VE475 Homework 5

Yiwen Yang

Ex.1 - RSA Setup

1. Since $n = pq$, the probability of $gcd(m, n) \neq 1$ is $\frac{1}{p} + \frac{1}{q} - \frac{1}{n}$ which is very small, so n is very likely to be coprime with m.

2. (a) According to Euler Theorem

$$m^{\varphi(p)} \equiv 1 \bmod p$$

Then

$$m^k \equiv m^{a\cdot\varphi(n)} \equiv m^{a\cdot\varphi(p)\varphi(q)} \equiv 1 \bmod p$$

And similarly

$$m^k \equiv 1 \bmod q$$

(b) If $gcd(m, p) = 1$, then obviously

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

If $gcd(m, p) \neq 1$, *i.e.*, $gcd(m, p) = p$.

$$m \equiv 0 \bmod p$$

$$m^{k+1} \equiv 0 \equiv m \bmod p$$

So for any m, $m^{k+1} \equiv m \bmod p$, and similarly $m^{k+1} \equiv m \bmod q$.

3. (a) Since we have

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

Then

$$ed = a\varphi(n) + 1$$

$$m^{ed} \equiv m^{a\varphi(n)+1} \equiv m \bmod n$$

For arbitrary m.

(b) The decryption of RSA calculates

$$c^d \equiv m^{ed} \equiv m \bmod n$$

Since this process holds true for arbitrary m as proved above, there is no such need that $gcd(m, n) = 1$.

Ex.2 - RSA Decryption

Factorizing 11413 gets 101 × 113, then $\varphi(11413) = 100 \times 112 = 11200$. Use Extended Euclidean Algorithm to find $d = e^{-1} \bmod \varphi(n)$

$$\begin{aligned}
11200 &= 7467 \times 1 + 3733 \\
7467 &= 3733 \times 2 + 1 \\
1 &= 7467 - 2 \times 3733 \\
&= 7467 - 2 \times (11200 - 7467) \\
&= 3 \times 7467 - 2 \times 11200
\end{aligned}$$

Yields $d = 3$. Then

$$m = c^d \bmod n = 5859^3 \bmod 11413 = 1415$$

So the plain text is 1415.

Ex.3 - Breaking RSA

1. Short keys are fast to generate and fast to encrypt/decrypt as well.
2. First introduce the continued fraction representation. Denote

   $$\langle q_0, q_1, \ldots, q_m \rangle = q_0 + \frac{1}{q_1 + \frac{1}{\cdots \frac{1}{q_{m-1} + \frac{1}{q_m}}}}$$

   To extract continued fraction from rational, just take the inverse of the rational and minus the maximum integer repeatedly. To calculate the rational in the order of q_0 to q_m, define

   $$\frac{n_i}{d_i} = \langle q_0, q_1, \ldots, q_m \rangle, gcd(n_i, d_i) = 1, i = 0, 1, \ldots, m$$

   And

   $$\begin{aligned}
   n_0 &= q_0 \\
   n_1 &= q_0 q_1 + 1 \\
   n_i &= q_i n_{i-1} + n_{i-2} \\
   \\
   d_0 &= 1 \\
   d_1 &= q_1 \\
   d_i &= q_i d_{i-1} + d_{i-2}
   \end{aligned}$$

   Then calculating $f = n_m / d_m$ gives the result.

   Given some f' such that $f' = f(1 - \delta)$, we can estimate f from f' when δ is small enough, and the following algorithm is used.

Algorithm 1 Reconstruct f

```
Input: Rational number $f^{'}$
Output: Array of possible rational number $f$
  $i \leftarrow 0$
  $q \leftarrow$ ContinuedFractionFormOf($f^{'}$)
  $r \leftarrow Array.empty$
  for $i \leftarrow 0$ until $q$.length do
      $c \leftarrow$ RationalFormOf($q[0], q[1], \ldots, q[i]$)
      if $i$ is Even then
          if $c$ Equals to RationalFormOf($q[0], q[1], \ldots, q[i-1], q[i]+1$) then
              $r+=c$
          end if
      else if $i$ is Odd then
          if $c$ Equals to RationalFormOf($q[0], q[1], \ldots, q[i-1], q[i]$) then
              $r+=c$
          end if
      end if
  end forreturn $r$
```

Next go back to Wiener's Attack, write

$$\begin{aligned} ed &= k\varphi(n) + 1 \\ &= k(n - p - q - 1) + 1 \\ \frac{ed}{n} &= k(1 - \delta) \\ \frac{e}{n} &= \frac{k}{d}(1 - \delta) \end{aligned}$$

Where $\delta = (p + q - 1 - 1/k)/n$. Then using the above method, we can derive a list of possible k and d given e and n. To verify and get correct keys, solve Eq.1 to see whether there are solutions to integer p and q.

$$x^2 - (n - \frac{ed - 1}{k} + 1)x + n = 0 \tag{1}$$

3. The length of the key should be larger than $\frac{1}{3}n^{\frac{1}{4}}$.

4. The result is found as $n = 12457 \times 25523, d = 41$. Source code can be seen in folder **ex3**.

Ex.4 - Programming

See in folder **ex4**.

