VE475 Intro to Cryptography Homework 4

Taoyue Xia, 518370910087

2021/06/16

Ex1

1. Let G be a group, and G = $\mathbb{Z}/p^k\mathbb{Z}$, thus it has $p^k - 1$ elements, which are $1, 2, \cdots, p^k - 1$. As p is a prime number, the numbers in G which are not coprime with p^k are $p, 2p, \cdots, (p-1)p^{k-1}$, which have $p^k/p = p^{k-1}$ in total.
   Thus according to Euler's totient function, $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$

2. Suppose that $\varphi(m) = m - k_m$, where k_m denotes the number of elements which are not coprime with m in $\mathbb{Z}/m\mathbb{Z}$. Similarly, $\varphi(n) = n - k_n$. For $\mathbb{Z}/mn\mathbb{Z}$, as m and n are coprime integers, m and n has no common divisor, so the elements that are not coprime with mn in the ring are the combination of those in ring M and N, adding the multiplication between each of them in M and N. Thus:

$$\varphi(mn) = mn - k_m - k_n - k_m \cdot k_n = (m - k_m)(n - k_n) = \varphi(m)\varphi(n)$$

   Proof done.

3. Suppose that $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_n^{k_n}$, where $p_1 \cdots p_n$ are different prime integers and $k_1 \cdots k_n \geq 1$ are integers. We can see that for all $p_i^{k_i},\ i = 1, \cdots, n$, they are coprime with one another,

thus:

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{k_1})\varphi(p_2^{k_2})\cdots\varphi(p_n^{k_n}) \\
&= p_1^{k_1-1}(p_1-1)\cdot p_2^{k_2-1}(p_2-1)\cdots p_n^{k_n-1}(p_n-1) \\
&= p_1^{k_1}(1-\frac{1}{p_1})\cdot p_2^{k_2}(1-\frac{1}{p_2})\cdots p_n^{k_n}(1-\frac{1}{p_n}) \\
&= p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n}\cdot(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_n}) \\
&= n\prod_{p|n}(1-\frac{1}{p})
\end{aligned}$$

Proof done.

4. To calculate 7^{803}'s last three digits, we can calculate 7^{803} mod 1000.
First, use Euler's totient function and the above equations to calculate $\varphi(1000)$. We can easily know that 1000 has two prime divisors 2 and 5, thus using the equation in (3):

$$\varphi(1000) = 1000\cdot(1-\frac{1}{2})\cdot(1-\frac{1}{5}) = 400$$

As 7 and 1000 are coprime, using Euler's Theorem, we can get:

$$7^{\varphi(1000)} = 7^{400} = 1 \ mod \ 1000$$

Finally, we can calculate 7^{803} mod 1000 as:

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

Therefore, we can conclude that the last three digits of 7^{803} is 343.

Ex2

1. For round 1, the original key is used, thus the key used is 128 bits of 1.

2.

$$K(5) = K(4)\oplus K(1)$$

3. It is obvious that for a 4-bit number X:

$$X \oplus 1111 = \overline{X}$$

As the key of first round is 128-bits 1, thus:

$$K(0) = K(1) = K(2) = K(3) = \begin{pmatrix} 1111 \\ 1111 \\ 1111 \\ 1111 \end{pmatrix}$$

Then we can calculate $K(10)$ as:

$$\begin{aligned} K(10) &= K(9) \oplus K(6) \\ &= (K(8) \oplus K(5)) \oplus (K(5) \oplus K(2)) \\ &= K(8) \oplus K(2) \\ &= \overline{K(8)} \end{aligned}$$

For $K(11)$:

$$\begin{aligned} K(11) &= K(10) \oplus K(7) \\ &= (K(9) \oplus K(6)) \oplus (K(6) \oplus K(3)) \\ &= K(9) \oplus K(3) \\ &= \overline{K(9)} \end{aligned}$$

Proof done.

