VE475 Introduction to Cryptography
Homework 5

Jiang, Sifan
jasperrice@sjtu.edu.cn
515370910040

June 23, 2019

Ex. 1 - RSA setup

1. In RSA encryption, we use

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

Then, based on Euler's theorem, let's assume m and n be two coprime integers, we would have

$$c^d \equiv m^{ed} \equiv m^{ed \mod \varphi(n)} \equiv m \mod n,$$

which is what expected in RSA decryption. So it is likely for n to be coprime with m.

2. Assume $k = a\varphi(n)$, where $a \in \mathbb{N}$.

a) With Euler's theorem, we have

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

Since $n = pq$, we can have $m^k \equiv 1 \mod p$ and $m^k \equiv 1 \mod q$.

b) If $\gcd(m, n) = 1$, from the result of the above question, it is obvious that $m^{k+1} \equiv m \mod p$ and $m^{k+1} \equiv m \mod q$.
If $\gcd(m, n) = p$, we can have $\gcd(m/p, q) = 1$, thus $(m/p)^{\varphi(q)} \equiv 1 \mod q$.

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

So, $m^k \equiv 1 \mod p$ and $m^k \equiv 1 \mod q$.
If $\gcd(m, n) = q$, similar to the case of $\gcd(m, n) = p$, we would have $m^k \equiv 1 \mod p$ and $m^k \equiv 1 \mod q$.

3. a) Since $ed \equiv 1 \mod \varphi(n)$, $ed = k + 1$. Then based on the previous result, we would have $m^{ed} \equiv m \mod n$ for all m.

   b) Based on the previous conclusion, no matter m and n are coprime or not, we would have $c^d \equiv m^{ed} \equiv m \mod n$ in decryption. So there's no need for having $\gcd(m, n) = 1$.

Ex. 2 - RSA decryption

We have $n = 101 \times 113$, thus $\varphi(n) = 100 \times 112 = 11200$. By applying the extended Euclidean algorithm, we can have $d = 3 = (11)_2$ such that $ed \equiv 1 \mod \varphi(n)$. Then the plaintext m would given by calculating $c^d \equiv m \mod n$. We can apply modular exponentiation to find m.

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 d is small, the calculation of $c^d \equiv m \mod n$ with modular exponentiation would be faster.

2. Since $ed \equiv 1 \mod \varphi(n)$, we have

$$\begin{aligned} ed &= K \times \varphi(pq) + 1 \\ &= K \times \operatorname{lcm}(p-1, q-1) + 1 \end{aligned}$$

Define $G = \gcd(p-1, q-1)$, the we would have

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

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

$$\begin{aligned} ed &= \frac{k}{g}(p-1)(q-1) + 1 \\ \frac{ed}{dpq} &= \frac{k}{dg}\frac{(p-1)(q-1)}{pq} + \frac{1}{dpq} \\ \frac{e}{pq} &= \frac{k}{dg}(1-\delta), \end{aligned}$$

where $\delta = \frac{p+q-1-\frac{g}{k}}{pq}$. Since p and q are two large primes, δ would be small, then $\frac{e}{pq}$ is slightly smaller than $\frac{k}{dg}$. Also, since $ed = \frac{k}{g}(p-1)(q-1) + 1$, let $k^* = \dfrac{k}{g}$ we can have

$$(p-1)(q-1) = \varphi(n) = \frac{ed-1}{k^*},$$

where $\dfrac{e}{n}$ is slightly smaller than $\dfrac{k^*}{d}$. Then continued fractions is applied on $\frac{e}{pq}$ to obtain multiple approximated $\frac{k^*}{d}$ validate them and get the right d if the equation $x^2 - (n - \varphi(n) + 1)x + n = 0$, where $\varphi(n) = \frac{ed-1}{k^*}$, has two valid solutions which are p and q.

3. According to Wiener's theorem, if $d < \frac{1}{3}n^{\frac{1}{4}}$, the attacker can efficiently recover d. So, d should be larger than $\frac{1}{3}n^{\frac{1}{4}}$.

4. By applying continued fractions on $\frac{e}{n}$, we have

$$\frac{77537081}{317940011} = 0 + \cfrac{1}{4 + \frac{1}{9+\frac{1}{1+\frac{1}{19+\cdots}}}}$$

Then we have convergent $\frac{k^*}{d}$: $0, \frac{1}{4}, \frac{9}{37}, \frac{10}{41}, \frac{199}{816}, \cdots$. And according to Wiener's theorem, $d < \frac{1}{3}n^{\frac{1}{4}} < 45$, we can start with $\frac{1}{4}$ and have

$$(n - \varphi(n) + 1)^2 - 4n = (n - \frac{ed-1}{k^*} + 1)^2 - 4n = 60709145712677,$$

which is not a square number.
Then try next possible $\frac{k^*}{d}$, and when $\frac{k^*}{d} = \frac{10}{41}$, we have

$$(n - \varphi(n) + 1)^2 - 4n = (n - \frac{ed-1}{k^*} + 1)^2 - 4n = 170720356 = 13066^2,$$

so $p = \frac{37980+13066}{2} = 25523$ and $q = \frac{37980-13066}{2} = 12457$, thus $n = 12457 \times 25523$.

