Xinyi Wu (5133709030)
UM-JI Joint Institude
Shanghai Jiao Tong University

July 5,2016

HOMEWORK VI — Ve475

Exercise 1

1)

a) We have p is a prime, therefore $gcd(\alpha, p) = 1$, so by Euler Formula we have

$$\alpha^r \equiv \alpha^{r(mod\ p-1)}\alpha^{k\cdot p} \equiv \alpha^{r(mod\ p-1)}(mod\ p-1)$$

where $k \in \mathbb{Z}$. To simplify the question we want all the result Bob gives back to Alice to be within $\mathbb{Z}_p$, therefore it's better to use x or x+r $mod\ p-1$.

b)On one hand, since Bob don't know Alice request r or $x+r$ and he can't simultaneously get x and $x+r$ unless he knows how to calculate $\log_\alpha \beta$. So Bob can't cheat. On the other hand, each time Alice can't know x and $x+r$ simultaneously, so she can't know x. Therefore Alice also can't cheat.

2)

No difference. Trivial. Usually repeat 5 to 6 times until Alice can ensure Bob.

3)

Zero Knowledge Proof Protocol

Exercise 2

1)

First how to perform the Pohlig-Hellman Algorithm:

i) Prime factorization of $\varphi(p) = p_1 p_2 \cdots p_n$

ii) Calculate with the formula:

$$\begin{aligned} e^{\varphi p/p_1} \equiv & (g^x)^{\varphi(p)/p_1}\ (mod\ p) \\ \equiv & (g^{\varphi(p)})^{\alpha_1} g^{b_1\varphi(p)/p_1}\ (mod\ p) \\ \equiv & (g^{\varphi(p)/p_1})^{b_1}\ (mod\ p) \end{aligned}$$

iii) Same operation from p_2 to p_n

iv) With b_i known we know the answer by Chinese Remainder Theorem.

Then we try to do the problem, first

$$\varphi(24389) = 23548 = 2^2 \times 7 \times 29^2$$

①: Assume $\log_3 3344 \equiv c_0 + 2c_1 (mod\ 4)$ where c_0 and c_1 are binary digits.

Then

$$3344^{\frac{p-1}{2}} \equiv 1\ (mod\ 24389) \Rightarrow c_0 = 0$$

Then

$$3344^{\frac{p-1}{4}} \equiv -1\ (mod\ 24389) \Rightarrow c_1 = 1$$

So

$$\log_3 3344 (mod\ 24389) \equiv 2\ (mod\ 4)$$

②: Assume $\log_3 3344 \equiv d_0 (mod\ 7)$ where d_0 are positive integers that are less than 8.

Then

$$3344^{\frac{p-1}{7}} \equiv 4850 \equiv 3^{2 \cdot \frac{p-1}{7}}\ (mod\ 24389)\ \Rightarrow d_0 = 2$$

So

$$\log_3 3344 (mod\ 24389) \equiv 2\ (mod\ 7)$$

③: Assume $\log_3 3344 \equiv e_0 + 29e_1 (mod\ 4)$ where e_0 and e_1 are positive integers that are less than 30.

Then

$$3344^{\frac{p-1}{29}} \equiv 11775 \equiv 3^{28 \cdot \frac{p-1}{29}}\ (mod\ 24389)\ \Rightarrow e_0 = 28$$

Since $8130 \times 3 \equiv 1\ (mod\ 24389)$, so we get $3344 \times 8130^{28} \equiv 6998\ (mod\ 24389)$

Then

$$6998^{\frac{p-1}{841}} \equiv 3365\ 3^{8 \times \frac{p-1}{841}} (mod\ 24389) \Rightarrow c_1 = 1$$

So

$$\log_3 3344 (mod\ 24389) \equiv 8 \times 29 + 28 \equiv 860\ (mod\ 24389)$$

We combine the first two equations to

$$\log_3 3344 (mod\ 24389) \equiv 2 (mod\ 28)$$

With Chinese remainder theorem we have:

$$\log_3 3344 (mod\ 24389) \equiv 2 \times 841 \times 1 + 811 \times 28 \times 260 \equiv 18762\ (mod\ 23548)$$

Exercise 3

1)

