VE475 Introduction to Cryptography
Homework 5

Jiang, Sifan
jasperrice@sjtu.edu.cn
515370910040

June 16, 2019

$$\frac{K_A K_L K_i K_s}{B_m J_L R_a s^3 + J_L K_b K_i s^3 + J_L J_m R_a s^4 + J_L K_L R_a s^2 + J_m K_L R_a s^2 + K_A K_L K_i K_s + B_m K_L R_a s + K_L K_b K_i s}$$

$$\frac{42000000000\pi K_A}{19530000000s + 23000000000\pi s + 184000000\pi s^2 + 23000\pi s^3 + 69\pi s^4 + 19530s^3 + 42000000000\pi K_A}$$

Ex. 1 - Euler's totient

1. Notice that for a given prime p, we have $\varphi(p) = p - 1$. So, positive integers n that is smaller than p^k, so that $\gcd(n, p^k) \neq 1$, can be $1 \times p$, $2 \times p$, $3 \times p$, $\cdots$, $(p^{k-1} - 1) \times p$. So the amount of possible n is $p^{k-1} - 1$. Also, there are $p_k - 1$ positive integers are smaller than p^k, so for any prime p, $\varphi(p^k) = (p^k - 1) - (p^{k-1} - 1) = p^{k-1}(p - 1)$.

2. Since m and n are coprime integers, according to Chinese Remainder theorem, there exists a ring isomorphism between $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. We have $\varphi(mn)$ is the order of $\mathbb{Z}/mn\mathbb{Z}$, $\varphi(m)$ is the order of $\mathbb{Z}/m\mathbb{Z}$, and $\varphi(n)$ is the order of $\mathbb{Z}/n\mathbb{Z}$. Since an isomorphism is a bijection that preserves algebraic structures, we would have $\varphi(mn) = \varphi(m) \times \varphi(n)$.

3. Assume $n = \prod_i p_i^{k_i}$, then applying the previous results to integer $n > 1$, we have

$$\begin{aligned}\varphi(n) =& \prod_i \varphi(p_i^{k_i}) \\ =& \prod_i p_i^{k_i - 1}(p_i - 1) \\ =& \prod_i p_i^{k_i}(1 - \frac{1}{p_i}) \\ =& n \prod_{p|n}(1 - \frac{1}{p})\end{aligned}$$

4. The three last digits of 7^{803} can be obtained by calculating $7^{803} \mod 1000$. We note that $1000 = 2^3 \times 5^3$, thus $\varphi(1000) = 1000 \times (1 - \frac{1}{2}) \times (1 - \frac{1}{5}) = 400$ according to the previous result. So we would have

$$\begin{aligned}7^{803} \equiv& (7^{400})^2 \times 7^3 \mod 1000 \\ \equiv& 7^3 \mod 1000 \\ \equiv& 7^3 \mod 1000 \\ \equiv& 343 \mod 1000\end{aligned}$$

So, the three last digits of 7^{803} are 343.

Ex. 2 - AES

1. The key used for round 1 is given by the columns $K(4), \cdots, K(7)$. Also, recall that for $i \not\equiv 0 \mod 4$, $K(i) = K(i-4) \oplus K(i-1)$, and for $i \equiv 0 \mod 4$, $K(i) = K(i-4) \oplus T(K(i-1))$.

   For $K(4)$, we have

   $$K(4) = K(0) \oplus T(K(3)) = \overline{T(K(3))}$$

   Then the only problem is to compute $T(K(3))$.

   - $r(4) = X^{\frac{4-4}{4}} = X^0 \equiv 00000001 \mod P(X)$.
   - Cyclically top shift the elements of the column by 1 would give the same vector.
   - Apply the *SubBytes* layer to each byte of the column and get the column vector, which is $(00010110, 00010110, 00010110, 00010110)$.
   - Finally return the column vector

   $$\begin{aligned} T(K(3)) =& (00010110 \oplus 00000001, 00010110, 00010110, 00010110) \\ =& (00010111, 00010110, 00010110, 00010110) \end{aligned}$$

   So, in all we have

   $$\begin{aligned} T(4) =& \overline{T(K(3))} = (11101000, 11101001, 11101001, 11101001) \\ K(5) =& K(1) \oplus K(4) = \overline{K(4)} = (00010111, 00010110, 00010110, 00010110) \\ K(6) =& K(2) \oplus K(5) = \overline{K(5)} = K(4) = (11101000, 11101001, 11101001, 11101001) \\ K(7) =& K(3) \oplus K(6) = \overline{K(6)} = \overline{K(4)} = (00010111, 00010110, 00010110, 00010110) \end{aligned}$$

