VE475 Homework 5

Liu Yihao 515370910207

Ex. 1 — RSA setup

1. In the RSA encryption and decryption, we use

$$ed \equiv 1 \bmod \varphi(n)$$

$$m^{ed} \equiv m \bmod \varphi(n)$$

This is based on the Euler's theorem, which has a condition that m and n be two coprime integers. So it is likely for n to be coprime with m.

2. Suppose $k = a\varphi(n)$, $a \in N^*$, and $m < n$.

(a)

$$\begin{aligned} m^k &\equiv (m^{\varphi(n)})^a \bmod n \\ &\equiv 1^a \bmod n \\ &\equiv 1 \bmod n \end{aligned}$$

So

$$m^k \equiv 1 \bmod p \quad \text{and} \quad m^k \equiv 1 \bmod q$$

(b) First, if $\gcd(m, n) = 1$, according to (a), it's obvious that

$$m^{k+1} \equiv m \bmod p \quad \text{and} \quad m^{k+1} \equiv m \bmod q$$

Second, if $\gcd(m, n) = p$, so $\gcd(m/p, q) = 1$

$$\begin{aligned} m^{k+1} &\equiv p\left[\left(\frac{m}{p}\right)^{k+1} \bmod q\right] \bmod n \\ &\equiv p\left[\left(\frac{m}{p}\right)^{a(p-1)\varphi(q)+1} \bmod q\right] \bmod n \\ &\equiv p \cdot \frac{m}{p} \bmod n \\ &\equiv m \bmod n \end{aligned}$$

So

$$m^{k+1} \equiv m \bmod p \quad \text{and} \quad m^{k+1} \equiv m \bmod q$$

Third, if $\gcd(m, n) = q$, it is similar to the second case.
We can conclude that for any arbitrary m, $m^{k+1} \equiv m \bmod p$ and mod q.

3. (a) We know that $ed \equiv 1 \bmod \varphi(n)$, which means that $ed = k+1$ where k is a multiple of $\varphi(n)$. According to part 2(b), we know that for any arbitrary m, $m^{k+1} \equiv m \bmod p$ and mod q, or we can say $m^{k+1} \equiv m \bmod n$, so $m^{ed} \equiv m \bmod n$,

   (b) From the previous calculation, we can find that for all $m < n$, no matter m and n are coprime or not, we can both find that $m^{ed} \equiv m \bmod n$, so that the RSA encryption and decryption can be performed. So we can conclude that it is not necessary that $\gcd(m, n) = 1$.

Ex. 2 — RSA decryption

$$n = 11413 = 101 \times 113$$

So we can find that $p = 101$ and $q = 113$, so $\varphi(n) = 11200$, and we should calculate d so that $ed \equiv 1 \bmod \varphi(n)$.

By applying the extended euclidean algorithm,

	q_i	r_i	s_i
0		7467	1
1		11200	0
2	$7467 \div 11200 = 0$	$7467 - 0 \times 11200 = 7467$	$1 - 0 \times 0 = 1$
3	$11200 \div 7467 = 1$	$11200 - 1 \times 7467 = 3733$	$0 - 1 \times 1 = -1$
4	$7467 \div 3733 = 2$	$7467 - 2 \times 3733 = 1$	$1 - 2 \times -1 = 3$

$$e \cdot 3 \equiv 1 \bmod \varphi(n)$$

So $d = 3$, then we can apply modulo exponentiation to the equation

$$m \equiv c^d \bmod n$$

i	d_i	power mod 11413
1	1	$1^2 \cdot 5859 \equiv 5859$
0	1	$5859^2 \cdot 5859 \equiv 1415$

So $m = 1415$.

Ex. 3 — Breaking RSA

1. When we decrypt an RSA ciphertext, we use $m \equiv c^d \bmod n$. When d is small, the decryption speed will be faster, so one would select short encryption or decryption keys.