Assume $X^3 + 2X^2 + 1$ is not irreducible, therefore assume

$$X^3 + 2X^2 + 1 \equiv (aX^2 + bX + c)(dX + e)$$

Therefore we have

$$\begin{cases} a \cdot d \equiv 1\ (mod\ 3) \\ c \cdot e \equiv 1\ (mod\ 3) \\ a \cdot e + b \cdot d \equiv 2\ (mod\ 3) \\ b \cdot e + c \cdot d \equiv 0\ (mod\ 3) \end{cases}$$

To solve the equation first we have $a = d$ and $c = e$, then the equation becomes

$$\begin{cases} a \cdot c + b \cdot a \equiv 2 \ (mod\ 3) \\ b \cdot c + c \cdot a \equiv 0 \ (mod\ 3) \end{cases}$$

There's no solution, so $X^3 + 2X^2 + 1$ is irreducible over $\mathbb{F}_{3^3}$. Since the degree $3 \geq 3$, it defines $\mathbb{F}_{3^3}$, that has $3^3 = 27$ elements.

2)

Since except 0, which is non invertible in $\mathbb{F}_{3^3}$, we have 26 elements. We can therefore construct a bijective reflection with the 26 characters in the alphabet. We can therefore define a simple map from the set of letters into $\mathbb{F}_{3^3}$.

3)

We write all the X^i generated from X , where $i \in \mathbb{A}$, and $1 \leq i \leq 27$: $\{x, x^2, x^2+2, x^2+2x+2, 2x+2, 2x^2+2x, x^2+1, x^2+x+2, 2x^2+2x+2, x^2+2x+1, x+2, x^2+2x, 2, 2x, 2x^2, 2x^2+1, 2x^2+x+1, x+1, x^2+x, 2x^2+2, 2x^2+2x+1, x^2+x+1, 2x^2+x+2, 2x+1, 2x^2+x, 1\}$

Therefore x has order of 27

4)

Since $x^{11} \equiv x + 2 \ (mod\ x^3 + 2x^2 + 1)$, so the plain text is 12.

5)

The plain text correspond to $\{X^7X^{15}X^{15}X^4X^{13}X^{15}X^{18}X^{14}X^9X^{14}X^7\}$ Then the decrypted text is $X^{7+11\ (mod\ 26)}X^{15+11\ (mod\ 26)}X^{15+11\ (mod\ 26)}X^{4+11\ (mod\ 26)}X^{13+11\ (mod\ 26)}$ $X^{15+11\ (mod\ 26)}X^{18+11\ (mod\ 26)}X^{14+11\ (mod\ 26)}X^{9+11\ (mod\ 26)}X^{14+11\ (mod\ 26)}X^{7+11\ (mod\ 26)}$ Which is $\{X^{18}X^{26}X^{26}X^{15}X^{24}X^{26}X^3X^{25}X^{20}X^{25}X^{18}\}$ which is $rzzoxzcytyr$, The decryption process is $\{X^{18-11\ (mod\ 26)}X^{26-11\ (mod\ 26)}X^{26-11\ (mod\ 26)}X^{15-11\ (mod\ 26)}X^{24-11\ (mod\ 26)}$ $X^{26-11\ (mod\ 26)}X^{3-11\ (mod\ 26)}X^{25-11\ (mod\ 26)}X^{20-11\ (mod\ 26)}X^{25-11\ (mod\ 26)}X^{18-11\ (mod\ 26)}\}$ which is *godmorning*.

Exercise 4

1)

Not pre-image resistant, since it needs big prime factorization which is very hard.

But second pre-image resistant and collision resistant, since $(x)^2 \equiv (n + x)^2 \ (mod\ n)$

2)

1)pre image, since we can always find

$$h(m) \equiv 0 \oplus 0 \oplus 0 \cdots m_l$$

where $m = m_l$ and all the other are 0.

Exercise 5

1)

Prove by contradiction: assume there are $x_1 \neq x_2$ such that $h(x_1) = h(x_2)$, then we have

2)

Otherwise the decompression may result in multiple different outcomes, so the compression failed.

3)

Submitted by Xinyi Wu (5133709030) on July 5,2016.