2. As shown in the above question, $K(5) = \overline{K(4)}$.

3. - Prove that $K(10) = \overline{K(8)}$

     $$\begin{aligned} K(10) =& K(6) \oplus K(9) \\ =& K(6) \oplus (K(5) \oplus K(8)) \\ =& K(6) \oplus K(5) \oplus K(8) \\ =& (11111111, 11111111, 11111111, 11111111) \oplus K(8) \\ =& \overline{K(8)} \end{aligned}$$

   - Prove that $K(11) = \overline{K(9)}$

     $$\begin{aligned} K(11) =& K(7) \oplus K(10) \\ =& K(7) \oplus (K(6) \oplus K(9)) \\ =& K(7) \oplus K(6) \oplus K(9) \\ =& (11111111, 11111111, 11111111, 11111111) \oplus K(9) \\ =& \overline{K(9)} \end{aligned}$$

Ex. 3 - Simple questions

1. In mode ECB, each block is encrypted independently with a function E and a key k, so corruption of one block wouldn't influence other blocks. So the number of plaintext decrypted incorrectly is one for the ECB mode.

   In mode CBC, after the second block, XOR operation between the previous ciphertext and the current plaintext is first done before the E function and key k. So if one block is corrupted, the next block will also be influenced, thus the number of plaintext decrypted incorrectly is two for the CBC mode.

2. Since the length of block is finite, so the IV would be repeated after 2^n trials, where n is the block length. The attacker then can use whatever plaintext and compare the ciphertext generated with the same IV to find the pattern. In this way, the schemes are not CPA secure.

3. Since $p - 1 = 29 - 1 = 28 = 2 \times 2 \times 7$, so $q \in \{2, 7\}$.

   - When $q = 2$, we have
   $$2^{(29-1)/2} \equiv 2^{14} \equiv 2^4 \cdot 32^2 \equiv 2^4 \cdot 3^2 \equiv 2^2 \cdot 7 \equiv 28 \not\equiv 1 \mod 29$$
   - When $q = 7$, we have
   $$2^{(29-1)/7} \equiv 2^4 \equiv 16 \not\equiv 1 \mod 29$$

   So, 2 is a generator of $\mathsf{U}(\mathbb{Z}/29\mathbb{Z})$.

4. Using proposition from Jacobi symbol, since 1801 and 8191 are odd prime positive integers, and $1801 \equiv 1 \mod 4$, we have
$$\begin{aligned}\left(\frac{1801}{8191}\right) &= +\left(\frac{8191}{1801}\right) = +\left(\frac{987}{1801}\right)\\ &= +\left(\frac{1801}{987}\right) = +\left(\frac{814}{987}\right) = +\left(\frac{2 \times 11 \times 37}{3 \times 7 \times 47}\right) = +\left(\frac{2}{987}\right)\left(\frac{11}{987}\right)\left(\frac{37}{987}\right)\\ &= +\left(\frac{987}{11}\right)\left(\frac{987}{37}\right) = +\left(\frac{8}{11}\right)\left(\frac{25}{37}\right) = +\left(\frac{2^3}{11}\right)\left(\frac{5^2}{37}\right) = +\left(\frac{2}{11}\right)^3\left(\frac{5}{37}\right)^2\\ &= -\left(\frac{37}{5}\right)^2 = -\left(\frac{2}{5}\right) = -1\end{aligned}$$

5. If $\left(\frac{b^2-4ac}{p}\right) = 0$, meaning $b^2 - 4ac = 0$, then the equation have one solution $x = -\frac{b}{2a}$ (more technically speaking, two same solutions). Since $-\frac{b}{2a}$ can always mod p, it's true that the number of solutions is $1 + \left(\frac{b^2-4ac}{p}\right) = 1$.

   If $\left(\frac{b^2-4ac}{p}\right) \neq 0$, meaning $b^2 - 4ac \neq 0$, then the equation have two different solutions $x_1 = \frac{-b+\sqrt{b^2-4ac}}{2a}$ and $x_2 = \frac{-b-\sqrt{b^2-4ac}}{2a}$. So we would have
$$\begin{aligned}\frac{-b \pm \sqrt{b^2-4ac}}{2a} &\equiv x \mod p\\ \sqrt{b^2-4ac} &\equiv \pm(2ax + b) \mod p\end{aligned}$$

   Then, if $\left(\frac{b^2-4ac}{p}\right) = 1$, meaning $b^2 - 4ac$ is a square mod p, then it's true that the number of solutions mod p is $1 + \left(\frac{b^2-4ac}{p}\right) = 2$.

Otherwise, if $\left(\frac{b^2-4ac}{p}\right) = -1$, meaning $b^2 - 4ac$ is not a square mod p, it's true that the number of solutions mod p is $1 + \left(\frac{b^2-4ac}{p}\right) = 0$.