2.
$$ed \equiv 1 \bmod \operatorname{lcm}(p-1, q-1)$$
$$ed = K \cdot \operatorname{lcm}(p-1, q-1) + 1, K \in N$$

   Suppose $G = \gcd(p-1, q-1)$, we can find

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

Let $k = \dfrac{K}{\gcd(K,G)}$, $g = \dfrac{G}{\gcd(K,G)}$,

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

$$\frac{e}{pq} = \frac{k}{dg}(1-\lambda), \lambda = \frac{p+q-1-g/k}{pq}$$

Since $p \approx q \gg 0$, λ would be very small, then $\dfrac{e}{pq}$ is slightly smaller than $\dfrac{k}{dg}$, and

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

Let $k_0 = \dfrac{k}{g}$ we can find

$$\varphi(n) = (p-1)(q-1) = \frac{ed-1}{k_0}$$

where $\dfrac{k_0}{d}$ converges to $\dfrac{e}{n}$.
Then we can apply continued fractions to get a list of approximate of k_0 and d, validate them and get the right d if it is small enough by the equation

$$x^2 - pq + n = 0$$

$$x^2 - (n - \varphi(n) + 1) + n = 0$$

$$p, q = \frac{n - \varphi(n) + 1 \pm \sqrt{(n-\varphi(n)+1)^2 - 4n}}{2}$$

3. According to Wiener's theorem, decryption key should be larger than $\dfrac{1}{3}n^{1/4}$. For security considerations, it should be randomly selected from the safe range.

4. We apply continued fraction to n and e and get the following table:

i	a	k_0	d
0	0	0	1
1	4	1	4
2	9	9	37
3	1	10	41
4	19	199	816
5	1	209	857
6	1	408	1673
7	15	6329	25952
8	3	19395	79529
9	2	45119	185010
10	3	154752	634559
11	71	11032511	45238699
12	3	33252285	136350656
13	2	77537081	317940011

According to Wiener's theorem, $d < \dfrac{1}{3}n^{1/4} < 45$, so we can try data from $i = 1, 2$.

First we can guess that $k_0 = 1$, $d = 4$,

$$\phi(n) = \frac{ed - 1}{k_0} = 310148323$$

$$n - \varphi(n) + 1 = 7791689$$

$$(n - \varphi(n) + 1)^2 - 4n = 60709145712677$$

It is not a square number, so d is wrong.

Second we can guess that $k_0 = 9$, $d = 37$,

$$\phi(n) = \frac{ed - 1}{k_0} = \frac{2868871996}{9}$$

It is not a integer, so d is wrong.

Third, we can guess that $k_0 = 10$, $d = 41$,

$$\phi(n) = \frac{ed - 1}{k_0} = 317902032$$

$$n - \varphi(n) + 1 = 37980$$

$$(n - \varphi(n) + 1)^2 - 4n = 170720356 = 13066^2$$

$$p = \frac{37980 + 13066}{2} = 25523$$

$$q = \frac{37980 - 13066}{2} = 12457$$

$$n = 317940011 = 25523 \times 12457$$

Ex. 4 — Programming

In the ex3 folder, with a README file inside it.

Ex. 5 — Simple Questions

1. We can calculate $c \cdot 2^e \bmod n$, and it equals to $2m \bmod n$. Since n is odd, if $2m \bmod n$ is even, $m = \dfrac{2m \bmod n}{2}$; if $2m \bmod n$ is odd, $m = \dfrac{(2m \bmod n) + n}{2}$.
2. No, it doesn't. Because the RSA problem is actually a factorization problem. If the attacker succeeded in factoring n, no matter how many exponents are chosen, the decryption method is the same.

3.

$$4 \cdot 516107^2 - 187722^2 \equiv 0 \text{ mod } n$$

$$(2 \cdot 516107 - 187722)(2 \cdot 516107 + 187722) \equiv 0 \text{ mod } n$$

$$1219936 \cdot 844492 \equiv 0 \text{ mod } n$$

$$64866 \cdot 844492 \equiv 0 \text{ mod } n$$

$$2 \cdot 3 \cdot 10811 \cdot 2^2 \cdot 211123 \equiv 0 \text{ mod } n$$

We can find that 64866 must have a factor of n since $211123 < n$ (suppose n have only two factors according to RSA), and the factorization of 10811 is easy since it's small enough. We can try the primes smaller than $\sqrt{10811}(< 104)$ and find that it has a factor 19. Then we can deduce that $10811 = 19 \times 569$, where 569 is also a prime.