Ex.5 - Simple Questions

1. Choose a proper r such that calculating $r^e \cdot c \bmod n$ will give $r \cdot m$, which means that we can indirectly decrypt the cipher derived from another one.

2. No, since doubling the encryption does not add to the difficulty of factorizing numbers, so if it takes the attacker some certain time to hack the first key, it will just take another same amount of time to hack the other one, which does not make a big difference.

3. $$187722^2 - 516107^2 \times 4 \equiv 0 \bmod n$$
$$(187722 + 516107 \times 2)(187722 - 516107 \times 2) \equiv 0 \bmod n$$
$$1219936 \times 844492 \equiv 0 \bmod n$$
$$64866 \times 844492 \equiv 0 \bmod n$$
$$2^3 \times 3 \times 19 \times 569 \times 211123 \equiv 0 \bmod n$$
   Obviously 2, 3, 19 are not factors of 642401, and 569 is. So $642401 = 569 \times 1129$.

4. The process is exactly the same except that $\varphi(n) = (p-1)(q-1)(r-1)$. If n has the same length, then with three factors the attack will be easier since each factor is smaller, so the security level is lower than two factors.

5. For all $q \mid 96$, $q = 2, 3$, test α from 2 such that $\alpha^{96/q} \not\equiv 1 \bmod 97$, and the smallest α is 5. So the smallest generator of $U(\mathbb{Z}/97\mathbb{Z})$ is 5.

6. (a) For all $q \mid 100$, $q = 2, 5$, test $\alpha = 2$ and get $\alpha^{50} \equiv 100 \not\equiv 1 \bmod 100$, $\alpha^{20} \equiv 95 \not\equiv 1 \bmod 100$, so 2 is a generator of $U(\mathbb{Z}/101\mathbb{Z})$.

   (b) $\log_2 24 = \log_2 3 + \log_2 8 = 69 + 3 = 72$

   (c) $\log_2 24 = \log_2 125 = 3 \log_2 5 = 72$

7. For all $q \mid 136$, $q = 2, 17$, test $\alpha = 3$ and get $\alpha^{68} \equiv 136 \not\equiv 1 \bmod 137$, $\alpha^8 \equiv 122 \not\equiv 1 \bmod 137$, so 3 is a generator of $U(\mathbb{Z}/137\mathbb{Z})$.

   Then $x = \log_3 11 = \log_3 44 - 2\log_3 2 = -14 = 122$.

8. (a) $6^5 \equiv 3^2 \times 6 \equiv 10 \bmod 11$

   (b) For all $q \mid 10$, $q = 2, 5$, test $\alpha = 2$ and get $\alpha^5 \equiv 10 \not\equiv 1 \bmod 11$, $\alpha^2 \equiv 4 \not\equiv 1 \bmod 11$. So 2 is a generator of $U(\mathbb{Z}/11\mathbb{Z})$.

   (c) $(2^5)^x \equiv 6^5 \equiv -1 \bmod 11$, so x should be odd.

Ex.6 - DLP

1.

$$\begin{aligned} 3^{16x} &\equiv 2^{16} \equiv -1 \bmod 65537 \\ 3^{32x} &\equiv 1 \bmod 65537 \\ 3^{65536} &\equiv 1 \bmod 65537 \end{aligned}$$

So $65536 \mid 32x$, $65536 \nmid 16x \Rightarrow 2048 \mid x$, $4096 \nmid x$.

2. x satisfies $x = 2048(2k+1)$, so there are 16 possible choices. Applying modular exponentiation, find that $3^{2048} \equiv 65529 \equiv -8 \bmod 65537$. Try k from 0 to 15.

$$(-8)^7 \equiv 32 \bmod 65537$$

$$(-8)^11 \equiv -2 \bmod 65537$$

$$(-8)^17 \equiv -2 \bmod 65537$$

$$(-8)^23 \equiv -32 \bmod 65537$$

$$(-8)^27 \equiv 2 \bmod 65537$$

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

3. The only factor of 65536 is 2, it is easy to apply Pohlig-Hellman algorithm.

Since $x = 2048(2k+1)$, then write $x = 2^{11} + c_{12}2^{12} + c_{13}2^{13} + c_{14}2^{14} + c_{15}2^{15}$.

$$(2 \times 3^{-1})^{32768/2^{12}} = (3^{32768})^{c_{12}} \Rightarrow c_{12} = 1$$

$$(2 \times 3^{-1})^{32768/2^{13}} = (3^{32768})^{c_{13}} \Rightarrow c_{12} = 0$$

$$2^{32768/2^{14}} = (3^{32768})^{c_{14}} \Rightarrow c_{14} = 1$$

$$(2 \times 3^{-1})^{32768/2^{15}} = (3^{32768})^{c_{15}} \Rightarrow c_{15} = 1$$

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

4. Such primes p has only one factor for $p-1$, and according to above methods, DLP is a lot easier to solve. It is not safe in a cryptographic context.