Ex3

1. For ECB mode, every block of plaintext is seperately encrypted by a transform E_K, which takes E as a transform function, and K as a key. So we know that the corruption of one block does not have influence on other blocks. Therefore, the number of plaintext encrypted incorrectly for ECB mode is one.
   For CBC mode, starting from the second block, every block will perform an “xor” transformation with the previous encrypted block. In this sense, if the corrupted block is

not the last one, the corrupted block and the next block will be incorrectly encrypted. Therefore, the number of plaintext encrypted incorrectly for CBC mode is two.

2. For a chosen plaintext P, The encryption function E, and the initial IV_0, we can have the ciphertext C as:

$$C = E(IV_0 \oplus P) = E(IV_1 \oplus (IV_1 \oplus IV_0 \oplus P))$$

As IV increments by 1 each time, it will reset after reaching max bits. So after one round of IV, we can easily know the exact composition of each IV, thus it is easier to deduce the encryption function and the key.
So it is not CPA secure under this circumstance.

3. The order of $U(\mathbb{Z}/29\mathbb{Z})$ is 28, then we calculate $2^i \ mod\ 29$ in the following table:

i	$2^i \ mod\ 29$	i	$2^i \ mod\ 29$	i	$2^i \ mod\ 29$	i	$2^i \ mod\ 29$
1	2	8	24	15	27	22	5
2	4	9	19	16	25	23	10
3	8	10	9	17	21	24	20
4	16	11	18	18	13	25	11
5	3	12	7	19	26	26	22
6	6	13	14	20	23	27	15
7	12	14	28	21	17	28	1

From the table we can easily see that 2^i, $(i = 1, 2, \cdots, 28)$ generates all the elements in $U(\mathbb{Z}/29\mathbb{Z})$. So 2 is a generator of $U(\mathbb{Z}/29\mathbb{Z})$.

Or we can use the method introduced in c3, page 17.
First, $p = 29$ is a prime integer, $2 \in U(\mathbb{Z}/29\mathbb{Z})$, and $p - 1 = 28$ have two prime divisors: $q_1 = 2$ and $q_2 = 7$. Thus we calculate:

$$2^{\frac{p-1}{q_1}} = 2^{14} \equiv 28 \ mod\ 29$$

$$2^{\frac{p-1}{q_2}} = 2^{4} \equiv 16 \ mod\ 29$$

As $2^{(p-1)/q} \not\equiv 1 \ mod\ 29$, thus 2 is a generator of $U(\mathbb{Z}/29\mathbb{Z})$.

4. As 1801 and 8191 are two prime numbers, according to the lagrange symbol's definition, we just need to calculate $1801^{\frac{8191-1}{2}} = 1801^{4095}$ mod 8191.
   Apply the Modular exponentiation method, and with the code in "ex3_4.cpp", we can finally calculate $1801^{4095} \equiv 8190 \equiv -1$ mod 8191. Thus we can conclude that $(\frac{1801}{8191}) = -1$.

5. For the equation $ax^2 + bx + c = 0$, it has two roots $x = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$.
   When $b^2 - 4ac = 0$, which means the equation has one root $x = -\frac{b}{2a}$, then $(\frac{b^2-4ac}{p}) = 0$, the equation holds.
   When $b^2 - 4ac \neq 0$, Then:

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = x \ mod \ p$$

$$(b^2 - 4ac)^{\frac{1}{2}} = (2ax \pm b) \ mod \ p$$

   As p is an odd prime, and $a \not\equiv 0$ mod p, we can show that:

$$(b^2 - 4ac)^{\frac{p-1}{2}} = (2ax \pm b)^{p-1} \ mod \ p$$

   Then if $2ax \pm b \not\equiv 0$ mod p, according to the Fermat's little theorem, we can find $(b^2 - 4ac)^{\frac{p-1}{2}} \equiv 1$ mod p, thus $b^2 - 4ac$ is a square mod p, which means that $(\frac{b^2-4ac}{p}) = 1$. Then the equation has two roots. Otherwise, $(\frac{b^2-4ac}{p}) = -1$, the equation has no root.
   In all, we prove that the number of solutions mod p to the equation $ax^2 + bx + c = 0$ is $1 + (\frac{b^2-4ac}{p})$.