At last we can take 3, 19 and 569 as the possible factors of n, validate them and conclude that

$$n = 642401 = 569 \times 1129$$

4. Thus

$$\varphi(n) = (p-1)(q-1)(r-1)$$

And we should also find e and d such that

$$ed \equiv 1 \text{ mod } \varphi(n)$$

Then

$$c \equiv m^e \text{ mod } n$$

$$c^d \equiv m^{ed} \equiv m^{\varphi(n)+1} \equiv m \text{ mod } n$$

However, if we use the same bits length of n with three prime factors instead of two, the length of each factor will become shorter, so the factorization can be more efficient, and the security is poorer.

5.

$$(97-1) = 96 = 2^5 \times 3$$

So the generator x should satisfy that

$$x^{32} \neq 1 \text{ mod } 97 \quad \text{and} \quad x^{48} \neq 1 \text{ mod } 97$$

$$x^{16} \neq \pm 1, 35, 61 \text{ mod } 97$$

We can find that

$$2^{16} \equiv 61 \text{ mod } 97$$
$$3^{16} \equiv 61 \text{ mod } 97$$
$$4^{16} \equiv 1 \text{ mod } 97$$
$$5^{16} \equiv 36 \text{ mod } 97$$

So the smallest generator of $U(Z/97Z)$ is 5.

6. (a)

$$101 - 1 = 100 = 2^2 \times 5^2$$

$$\begin{aligned} 2^{100/2} &\equiv (2^{10})^5 \bmod 101 \\ &\equiv 14^5 \bmod 101 \\ &\equiv 100 \bmod 101 \\ 2^{100/5} &\equiv (2^{10})^2 \bmod 101 \\ &\equiv 14^2 \bmod 101 \\ &\equiv 95 \bmod 101 \end{aligned}$$

Since $2^{50} \not\equiv 1 \bmod 101$ and $2^{20} \not\equiv 1 \bmod 101$, 2 is a generator of G.

(b)

$$\log_2 2 = 1$$

$$\log_2 24 = \log_2 3 + 3\log_2 2 = 72$$

(c)

$$\log_2 24 = \log_2 125 = 3\log_2 5 = 72$$

7.

$$(137 - 1) = 136 = 2^3 \times 17$$

$$\begin{aligned} 3^{136/2} &\equiv 3^5 \cdot (3^7)^9 \bmod 137 \\ &\equiv 243 \cdot (-5)^9 \bmod 137 \\ &\equiv 106 \cdot 12^3 \bmod 137 \\ &\equiv 106 \cdot 7 \cdot 12 \bmod 137 \\ &\equiv 136 \bmod 137 \\ 3^{136/17} &\equiv 3^8 \bmod 137 \\ &\equiv 3 \cdot -5 \bmod 137 \\ &\equiv 122 \bmod 137 \end{aligned}$$

Since $3^{68} \not\equiv 1 \bmod 137$ and $3^8 \not\equiv 1 \bmod 137$, 3 is a generator of $U(Z/137Z)$.

$$\log_3 44 = 6$$

$$\log_3 2 = 10$$

$$\log_3 11 = \log_3 44 - 2\log_3 2 = -14$$

So $x = 122$.

8. (a)

$$6^5 \equiv 10 \bmod 11$$

So $6^5 = 10$ in $U(Z/11Z)$

(b)

$$(11-1) = 10 = 2 \times 5$$
$$2^{10/2} \equiv 10 \bmod 11$$
$$2^{10/5} \equiv 4 \bmod 11$$

Since $2^5 \not\equiv 1 \bmod 11$ and $2^2 \not\equiv 1 \bmod 11$, 2 is a generator of G.

(c)

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

So we can find that x is odd.