Ex. 5 - Simple questions

1.

2. No, this double encryption isn't adding any security. The nature of breaking RSA is to factorize n, using double exponents won't make it more secure.

3. Since $n = 642401$, we have

$$\begin{aligned}
4 \cdot 516107^2 - 187722^2 &\equiv 0 \mod n \\
(2 \cdot 516107 - 187722)(2 \cdot 516107 + 187722) &\equiv 0 \mod n \\
844492 \cdot 1219936 &\equiv 0 \mod n \\
(-440310) \cdot (-64866) &\equiv 0 \mod n \\
(2 \cdot 3 \cdot 5 \cdot 13 \cdot 1129) \cdot (2 \cdot 3 \cdot 19 \cdot 569) &\equiv 0 \mod n
\end{aligned}$$

So, we would get $n = 642401 = 569 \times 1129$.

4. With three primes p, q, and r, $n = pqr$ and $\varphi(n) = (p-1)(q-1)(r-1)$. Find e such that $\gcd(e, \varphi(n)) = 1$, and then find d such that

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

Then

$$\begin{aligned}
c &\equiv m^e \mod n \\
m &\equiv c^d \equiv m^{ed} \equiv m^{\varphi(n)+1} \mod n
\end{aligned}$$

If the length of the public keys are same in both cases, it would result in short separate primes, making the factorization easier.

5. Since $97-1=96=2^5\times 3$, then a α is a generator if $\alpha^{48}\not\equiv 1 \mod 97$ and $\alpha^{32}\not\equiv 1 \mod 97$. Or, since $32=2\times 16$ and $48=3\times 16$, we can first calculate 2

$$\alpha^{16}\not\equiv \pm 1, 35, 61 \mod 97$$

We can take the numbers in consequence and have

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

So, 5 is the smallest generator of the group.

6. a) Since $101-1=100=2^2\times 5^2$, we would have

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

Also,

$$2^{\frac{100}{5}}\equiv 2^{20}\equiv 95\not\equiv 1 \mod 101$$

So, 2 is a generator of G.

b) Since $\log_2 2=1$, we would have

$$\log_2 24=\log_2 3+3\log_2 2=69+3=72$$

c) Since in group G,

$$\log_2 24=\log_2(24+101)=\log_2(125)=3\log_5=3\times 24=72$$

7. Since $\gcd(3,137)=1$, we have $3^{\varphi(137)}\equiv 3^{136}\equiv \mod 137$. Also, notice that $44=2^2\times 11$, we would have

$$3^6\equiv 3^{136+6}\equiv 3^{142}\equiv 44\equiv 2^2\times 11\equiv (3^{10})^2\times 3^x \mod 137$$

So, $x=142-2\times 10=122$.

8. a) Since $6^5\equiv 10 \mod 11$, 6^5 in G is 10.

b) For $q|(p-1)$, $q\in\{2,5\}$.

$$2^{\frac{10}{2}}\equiv 10\not\equiv 1 \mod 11$$
$$2^{\frac{10}{5}}\equiv 4\not\equiv 1 \mod 11$$

So 2 is a generator of G.

c) From previous result, we have

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

Also,

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

So, $(-1)^x=-1$, thus x is odd.

Ex. 6 - DLP

1. From what we known, we can have

$$\begin{aligned} 3^x &\equiv 2 \mod 65537 \\ 3^{16x} &\equiv -1 \mod 65537 \\ 3^{32x} &\equiv 1 \mod 65537 \end{aligned}$$

   Since 3 and 65537 are coprime integers and $\varphi(65537) = 65536$, we would also have

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

   So $65536 | 32x$ and $65536 \nmid 16x$, which gives that 2048 divides x, while 4096 does not.

2. Let $x = (2k+1) \cdot 2048$, where $k \in \mathbb{N}$. And there are 16 possible choices for k, which are $0, 1, 2, \cdots, 15$. And when $k = 13$ ($x = 55296$), we have $3^x \equiv 2 \mod 65537$.

3. Since $x|2048$ and $x \nmid 4096$, we can apply the Pohlig-Hellman algorithm by using

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

   For a_{12},

$$\left(\frac{3^x}{3^{2^{11}}}\right)^{2^{15-12}} \equiv (2^{14})^8 \equiv -1 \mod 65537$$

   So, $a_{12} = 1$.

   For a_{13},

$$\left(\frac{3^x}{3^{2^{11}+2^{12}}}\right)^{2^{15-13}} \equiv (2^8)^4 \equiv 1 \mod 65537$$

   So, $a_{13} = 0$.

   Similarly, we would have $a_{14} = 1$ and $a_{15} = 1$, which gives

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

4. 65537 is a prime but in the form $p^k + 1$. If $c^x \equiv p \mod p^k + 1$, in order to find x, we can find a generator of the group and since $c^{2k} \equiv p^{2k} \equiv 1 \mod p^k + 1$, we can find $\frac{p^k}{2k}|x$ and $\frac{p^k}{k} \nmid x$. Then there would only be k possible choices for x.