6. As p and q are two primes, we can have:

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

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

   Since $q - 1$ divides $p - 1$, there exists a positive integer k, so that $p - 1 = k(q - 1)$, then:

$$(n^{q-1})^k = n^{p-1} \equiv 1 \ mod \ q \tag{2}$$

   Finally, because $gcd(n, pq) = 1$, which means n and pq are coprime, applying the CRT to equation (1) and (2), we can get:

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

   Proof done.

7. Proof

(⇒) For $(\frac{-3}{p}) = 1$, as p is an odd prime, we can decomposite the former lagrange symbol as:

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

Firstly, if $(\frac{-1}{p}) = 1$, then $(-1)^{\frac{p-1}{2}} \equiv 1\ mod\ p$, which indicates that $p \equiv 1\ mod\ 4$. Then $(\frac{3}{p}) = 1$. As $p \not\equiv 3\ mod\ 4$, according to Jacobi symbol, $(\frac{3}{p}) = (\frac{p}{3}) = 1$, thus $p^{\frac{3-1}{2}} = p \equiv 1\ mod\ 3$.

Then, if $(\frac{-1}{p}) = -1$, then similarly we can have $p \equiv 3\ mod\ 4$. This means $(\frac{3}{p}) = -1$. According to the Jacobi symbol, $(\frac{3}{p}) = -(\frac{p}{3}) = -1 \ \Rightarrow\ (\frac{p}{3}) = 1$, which means that $p \equiv 1\ mod\ 3$.

According to both of the conditions, we can prove that if $(\frac{-3}{p}) = 1$, then $p \equiv 1\ mod\ 3$

(⇐) Since we know that $p \equiv 1\ mod\ 3$, we can have $(\frac{p}{3}) = 1$.

As p is an odd prime, $p \equiv 1\ mod\ 4$ or $p \equiv 3\ mod\ 4$.

When $p \equiv 1\ mod\ 4$, we can get $(\frac{3}{p}) = (\frac{p}{3}) = 1$, and $(\frac{-1}{p}) = 1$, thus:

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

When $p \equiv 3\ mod\ 4$, we can get $(\frac{3}{p}) = -(\frac{p}{3}) = -1$, and $(\frac{-1}{p}) = -1$, thus:

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

According to the above procedure, we can prove that if $p \equiv 1\ mod\ 3$, $(\frac{-3}{p}) = 1$.

8. We don't take $p = 2$ into account as $1^{\frac{1}{2}} = 1\ mod\ 2$, it does not representitive.

Then p is an odd prime, and 2 is a factor of the order of $\mathbb{F}_p^*$.

Since $(\frac{a}{p}) = 1$, it is for sure that:

$$a^{\frac{p-1}{2}} \equiv 1\ mod\ p$$

However, if a is a generator of $\mathbb{F}_p^*$, for all primes q that $q|(p-1)$,

$$a^{\frac{p-1}{q}} \not\equiv 1\ mod\ p$$

This raises a contradiction with the property deduced above.

Therefore, it is proved that if $(\frac{a}{p}) = 1$, then a is not a generator of $\mathbb{F}_p^*$.

Ex4

1. We will prove by contradiction.
   Suppose that there exists a prime p that is irreducible in the integral domain, which means that $p = mn$, for some m, n that are non-zero, non-invertible elements. According to property (*), there exists some $k_1, k_2 \neq 0$ so that $p|(k_1k_2mn)$. Let $x = k_1m$, $y = k_2n$. If $n \nmid k_1$ and $m \nmid k_2$, then $p = mn \nmid k_1m$ and $p = mn \nmid k_2n$, which raises a contradiction to (*).
   Therefore, in an integral domain, any prime element is irreducible.

2. Still prove by contradiction.
   Suppose that there exists an irreducible element p in $\mathbb{Z}$ but it is not a prime. In this sense, p cannot be represented by the multiplication of two non-zero elements, which indicates that $p \neq mn$ for any $m, n \in \mathbb{Z}$. In other words, p's divisor is only 1 and itself. However, according to (**), this property indicates that p is a prime, which raises a contradiction. Therefore, in $\mathbb{Z}$ any irreducible element is a prime in the classical sense (**).