Ex. 6 — DLP

1.

$$3^x \equiv 2 \bmod 65537$$
$$3^{16x} \equiv -1 \bmod 65537$$
$$3^{32x} \equiv 1 \bmod 65537$$

And we also know

$$3^{65536} \equiv 1 \bmod 65537$$

So $65536 \mid 32x$ and $65536 \nmid 16x$, which means $2048 \mid x$ and $4096 \nmid x$.

2. x can be $2048(2k+1)$, where $k = 0, 1, \ldots, 15$, so there are 16 possible choices.

First we determine $3^{2048} \bmod 65537$ and $3^{63488} \bmod 65537$

i	d_i	power mod 65537
11	1	$1^2 \cdot 3 \equiv 3$
10	0	$3^2 \equiv 9$
9	0	$9^2 \equiv 81$
8	0	$81^2 \equiv 6561$
7	0	$6561^2 \equiv 54449$
6	0	$54449^2 \equiv 61869$
5	0	$61869^2 \equiv 19139$
4	0	$19139^2 \equiv 15028$
3	0	$15028^2 \equiv 282$
2	0	$282^2 \equiv 13987$
1	0	$13987^2 \equiv 8224$
0	0	$8224^2 \equiv 65529$

i	d_i	power mod 65537
15	1	$1^2 \cdot 3 \equiv 3$
14	1	$3^2 \cdot 3 \equiv 27$
13	1	$27^2 \cdot 3 \equiv 2187$
12	1	$2187^2 \cdot 3 \equiv 61841$
11	1	$61841^2 \cdot 3 \equiv 20623$
10	0	$20623^2 \equiv 38536$
9	0	$38536^2 \equiv 20413$
8	0	$20413^2 \equiv 6323$
7	0	$6323^2 \equiv 2759$
6	0	$2759^2 \equiv 9789$
5	0	$9789^2 \equiv 9427$
4	0	$9427^2 \equiv 157$
3	0	$157^2 \equiv 24649$
2	0	$24649^2 \equiv 45211$
1	0	$45211^2 \equiv 1028$
0	0	$1028^2 \equiv 8192$

$$3^{2048} \equiv -8 \bmod 65537$$
$$3^{2048\cdot 31} \equiv 8192 \bmod 65537$$
$$3^{2048\cdot(31-4)} \equiv 2 \bmod 65537$$

So $x = 2048 \cdot 27 = 55296$.

3. From Part 1, we know $x \mid 2048$ and $x \nmid 4096$, so we can set

$$x = 2^{11} + a_{12}2^{12} + a_{13}2^{13} + a_{14}2^{14} + a_{15}2^{15}$$

Then we can apply the Pohlig-Hellman algorithm.

For a_{12},

$$\left(\frac{3^x}{3^{2^{11}}}\right)^{2^{15-12}} \equiv (2^{14})^8 \equiv -1 \bmod 65537, \quad a_{12} = 1$$

For a_{13},

$$\left(\frac{3^x}{3^{2^{11}+2^{12}}}\right)^{2^{15-13}} \equiv (2^8)^4 \equiv 1 \bmod 65537, \quad a_{13} = 0$$

For a_{14},

$$\left(\frac{3^x}{3^{2^{11}+2^{12}}}\right)^{2^{15-14}} \equiv (2^8)^2 \equiv -1 \bmod 65537, \quad a_{14} = 1$$

For a_{15},

$$\left(\frac{3^x}{3^{2^{11}+2^{12}+2^{14}}}\right)^{2^{15-14}} \equiv -1 \bmod 65537, \quad a_{15} = 1$$

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

4. 65537 is a prime and is in the form $p^k + 1$. Suppose we can make $c^x \equiv p \bmod p^k + 1$, in order to find x for this kind of prime, we can first determine a generator of it, which is quite easy. And since $c^{2k} \equiv p^{2k} \equiv 1 \bmod p^k + 1$, we can find $p^k/2k \mid x$ and $p^k/k \nmid x$, and there are only k possible choices for x, which makes the decryption much more easier. So such primes are not fitting a cryptography context.