# VE475 Intro to Cryptography Homework 4

Taoyue Xia, 518370910087

2021/06/16

## Ex1—-RSA setup

1. In RSA encryption and decryption, we first choose two different primes $p$ and $q$, and calculate their product $n$ and $\varphi(n)$.

   Then choose an integer $e$ that is coprime with $\varphi(n)$, and use the extended Euclidean algorithm to find the multiplication inverse $d$ so that:

   $$ed \equiv 1 \; mod \; \varphi(n)$$

   Thus for some integer $k$, we can describe $ed$ as $ed = k\varphi(n) + 1$ Then for $c \equiv m^e \; mod \; n$, we can calculate:

   $$c^d \equiv (m^e)^d \equiv m^{k\varphi(n)+1} \equiv m \cdot m^{k\varphi(n)} \; mod \; n$$

   As we know that $c^d \equiv m \; mod \; n$, we can easily deduce that $m^{k\varphi(n)} \equiv 1 \; mod \; n$. According to Euler's Theorem, this formula is equivalent to $m$ is coprime with $n$. Therefore, it is likely for $n$ to be coprime with $m$.

2. As $k$ is a multiple of $\varphi(n)$, let $k = a\varphi(n)$, $a$ is some positive integer. Then:

   (a)

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

   As $n = pq$, we can get $m^k \equiv 1 \; mod \; pq$. Since $p$ and $q$ are primes, we can conclude:

   $$m^k \equiv 1 \; mod \; p \qquad \text{and} \qquad m^k \equiv 1 \; mod \; q$$

(b) Firstly, if $gcd(m,n) = 1$, with the conclusion in (a), we can have:

$$m^{k+1} \equiv m \cdot m^k \equiv m\ mod\ p$$

In the same way, $m^{k+1} \equiv m\ mod\ p$.

Then if $gcd(m,n) = p$, we can have $gcd(m/p, q) = 1$, thus according to (a):

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

Since $k = a\varphi(n)$, $k = a\varphi(p)\varphi(q)$, so we can get:

$$(\frac{m}{p})^k \equiv ((\frac{m}{p})^{\varphi(q)})^{a\varphi(p)} \equiv 1\ mod\ q$$

$$(\frac{m}{p})^{k+1} \equiv \frac{m}{p}\ mod\ q \equiv \frac{m}{p}\ mod\ n$$

Then we can calculate $m^{k+1}\ mod\ q$ as following:

$$\begin{aligned} m^{k+1} &\equiv p^{k+1} \cdot (\frac{m}{p})^{k+1}\ mod\ q \\ &\equiv p^k \cdot m\ mod\ q \\ &\equiv (p^{\varphi(q)})^{a\varphi(p)} \cdot m\ mod\ q \\ &\equiv m\ mod\ q \end{aligned}$$

Since $m = bp$ for some positve integer $b$,

$$m^{k+1} \equiv (bp)^{k+1} \equiv 0\ mod\ p \equiv m\ mod\ p$$

Similarly, for $gcd(m,n) = q$, we can also prove that

$$m^{k+1} \equiv m\ mod\ p \qquad \text{and} \qquad m^{k+1} \equiv m\ mod\ q$$

3. We know that $ed \equiv 1\ mod\ \varphi(n)$, then for some $k$ which is a multiple of $\varphi(n)$, $ed = k + 1$.

(a) According to the conclusion in (2),

$$m^{ed} \equiv m^{k+1} \equiv m\ mod\ p \text{ and } mod\ q$$

So we can conclude that $m^{ed} \equiv m\ mod\ n$

(b) From the above problems, we find that for any arbitrary $m$, $m^{ed} \equiv m\ mod\ n$, so it is not necessary for $gcd(m,n) = 1$.

