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

June 27,2016

HOMEWORK V — Ve475

Exercise 1

1)

If m is not coprime with n, since $n = p \times q$, we know that m can only be $m = p^k q^l$, where $m, l \in \mathbb{N}^+$. There is little probability to have m like this (less than $\dfrac{\log_p n \log_q n}{n}$). So it's not like for n to be coprime with m.

2)

a) By Euler theorem:

$$m^k \equiv m^{\varphi(n)} \equiv 1(mod\ n)$$

Since $gcd(m^{\varphi(n)}, n) = 1$, and $p|n$, $q|n$, then

$$m^{\varphi(n)} \equiv 1(mod\ p)\ and\ (mod\ q)$$

b) Since

$$m^{k+1} \equiv m(mod\ p)\ and\ (mod\ q) \Leftarrow m^{k+1} \equiv m(mod\ p) \Leftrightarrow n|m(m^k - 1)$$

① If $gcd(m, n) = 1$, from the proof of the previous question we know this is proved.
② If $n|m$, then $n|m(m^k - 1)$, so this proved.
③ If $m = p^t$ where $t \in \mathbb{Z}^+$. Then $gcd(n, m) = p$. Moreover $gcd(m, q) = 1$,then $m^k = (m^{(q-1)})^{p-1} \equiv 1^{p-1} \equiv 1(mod\ q)$, so $gcd(m^k - 1, q) = q$, therefore $n|m(m^k - 1)$ and we proved the result.
④ If $m = q^t$ where $t \in \mathbb{Z}^+$, the proof is similar to ③.

3)

a) By definition we have $ed \equiv 1(mod\ \varphi(n))$, therefore from previous proof we have $m^{ed} \equiv m(mod\ n)$.
b) If $gcd(m, n)! = 1$, then m are possible for all integers and therefore can't be recovered.

Exercise 2

The prime factorization of 11413 is $11413 = 101 \times 113$.
We want to find d, note that $7467 \times 3 \equiv 1(mod\ 11200)$, we can get $d = 3$.
The plain text $m \equiv 5859^3 \equiv 1415(mod\ 11200)$
So the plain text is 1415.

Exercise 3

1)

Since both encryption and decryption needs modular exponentiation, it's easier to perform exponentiation is the encryption keys or the decryption keys are short.

2)

Cited from wikipedia:

How Wiener's attack works [edit]

Since

$$ed \equiv 1 (\bmod \ \operatorname{lcm}(p-1, q-1)),$$

there exists an integer K such that

$$ed = K \times \operatorname{lcm}(p-1, q-1) + 1$$

Define $G = \gcd(p-1, q-1)$ to be substituted in the equation above which gives:

$$ed = \frac{K}{G}(p-1)(q-1) + 1$$

Defining $k = \frac{K}{\gcd(K, G)}$ and $g = \frac{G}{\gcd(K, G)}$, and substituting into the above gives:

$$ed = \frac{k}{g}(p-1)(q-1) + 1.$$

Divided by dpq:

$$\frac{e}{pq} = \frac{k}{dg}(1-\delta), \text{ where } \delta = \frac{p+q-1-\frac{g}{k}}{pq}.$$

So, $\frac{e}{pq}$ is slightly smaller than $\frac{k}{dg}$, and the former is composed entirely of public information. However, a method of checking a guess is still required. Assuming that $ed > pq$ (a reasonable assumption unless G is large) the last equation above may be written as:

$$edg = k.(p-1)(q-1) + g$$

By using simple algebraic manipulations and identities, a guess can be checked for accuracy. [1]

3)

It's trivial.

4)

First $\langle N, e \rangle = \langle 317940011, 77537081 \rangle$

The continued fraction is

$$\frac{e}{N} = \frac{77537081}{317940011} = [0, 4, 9, 1, 19, 1, 1, 15, 3, 2, 3, 71, 3, 2]$$

Therefore

$$\frac{k}{d} = 0, \frac{1}{4}, \frac{9}{37}, \frac{10}{41}, \frac{199}{816}, \frac{209}{857}, \frac{408}{1673}, \frac{199}{816}, \frac{6329}{25952}, \frac{19395}{79529}, \frac{45119}{185010}, \frac{154752}{634559}, \frac{33252285}{136350656}, \frac{77537081}{317940011}$$

Proceed testing:

1: the convergent $\frac{1}{4}$ yields,

$$\varphi(N) = \frac{e \cdot d - 1}{k} = \frac{77537081 \times 4 - 1}{1} = 310148323$$

We need to solve the equation is :

$$x^2 - (317940011 - 77537081 + 1)x + 317940011 = 0$$

x is not integer $\{\{x \to 1.32253\}, \{x \to 2.40403 \times 10^8\}\}$.