6. Since $\gcd(n, pq) = 1$, we have $\gcd(n, p) = 1$ and $\gcd(n, q) = 1$. Also, since $q - 1$ divides $p - 1$, we have $(p - 1) = k(q - 1)$, where k is a positive integer. So, according to Euler's theorem, we have

$$\begin{aligned} n^{p-1} &\equiv 1 \mod p \\ (n^{q-1})^k \equiv n^{p-1} &\equiv 1 \mod q \end{aligned}$$

Since $\gcd(n^{p-1}, p) = 1$ and $\gcd(n^{p-1}, q) = 1$, we can conclude that $\gcd(n^{p-1}, pq) = 1$, which is

$$n^{p-1} \equiv 1 \mod pq$$

7. - Sufficiency: if $p \equiv 1 \mod 3$, then we can obtain

$$\left(\frac{p}{3}\right) = 1$$

Also, note that p is an odd prime. If $p \equiv 1 \mod 4$

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 = 1$$

If $p \equiv 3 \mod 4$

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1) \cdot (-1) = 1$$

   - Necessity: We already known $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1$, since p is an odd prime, $p \equiv 1 \mod 4$ or $p \equiv 3 \mod 4$.
If $p \equiv 1 \mod 4$, $\left(\frac{-1}{p}\right) = 1$, thus $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1$.
If $p \equiv 3 \mod 4$, $\left(\frac{-1}{p}\right) = -1$, thus $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -1$.
So, in both case $\left(\frac{p}{3}\right) = 1$, which gives $p^{(3-1)/2} \equiv p \equiv 1 \mod 3$.

8. If $\left(\frac{a}{p}\right) = 1$, we would have $a^{(p-1)/2} \equiv 1 \mod p$. However 2 is a prime factor of $p - 1$, meaning $2|(p - 1)$. So conflict with the requirement to be a generator, thus a is not a generator of $\mathbb{F}_p^*$.

Ex. 4 - Prime vs. irreducible

1. Assume p is not irreducible and $p = a \cdot b$, where a and b are two non-invertible and non-zero elements and also not equal to element 1. Assume $x = k_1 a$ and $y = k_2 b$, where $k_1, k_2 \neq 0$, then $p \nmid (x \cdot y)$ holds. Let $a \nmid k_2$ and $b \nmid k_1$. Then $ab \nmid k_1 a$ and $ab \nmid k_2 b$, thus $p \nmid x$ and $p \nmid y$ which is contradictory to the definition. So any prime element is irreducible.

2. Assume $p \in \mathbb{Z}$ and p is an irreducible integer. If $p > 1$ and $a|p$, then we can assume that $p = k \cdot a$. Since p is irreducible, $k > 1$ and $a > 1$ cannot both be true. Then either $a = 1$ or $k = 1$. If $k = 1$, $p = 1 \cdot a = a$. So, $a = 1$ or $a = p$ is true for any irreducible integer $p \in \mathbb{Z}$ if $p > 1$ and $a|p$.

3. For $p \in \mathbb{Z}$, from $(**)$ we know if $p > 1$ and $a|p$, then p is prim if $a = 1$ or $a = p$. Assume $a = p$, it's true that $a|(p \cdot \prod_i q_i^{e_i})$, where q_i are prime. So for $(*)$, in the factors of x or y, there must be one is p, which implies that $p|x$ or $p|y$.

4. According to $(*)$, any prime integer is irreducible. Then, for p is prime and $a|p$, we can assume that $a \neq 1$ and $a \neq$, which gives $1 < a < p$. But for such a, $a|p$ doesn't hold, so $(*)$ implies $(**)$. Also according to above question, we can conclude that $(*)$ and $(**)$ are equivalent for integers.

Ex. 5 - Primitive root mod 65537

1. Using proposition of Jacobi symbol, since $65537 \equiv 1 \mod 4$ and $\gcd(3, 65537) = 1$, we have

$$\begin{aligned}\left(\frac{3}{65537}\right) &= + \left(\frac{65537}{3}\right) \\ &= + \left(\frac{2}{3}\right) \\ &= -1\end{aligned}$$

Meaning 3 is not a square mod 65537.

2. Since 65537 is a prime integer, $\frac{65537-1}{2} = 32768$, and 3 is not a square mod 65537, we can conclude that $3^{32768} \not\equiv 1 \mod 65537$.

3. First note that $p - 1 = 65537 - 1 = 2^{16}$, thus $q = 2$ is the only prime such that $q|(p-1)$. Also, since $3^{32768} \equiv \alpha^{(p-1)/q} \not\equiv 1 \mod p$, and according to the theorem, we can conclude that $\alpha = 3$ is a primitive root mod 65537.