# Ex2—-RSA decryption

For $n = 11413$, we can decompose it as two primes $p = 101$ and $q = 113$, so we can calculate $\varphi(n)$ as:

$$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = 11200$$

Then use extended Euclidean algorithm to calculate $e$'s multiplication inverse of $\varphi(n)$.

$$\begin{pmatrix} 1 & 0 & 7467 \\ 0 & 1 & 11200 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 & 1 & 11200 \\ 1 & 0 & 7467 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 7467 \\ -1 & 1 & 3733 \end{pmatrix} \Rightarrow \begin{pmatrix} -1 & 1 & 3733 \\ 3 & -2 & 1 \end{pmatrix}$$

So we find that $d = 3$. Then we can calculate $c^d \equiv m \ mod \ n$,

$$5859 \equiv 5859 \ mod \ 11413$$

$$5859 \cdot 5859 \equiv 8990 \ mod \ 11413$$

$$8990 \cdot 5859 \equiv 1415 \ mod \ 11413$$

Therefore, the plaintext is 1415.

# Ex3—-Breaking RSA

1. For RSA encryption and decryption, we calculate $c \equiv m^e \ mod \ n$ and $m \equiv c^d \ mod \ n$. If the key is short, it is faster to encrypt and decrypt, saving time for senders and receivers. Therefore, it is why one would select short encryption or decryption keys.

2. This part is referred from wikipedia.
   For $G = gcd(p-1, q-1)$, define $\lambda(n)$ as:

   $$\lambda(n) = \text{lcm}(p-1, q-1) = \frac{(p-1)(q-1)}{G} = \frac{\varphi(n)}{G}$$

   Since $ed \equiv 1 \ mod \ \varphi(n)$, it is obvious that:

   $$ed \equiv 1 \ mod \ \lambda(n)$$

   So there exist some positive integer $K$ such that:

   $$ed = K\lambda(n) + 1$$

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

Then define $k = \frac{K}{\gcd(K,G)}$ and $g = \frac{G}{\gcd(K,G)}$, we can have:

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

Divided by $dpq$, we can get:

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

It's common sense that $p$ and $q$ are very large primes, so that $\delta \to 0$. Therefore, $\frac{e}{pq}$ is just a little bit smaller than $\frac{k}{dg}$. Let $k_0 = \frac{k}{g}$, and we also have:

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

So we can deduce that:

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

After that, we can apply continued fractions to get some approximate $d$ and $k_0$. If we can find one $d$ that is quite small, we can use the above equation to calculate $\varphi(n)$. Then we need to solve the following equation to get $p$ and $q$:

$$x^2 - (p+q)x + pq = 0$$

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

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

Then $p$ and $q$ are the two roots of the equation. Note that Wiener's theorem can apply when $d < \frac{1}{3}n^{\frac{1}{4}}$.

3. In order not to generate a weak decryption key, $d$ should be larger than $\frac{1}{3}n^{\frac{1}{4}}$, where $n$ represents for the production of $p$ and $q$.

4. The code is attached in the folder *ex3*, with a readme file in it. For $n = 317940011$, we can calculate $d$ which satisfies the constraint is:

$$d < \frac{1}{3}(n)^{\frac{1}{4}} = 44.51$$

After running the code, we can find $d = 4,\ 37,\ 41$ which meet the condition. Then use the equation $\varphi(n) = \frac{ed-1}{k}$ to calculate each $\varphi(n)$. After the whole computing, we find that only $d = 41$ can result in $p, q$ which are both integers. Therefore, we conclude that $p = 25523$, $q = 12457$ is the factorization of $n = 317940011$.

## Ex4—-Programming

For details, please refer to the codes in folder ***ex4***, with a readme file in it.

## Ex5—-Simple questions

1. For some ciphertext $c$, we can calculate $c \cdot 2^e\ mod\ n$. After decryption, we can get $2m\ mod\ n$. Finally, we just need to halve the result to get the plaintext.

2. No, it doesn't. No matter how many exponents is used, if $n$ remains the same, the factorization will never change, so the attack procedure and difficulty will not change.