②: the convergent $\dfrac{9}{37}$ yields,

$$\varphi(N) = \frac{e \cdot d - 1}{k} = \frac{77537081 \times 37 - 1}{9} = \frac{2868871996}{9}$$

Not a integer.

③: the convergent $\dfrac{10}{41}$ yields,

$$\varphi(N) = \frac{e \cdot d - 1}{k} = \frac{77537081 \times 41 - 1}{10} = 317902032$$

We need to solve the equation is :

$$x^2 - (317940011 - 317902032 + 1)x + 317940011 = 0$$

x is integer $\{\{x \to 12457\}, \{x \to 25523\}\}$.

$N = 317940011 = 12457 \times 25523 = p \times q$.

Exercise 5

1)

We will use the Choose Cipher-text Attack(CPA). Since $2^e c \equiv (2m)^e (mod\ n)$,we know by input the $2^e c$ we can get the coordinate plain-text 2m. Then we can get the plaintext m by dividing 2 modulo n.

2)

Not adding any securities. Assume the encryption keys are e_1 and e_2 ,then after two encryption we have $m^{e_1 e_2} \equiv c(mod\ n)$. Since e_1 and e_2 are both coprime with n, then $e_1 e_2$ is coprime with n. Therefore it equals to a single encryption and not add any securities.

3)

Incorporate the first equation into the second one:

$$187722^2 \equiv (2 \cdot 516107)^2 (mod\ 642401)$$

since 2 is coprime with n, then

$$93861 \equiv (516107)^2 (mod\ 642401)$$

Therefore we have

$$642401 \mid (516107 + 93861)(516107 - 93861) \Rightarrow 642401 \mid 609968 \times 422246$$

We want to find the gcd of them with Euclidean algorithm:

$$\begin{aligned}642401 =&1 \times 609968 + 32433\\609968 =&18 \times 32433 + 26174\\32433 =&1 \times 26714 + 6259\\26714 =&4 \times 6259 + 1138\\6259 =&5 \times 1138 + 569\\1138 =&2 \times 569\end{aligned}$$

Therefore $gcd(642401, 609968) = 569$.

Furthermore

$$\begin{aligned}642401 =&1 \times 422246 + 220155\\422246 =&1 \times 220155 + 202091\\220155 =&1 \times 202091 + 18064\\202091 =&11 \times 18064 + 3387\\18064 =&5 \times 3387 + 1129\\3387 =&3 \times 1129\end{aligned}$$

Therefore $gcd(642401, 422246) = 1129$.

Therefore $642401 = 569 \times 1129$

4)

Firstly calculate $\varphi(n) = (p-1)(q-1)(r-1)$, then find an encryption key e that $gcd(e, \varphi(n)) = 1$, then find a d such that d is the inverse of e modulo $\varphi(n)$. Then serve $\langle n, e\rangle$ as encryption key and $\langle n, d\rangle$ as private key.

The drawback is that its easier to find a factor of n since n has one more factor, s its easier to break the "triple RSA".

5)

We know $96 = 2^5 \times 3$.

By the properties of generator we have

$$\alpha\ is\ a\ generator\ of\ U(\mathbb{Z}/97\mathbb{Z}) \Leftrightarrow \alpha^{48} \not\equiv 1(mod\ 97)\ and\ \alpha^{32} \not\equiv 1(mod\ 97)$$

First we test 2:

$$\begin{aligned}2^6 &\equiv 64(mod\ 97) & 2^{12} &\equiv 122(mod\ 97)\\2^{24} &\equiv 96(mod\ 97) & 2^{48} &\equiv 1(mod\ 97)\end{aligned}$$

So 2 is not a generator, also 4 is not a generator.