3. Let $p \in \mathbb{Z}$ be an irreducible element, which is a prime. Suppose there exist $x, y \in \mathbb{Z}$ that $p|(x \cdot y)$. In this sense, $x \cdot y = k \cdot p$, where $k \in \mathbb{Z}$ is some arbitrary integer.
   Firstly, if k is irreducible too, then $x = k$ and $y = p$, which indicates $p|y$.
   If k is not irreducible, then divide k into $k = k_1 \cdot k_2$, where $k_1, k_2 \neq 0, 1$, thus $x \cdot y = k_1k_2p$. Then combination of x and y are shown in the table below:

x	y
k_1	k_2p
k_2	k_1p
p	k_1k_2
k_1k_2	p
k_1p	k_2
k_2p	k_1

   From the above table, we can easily find that for any $k \in \mathbb{Z}$, $p|x$ or $p|y$ is always true. Therefore, for $p \in \mathbb{Z}$, (**) implies (*).

4. We need to prove (*) implies (**), using contradiction.
As p is an integer, (*) indicates that if $p|(x \cdot y)$, then at least one of x and y would be a multiple of p, and p is irreducible.
Suppose that (**) does not hold taking (*) as the prerequisite. This indicates that there exists some a, which satisfies $a \neq 1$, $a \neq p$, but $a|p$. However, this raises a contradiction with (*) that p is irreducible. Therefore, for $p \in \mathbb{Z}$, (*) implies (**).
Since we have proved in question 3 that (**) implies (*) for $p \in \mathbb{Z}$, we can have the conclusion that (*) and (**) are equivalent for integers.

Ex5

1. Similar to Ex3.4, this time, apply the "Right-to-left binary method" of Modular exponentiation. Since $65537 = 65536 + 1 = 2^{16} + 1$, we just need to calculate $3^{\frac{65537-1}{2}} = 3^{2^{15}}$ mod 65537, the procedure is shown in the table below:

i_{th} multi	modulo 65537
3^{2^0}	$1 \cdot 3 \equiv 3$ mod 65537
3^{2^1}	$3^2 \equiv 9$ mod 65537
3^{2^2}	$9^2 \equiv 81$ mod 65537
3^{2^3}	$81^2 \equiv 6561$ mod 65537
3^{2^4}	$6561^2 \equiv 54449$ mod 65537
3^{2^5}	$54449^2 \equiv 61869$ $mod 65537$
3^{2^6}	$61869^2 \equiv 19139$ mod 65537
3^{2^7}	$19139^2 \equiv 15028$ mod 65537
3^{2^8}	$15028^2 \equiv 282$ mod 65537
3^{2^9}	$282^2 \equiv 13987$ mod 65537
$3^{2^{10}}$	$13987^2 \equiv 8224$ mod 65537
$3^{2^{11}}$	$8224^2 \equiv 65529$ mod 65537
$3^{2^{12}}$	$65529^2 \equiv 64$ mod 65537
$3^{2^{13}}$	$64^2 \equiv 4096$ mod 65537
$3^{2^{14}}$	$4096^2 \equiv 65281$ mod 65537
$3^{2^{15}}$	$65281^2 \equiv 65536$ mod 65537

Since $3^{32768} \equiv 65536 \ mod \ 65537 \not\equiv 1 \ mod \ 65537$, we can get the result that $(\frac{3}{65537}) = -1$

2. From question 1, we obtain that $3^{32768} \equiv 65536 \ mod \ 65537$, thus it is obvious that $3^{32768} \not\equiv 1 \ mod \ 65537$.

3. Firstly, we find that for $p = 65537$, $p - 1 = 65536$, which has only one prime divisor 2. Then, according to the theorem on page 17, c3, since $3^{\frac{65537-1}{2}} = 3^{32768} \not\equiv 1 \ mod \ 65537$, then 3 is a generator of $U(\mathbb{Z}/65537\mathbb{Z})$.
   Therefore, 3 is a primitive root mod 65537.