3. Knowing that $516107^2 \equiv 7\ mod\ n$, and $187722^2 \equiv 4 \cdot 7\ mod\ n$, we can have:

$$\begin{aligned} 4 \cdot 516107^2 - 187722^2 &\equiv 0\ mod\ n \\ (2 \cdot 516107 + 187722)(2 \cdot 516107 - 187722) &\equiv 0\ mod\ n \\ 1219936 \cdot 844492 &\equiv 0\ mod\ n \\ (2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 38123)(2 \cdot 2 \cdot 211123) &\equiv 0\ mod\ n \end{aligned}$$

   Since $n$ is the product of two odd primes, we can deduce that $38123 \cdot 211123 \equiv 0\ mod\ n$.
   $38123 = 67 \cdot 569$, $211123 = 11 \cdot 17 \cdot 1129$.
   Therefore, by trying every combination of $67,\ 569,\ 11,\ 17,\ 1129$, we can finally factorize $n$ as:

$$n = 569 \cdot 1129 = 642401$$

4. If we use $n$ which can be factorized into three prime numbers $p$, $q$ and $r$, then:

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

For a public key $e$, we should also find a private key $d$ so that:

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

$$m^{ed} \equiv m\ nod\ n$$

However, if we use $n$ to be the same number of digits as which is used for two-prime factorization, it is obvious that the three primes would be smaller, which means the factorization will be found out more efficiently.
If the three primes have the similar numbers of digits as the two-prime factorization, $n$, $e$ and $d$ would be too large, which will be very hard to solve.

5. First, we can calculate $\varphi(97) = 97 - 1 = 96 = 2^5 \cdot 3$.
So if an element $x \in U(\mathbb{Z}/97\mathbb{Z})$ is a generator, then:

$$x^{\frac{96}{2}} \equiv x^{48} \not\equiv 1\ mod\ 97$$
$$x^{\frac{96}{3}} \equiv x^{32} \not\equiv 1\ mod\ 97$$

We can easily calculate that $2^{48} \equiv 1\ mod\ 97$, $3^{48} \equiv 1\ mod\ 97$, and $4^{48} \equiv 1\ mod\ 97$.
For 5, using the modular exponentiation for $5^{48}\ mod\ 97$ as the table below:

| $i$ | $d_i$ | power mod 97 |
|---|---|---|
| 5 | 1 | $1^2 \cdot 5 \equiv 5\ mod\ 97$ |
| 4 | 1 | $5^2 \cdot 5 \equiv 28\ mod\ 97$ |
| 3 | 0 | $28^2 \equiv 8\ mod\ 97$ |
| 2 | 0 | $8^2 \equiv 64\ mod\ 97$ |
| 1 | 0 | $64^2 \equiv 22\ mod\ 97$ |
| 0 | 0 | $22^2 \equiv 96\ mod\ 97$ |

So $5^{48} \equiv 96\ mod\ 97 \not\equiv 1\ mod\ 97$.
Similarly, we can calculate $5^{32} \equiv 35\ mod\ 97$. Therefore, 5 is the smallest generator of $U(\mathbb{Z}/97\mathbb{Z})$.

6. For group $G = U(\mathbb{Z}/101\mathbb{Z})$:

(a) For $p = 101$, which is a prime, we can calculate $\varphi(p) = 101 - 1 = 100 = 2^2 \cdot 5^2$. Then if an element $x$ is a generator,

$$x^{\frac{100}{2}} \equiv x^{50} \not\equiv 1 \; mod \; 101$$

$$x^{\frac{100}{5}} \equiv x^{20} \not\equiv 1 \; mod \; 101$$

Then for the element 2, using the modular exponentiation method, we can have:

$$2^{50} \equiv 100 \; mod \; 101$$

$$2^{20} \equiv 95 \; mod \; 101$$

Therefore, we prove that 2 is a generator of $G$.

(b) Knowing that $\log_2 3 = 69$, and $\log_2 2 = 1$ we can calculate $\log_2 24$ as:

$$\begin{aligned} \log_2 24 &= \log_2(3 \cdot 8) \\ &= \log_2 3 + 3\log_2 2 \\ &= 69 + 3 = 72 \end{aligned}$$

Therefore, $\log_2 24 = 72$.

(c) Knowing that $\log_2 5 = 24$, thus:

$$\begin{aligned} \log_2 24 &= \log_2 125 \\ &= 3\log_2 5 \\ &= 3 \cdot 24 = 72 \end{aligned}$$

Therefore, $\log_2 24 = 72$.