Then we test 3:

$$\begin{aligned}3^3 &\equiv 27(mod\ 97) & 3^6 &\equiv 50(mod\ 97)\\3^{12} &\equiv 75(mod\ 97) & 3^{24} &\equiv 96(mod\ 97)\\3^{48} &\equiv 1(mod\ 97)\end{aligned}$$

So 3 is also not a generator.
Then we test 5:

$$5^3 \equiv 28(mod\ 97) \qquad 5^6 \equiv 8(mod\ 97)$$
$$5^{12} \equiv 64(mod\ 97) \qquad 5^{24} \equiv 22(mod\ 97)$$
$$5^{48} \equiv 96 \not\equiv 1(mod\ 97)$$

Another test:

$$5^2 \equiv 25(mod\ 97) \qquad 5^4 \equiv 43(mod\ 97)$$
$$5^8 \equiv 6(mod\ 97) \qquad 5^{16} \equiv 36(mod\ 97)$$
$$5^{32} \equiv 35 \not\equiv 1(mod\ 97)$$

Therefore 5 is the smallest generator in $U(\mathbb{Z}/97\mathbb{Z})$.

6)

a) We know $100 = 2^2 \times 5^2$.
By the properties of generator we have

$$\alpha \textit{ is a generator of } U(\mathbb{Z}/101\mathbb{Z}) \Leftrightarrow \alpha^{20} \not\equiv 1(mod\ 97) \textit{ and } \alpha^{50} \not\equiv 1(mod\ 97)$$

First we test 2:

$$2^5 \equiv 32(mod\ 101) \qquad 2^{10} \equiv 14(mod\ 101)$$
$$2^{20} \equiv 95 \not\equiv 1(mod\ 101)$$

Also the other test

$$2^5 \equiv 32(mod\ 101) \qquad 2^{25} \equiv 10(mod\ 101)$$
$$2^{50} \equiv 100 \not\equiv 1(mod\ 101)$$

So 2 is a generator in $U(\mathbb{Z}/101\mathbb{Z})$.

b) We know that $2^{69} \equiv 3(mod\ 101)$, then $2^{72} \equiv 3 \times 2^3 \equiv 24(mod\ 101)$ is non trivial. So $\log_2 24 = 72$.

c) Assume $2^x \equiv 24 \equiv 125 \equiv 5^3(mod\ 101)$.
On the other side $2^{24} \equiv 5(mod\ 101)$,therefore

$$(2^{24})^3 \equiv 5^3(mod\ 101) \Rightarrow 2^{72} \equiv 125(mod\ 101)$$

So $\log_2 24 = 72$.

7)

From the qualification $3^{6-2\cdot 10} \equiv 44/4 \equiv 11(mod\ 137)$.
Since 3 and 137 are coprime, $x = 136 + 6 - 2 \times 10 = 122$.

8)

a)The exponent calculate calculation of $6^i(mod\ 11)$ is $\{6, 3, 7, 9, 10, 5\}$, so

$$6^5 \equiv 10 \equiv -1(mod\ 11)$$

b) Since

$$2^2 \equiv 4 \not\equiv 1(mod\ 11) \qquad 2^5 \equiv 10 \not\equiv 1(mod\ 11)$$

and $10 = 2 \times 5$, we know that 2 is a generator of G.
c) By the answer of a) we have

$$(2^x)^5 \equiv 2^{5x} \equiv 6^5 \equiv -1(mod\ 11)$$

, since 2 is a generator of G, we know

$$2^{10k+5} \equiv -1(mod\ 11)$$

where k is an integer so

$$5x = 10k + 5 \Rightarrow x = 2k + 1$$

So x is an odd number.

Exercise 6

1)

We know $3^{2048} \equiv 65529(mod\ 65537)$ and $3^{4096} \equiv 64(mod\ 65537)$, also

$$\left(\frac{65529}{65537}\right) = -1\ and\ \left(\frac{65529}{65537}\right) = 1$$

Therefore 2048 divides x but 4096 does not.

2)

Since $3^{2048*27} \equiv 2(mod\ 27)$,then

$$x \equiv 27 \times 2048 \equiv 55296(mod\ 65537)$$

.

We have k an integer and $x = 65537k + 55296$.

3)

We have $65537 - 1 = 2^{16}$, also we have $x = \prod_{i=0}^{15} c_i 2^i$. The solution lies that $c_{15} = c_{14} = c_{12} = c_{11} = q$ while others are all 0. So

$$x = 2^{15} + 2^{14} + 2^{12} + 2^{11} = 55296$$

4)

A large prime whose p-1 can have many small prime factors,it's easy to factor, and easy to tactic on the DLP problem.

Submitted by Xinyi Wu (5133709030) on June 27,2016.