x = \log_\alpha \beta$
2.
(a)128 times
(b) 192 times
3. The protocol is called digital signature protocol.

Problem 2

Let g be the generator and $x = log_g h$. First, we factorize $n = \sum_{i=1}^{i=r} p_i^{e_i}$. Second, we can calculate the order of the group, order=$\sum_{i=1}^{i=r}(p_i - 1)p_i^{e_i - 1}$.Thirdly, for all $i \in Z \cup [1, r]$, $g_i = g^{\frac{n}{p_i^{e_i}}}$, $h_i = h^{\frac{n}{p_i^{e_i}}}$.
Initilize $x = x_i, g = g_i, h = h_i$, and $g = p^e$, and initialize $x_0 = 0$, and let $\gamma = g^{p^{e-1}}$, then for all $k \in [0, e-1]$, $h_k = (g^{-x_k} h)^{p^{e-1-k}}$, notice that the order of element divides p, so $h_k \in \gamma$. Lastly, calculate d_k such that $\gamma^{d_k} = h_k$ and let $x_{k+1} = x_k + d_k p^k$, and get $x = x_e$
After getting all x_i, we can use chinese remainder theorem to solve $x \equiv x_i \mod p_i^{e_i}$ such that $i \in [1, r]$, and get $x = log_g h$
For example, we calculate $3^x \equiv 3344 \mod 24389$. $24389 = 29^3$, and we can get the order $n = 28 * 29^2 = 2^2 * 7 * 29^2$
Since 3 is a generator of G, we can get:

$$\begin{aligned}
g_1 &\equiv 10133 \mod 24389 \\
h_1 &\equiv 24388 \mod 24389 \\
g_2 &\equiv 7302 \mod 24389 \\
h_2 &\equiv 4850 \mod 24389 \\
g_3 &\equiv 11369 \mod 24389 \\
h_3 &\equiv 23114 \mod 24389
\end{aligned}$$

For p=2,e=2, g=10133, h=24388, we can get $x_a = 2 \mod 4$
For p=7,e=1, g=7302, h=4850, we can get $x_b = 2 \mod 7$
For p=29,e=2, g=11369, h=23114, we can get $x_c = 260 \mod 841$
And we can use Chinese Remainder theorem to get:
$x \equiv 2 \mod 28$
$x \equiv 260 \mod 841$
$x \equiv 841 * 1 * 2 + 28 * 811 * 260 \equiv 18762 \mod 23548$

Problem 3

1.
Prove by contradiction: Suppose polynomial X^3+2X^2+1 is reducible over $F_3[x]$ $X^3+2X^2+1=(X^2+AX+B)(X+C)=X^3+(A+C)X^2+(AC+B)X+BC$.
There are only two pairs of (B,C): (1,1) and (2,2) which make BC=1.
If B=C=1, then A=-1, then it's wrong.
If B=C=2, then A=2, then it's wrong.
So polynomial is irreducible over $F_3[x]$
Since X^3+2X^2+1 is an irreducible polynomial of degree three in $F_3[x]$, and F_3^3 is the set such that all the polynomial of degree smaller than 3 in $F_3[x]$, so $F_3^3[x]$ is finite set with 27 elements.
2.
We define a map $x \leftrightarrow f(x)$, and x symbolizes 26 English letters a,b,c,d.... And the relationship is $a \leftrightarrow 1$, $b \leftrightarrow 2$,......$z \leftrightarrow 26$.
Let $P(X)=X^3+2X^2+1$, we can calculate:
$X^1 \equiv X \mod P(X)$
$X^2 \equiv X^2 \mod P(X)$
$X^3 \equiv X^2+2 \mod P(X)$
......(omit)
$X^{26} \equiv 1 \mod P(X)$
X can generate every elements in $F_3^3[X]$, so X is a generator of $F_3^3[X]$.
So we can define the map as: $x \rightarrow g(x)(g(x)=X^{f(x)} \mod P(X))$
3. The order of the subgroup generated by X is 26 (see previous part).
4.
Let X be the generator and 11 is the secret key.
$X^11 \equiv X+2 \mod P(X)$
The public key is X+2.
5.
We first map "goodmorning" into F_3^3 and we can get: $X^2+1, 2X^2, 2X^2, X2+2X2, 2, 2X^2, X+1, 2X, 2X^2+2X+2, 2X, X^2+1$. And we can encrypt plaintext m through the equation $c \equiv \beta^{18}m \equiv (X+2)^{18}m \mod P(X)$, then we map the result back to letter we can get ciphertext c: "saapyadzuzs". Then we use $m \equiv tr^{-x} \equiv t(X+1)^{-11} \mod P(X)$ to get $X^2+1, 2X^2, 2X^2, X2+2X2, 2, 2X^2, X+1, 2X, 2X^2+2X+2, 2X, X^2+1$, and map the result back to plaintext.

Problem 4

1.
(i)pre-image resistant
Yes, it is pre-image resistant. If we know $y=h(x) \equiv x^2 \mod pq$, We can compute $x^2 \equiv y \mod p$ and $x^2 \equiv y \mod q$ and apply Chinese remainder theorem to get $x^2 \equiv y \mod pq$, and we can get x. But factoriztion of n is hard since p,q are two big prime integers. So it's pre-image resistant.
(ii)second pre-image resistant
No, it's not second pre-image resistant., if we know x, we can find x'=-x such that $h(x)=h(x')=x^2 \mod p$.
(iii)collision resistant
No, it's not collision resistant, we can find any x,x' such that x'=-x, and $h(x)=h(x')=x^2 \mod p$
2.
(i)efficiently computed
Yes, it can be efficiently computed. Any message n can be seperated into blocks of 160 bits and pass through xor.

(ii)pre-image resistant
No, it's not pre-image resistant. If we have y, then we can find x=y such that h(x)=x=y.
(iii)second pre-image resistant
No, it's not second pre-image resistant. If we have x, we can find x'=x+160bits 0 such that h(x)=h(x') (anything xor with 0 is itself).
(iv)collision resistant
No, it's not collision resistant, we can find any x,x' such that x'=x+160bits 0, and h(x)=h(x') (anything xor with 0 is itself).

Problem 5

next time homework

Problem 6

programming homework