7. First, we are going to prove that 3 is a generator of $U(\mathbb{Z}/137\mathbb{Z})$. Since $p = 137$ is a prime, we can easily calculate:

$$\varphi(p) = 137 - 1 = 136 = 2^3 \cdot 17$$

Knowing that $3^6 \equiv 44 \; mod \; 137$ and $3^{10} \equiv 2 \; mod \; 137$, thus:

$$3^{\frac{136}{2}} \equiv 3^{68} \equiv (3^6)^3 \cdot (3^10)^5 \equiv 44^3 \cdot 2^5 \equiv 136 \; mod \; 137$$

$$3^{\frac{136}{17}} \equiv 3^8 \equiv 3^6 \cdot 3^2 \equiv 44 \cdot 9 \equiv 122 \; mod \; 137$$

Therefore, 3 is a generator of $U(\mathbb{Z}/137\mathbb{Z})$.
Moreover, we can transform the expression in question as: $\log_3 44 = 6$, and $\log_3 2 = 10$. Then we need to calculate $\log_3 11$ as the equation below:

$$\begin{aligned} \log_3 11 &= \log_3(44 \div 2^2) \\ &= \log_3 44 - 2\log_3 2 \\ &= 6 - 2 * 10 = -14 \end{aligned}$$

Therefore, $x = 136 + (-14) = 122$.

8. Knowing that $G = U(\mathbb{Z}/11\mathbb{Z})$:

(a) As $6^5$ is small, we can directly calculate:

$$6^5 \equiv 7776 \equiv 10 \; mod \; 11$$

Therefore, $6^5 \equiv 10 \; mod \; 11$.

(b) Since $p = 11$ is a prime, we can calculate $\varphi(p) = 11 - 1 = 10 = 2 \cdot 5$. Then use the calculation below:

$$2^{\frac{10}{2}} \equiv 2^5 \equiv 10 \; mod \; 11$$

$$2^{\frac{10}{5}} \equiv 2^2 \equiv 4 \; mod \; 11$$

Therefore, we can see that for any prime $q$ which satisfies $q|(p-1)$, $2^{\frac{p-1}{q}} \not\equiv 1 \; mod \; 11$, so 2 is a generator of $G$.

(c)

$$\begin{aligned} 2^x &\equiv 6 \; mod \; 11 \\ (2^x)^5 &\equiv 6^5 \; mod \; 11 \\ (2^5)^x &\equiv 10 \; mod \; 11 \\ (-1)^x &\equiv -1 \; mod \; 11 \end{aligned}$$

Then we can obviously see that $x$ is odd.

# Ex6—-DLP

1. In hw4-ex5, we have proved that $3^{32768} \not\equiv 1 \; mod \; 65537$, so 3 is a generator of $U(\mathbb{Z}/65537\mathbb{Z})$, and $3^{65536} \equiv 1 \; mod \; 65537$.
   For $3^x \equiv 2 \; mod \; 65537$:
   $$(3^x)^{16} \equiv 2^{16} \equiv -1 \; mod \; 65537$$
   $$(3^x)^{32} \equiv 2^{32} \equiv 1 \; mod \; 65537$$
   Thus we can find that $65536|(32x)$ and $65536 \nmid (16x)$, which yields that:
   $$2048 \mid x \qquad \text{and} \qquad 4096 \nmid x$$
   Proof done.

2. Since $2048 \mid x$ and $4096 \nmid x$, we know that $x = 2048a$, where $a$ is an odd integer. We also know that $65536 \div 2048 = 32$, thus there are 16 possible choices of $x$.
   First, we can apply modular exponentiation method to calculate $3^{2048} \; mod \; 65537$.

| $i$ | $d_i$ | power mod 65537 |
|---|---|---|
| 11 | 1 | $1^2 \cdot 3 \equiv 3 \; mod \; 65537$ |
| 10 | 0 | $3^2 \equiv 9 \; mod \; 65537$ |
| 9 | 0 | $9^2 \equiv 81 \; mod \; 65537$ |
| 8 | 0 | $81^2 \equiv 6561 \; mod \; 65537$ |
| 7 | 0 | $6561^2 \equiv 54449 \; mod \; 65537$ |
| 6 | 0 | $54449^2 \equiv 61869 \; mod \; 65537$ |
| 5 | 0 | $61869^2 \equiv 19139 \; mod \; 65537$ |
| 4 | 0 | $19139^2 \equiv 15028 \; mod \; 65537$ |
| 3 | 0 | $15028^2 \equiv 282 \; mod \; 65537$ |
| 2 | 0 | $282^2 \equiv 13987 \; mod \; 65537$ |
| 1 | 0 | $13937^2 \equiv 8224 \; mod \; 65537$ |
| 0 | 0 | $8224^2 \equiv 65529 \; mod \; 65537$ |

   Therefore, we just need to calculate $(-8)^a \equiv 2 \; mod \; 65537$, where $a = 1, 3, \cdots, 31$.
   $$(-2)^{3a} \equiv 2 \; mod \; 65537 \Rightarrow 2^{3a} \equiv -2 \; mod \; 65537$$

We know that $2^{17} \equiv -2 \; mod \; 65537$, thus we need to calculate an integer $b$, such that $17 + 32b \equiv 0 \; mod \; 3$, while $17 + 32b \leq 93$.

After simple computing, we get $b = 2$, and the corresponding $a = 27$. Therefore, $x = 2048 \cdot 27 = 55296$.

3. For simple Pohlig-Hellman algorithm, it cannot solve the question because $65536 = 2^{16}$, which contains only one prime, thus it is impossibleto use the CRT to combine the results.

   However, we can apply the optimized Pohlig-Hellman algorithm. Since $2048 \mid x$, and $4096 \nmid x$, we can write $x$ as:

$$x = 2^{11} + a_0 2^1 2 + a_1 2^1 3 + a_2 2^1 4 + a_3 2^1 5$$

   where $a_0, a_1, a_2, a_3$ take the value 0 or 1. Then we can calculate $a_0$ as:

$$(\frac{3^x}{3^{2048}})^{\frac{2^{15}}{2^{12}}} \equiv 3^{a_0 2^{15} + a_1 2^{16} + a_2 2^{17} + a_3 2^{18}}$$

   Since $3^{16} \equiv 1 \; mod \; 65537$, then the above equation can be expressed as:

$$3^{a_0 2^{15}} \; mod \; 65537$$

   We can easily find that $3^{2048} \equiv -8 \; mod \; 65537$, which has a multiplicative inverse $8192 = 2^{13}$. Thus:

$$(\frac{3^x}{3^{2^{11}}})^{\frac{2^{15}}{2^{12}}} \equiv (2 \cdot 2^{13})^8 \equiv 2^{16} \equiv -1 \; mod \; 65537$$

   So $a_0 = 1$. Similarly, for $a_1$,

$$3^{a_1 2^{15}} \equiv (\frac{3^x}{3^{2^{11}+2^{12}}})^{\frac{2^{15}}{2^{13}}} \equiv (2 \cdot 2^7)^{2^2} \equiv 1 \; mod \; 65537$$

   So $a_1 = 0$. For$a_2$:

$$3^{a_2 2^{15}} \equiv (\frac{3^x}{3^{2^{11}+2^{12}}})^{\frac{2^{15}}{2^{14}}} \equiv (2 \cdot 2^7)^2 \equiv -1 \; mod \; 65537$$

   So $a_2 = 1$. For $a_3$:

$$3^{a_3 2^{15}} \equiv (\frac{3^x}{3^{2^{11}+2^{12}+2^{14}}})^{\frac{2^{15}}{2^{15}}} \equiv 2 \cdot 2^1 5 \equiv -1 \; mod \; 65537$$

   So $a_3 = 1$. Therefore, $x = 2^{11} + 2^{12} + 2^{14} + 2^{15} = 55296$.

4. 65537 is a prime that can be expressed as $p^k + 1$ where p is a quite small prime. Suppose we have some $c^x \equiv p \ mod \ p^k + 1$, then $c^{kx} \equiv -1 \ mod \ p^k + 1$, $c^{2kx} \equiv 1 \ mod \ p^k + 1$. If $c$ is a generator, we can easily find that $c^{p^k} \equiv 1 \ mod \ p^k + 1$, so $p^k \mid 2kx$ and $p^k \nmid kx$, thus:

$$\frac{p^k}{2k} \mid x \qquad \text{and} \qquad \frac{p^k}{k} \nmid x$$

So there only exist a little possibility for deciding $x$. Therefore, such primes are not fitting a cryptographic context.