UM-SJTU JOINT INSTITUTE
VE475 Introduction to Cryptography

Homework 4

Li Yong 517370910222

June 20, 2021

Ex.1 Euler's totient

1. $G = \mathbb{Z}/p^k\mathbb{Z}$, $\varphi(p^k)$ is the number of invertible elements. Also, $\varphi(p^k)$ equals to the number of elements of G - the number of elements i such that $\gcd(p^k, i) = p$, so that $i = jp$, $i \in [1, p^k - 1]$, $j \in \mathbb{Z}^+$. Hence the number of elements i is $p^{k-1} - 1$ because the maximum value of j is $p^{k-1} - 1$. Then

$$\varphi(p^k) = (p^k - 1) - (p^{k-1} - 1) = p^{k-1}(p - 1)$$

2. According to CRT in the slides, there exists a ring isomorphism between $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Due to ismorphism, there exist a bijection between G_{mn} and $G_m \times G_n$, so that $\varphi(mn) = \varphi(m)\varphi(n)$.

3. Let the prime decomposition of n be $\prod_i p_i^{e_i}$, so that

$$\begin{aligned}
\varphi(n) &= \prod_i \varphi(p_i^{e_i}) \\
&= \prod_i [p_i^{e_i - 1}(p_i - 1)] \\
&= \prod_i \left[p_i^{e_i} \left(1 - \frac{1}{p_i} \right) \right] \\
&= \prod_i p_i^{e_i} \prod \left(1 - \frac{1}{p_i} \right) \\
&= n \prod_{p|n} \left(1 - \frac{1}{p} \right)
\end{aligned}$$

4. 7 and 1000 are two coprime integers. Then

$$7^{\varphi(1000)} \equiv 1 \bmod 1000$$

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

Then

$$7^{400} \equiv 1 \bmod 1000$$

$$7^{803} \equiv 7^3 \bmod 1000$$

Hence, the three last digits of 7^{803} is 343.

Ex.2 AES

1. 128 bits of 1.
2. $K(5) = K(1) \oplus K(4)$
3.

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

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

Ex.3 Simple questions

1. As for ECB mode, each block is encrypted parallelly. The corrupted block will lead to one incorrectly decrypted block.

   As for CBC, the result of the corrupted block will be performed XOR with the next plaintext block. Hence the number is two.

2. ..

3. Primes q that $q|(29-1)$ are 2 and 7.

   2 and 29 are coprime, then

   $$
   \begin{aligned}
   2^{\varphi(29)} &\equiv 1 \bmod 29 \\
   2^{28} &\equiv 1 \bmod 29 \\
   2^{14} &\equiv -1 \bmod 29
   \end{aligned}
   $$

   $$
   7^4 \bmod 29 = 23
   $$

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

4. $$
   \left(\frac{1801}{8191}\right) \equiv 1801^{\frac{8191-1}{2}} \bmod 8191 \equiv 1801^{4095} \bmod 8191
   $$

   According to modular exponentiation, calculated by online Modular exponentiation calculator

   $$
   1801^{4095} \equiv -1 \bmod 8191
   $$

   Hence, $\left(\frac{1801}{8191}\right) = -1$.

5. - If $b^2-4ac=0$, then there is only one solution to the equation, $x=-\frac{b}{2a}$, which mod p. The number of solutions is $1+\left(\frac{b^2-4ac}{p}\right)=1$.
   - If $b^2-4ac>0$, then there are two solutions to the equation, $x=-\frac{b\pm\sqrt{b^2-4ac}}{2a}$.

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

     We need to check whether b^2-4ac is square mod p. If $\left(\frac{b^2-5=4ac}{p}\right)=1$, then b^2-4ac is square mod p. The number of solutions is $1+\left(\frac{b^2-4ac}{p}\right)=2$. If $\left(\frac{b^2-5=4ac}{p}\right)=-1$, then b^2-4ac is not square mod p. The number of solutions is $1+\left(\frac{b^2-4ac}{p}\right)=0$.

6. p and q are two primes, then

$$n^{\varphi(q)} \equiv n^{q-1} \equiv 1 \bmod q$$
$$n^{\varphi(p)} \equiv n^{p-1} \equiv 1 \bmod p$$

$q-1|p-1$, then

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

$\gcd(n, pq) = 1$, so that

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

7. • $\left(\frac{-3}{p}\right) = 1 \Rightarrow p \equiv 1 \bmod 3$

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

If $p \equiv 1 \bmod 4$, then $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{3}{p}\right) = 1$. $p \not\equiv 3 \bmod 4$, so that $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) \equiv p \bmod 3 = 1$.

If $p \equiv 3 \bmod 4$, then $\left(\frac{-1}{p}\right) = -1$ and $\left(\frac{3}{p}\right) = -1$. $p \equiv 3 \bmod 4$, so that $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) \equiv -(p \bmod 3) = -1$, $p \equiv 1 \bmod 3$.

• $p \equiv 1 \bmod 3 \Rightarrow \left(\frac{-3}{p}\right) = 1$

If $p \equiv 1 \bmod 3$, then

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

If $p \equiv 1 \bmod 4$, $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{p}{3}\right) = \left(\frac{3}{p}\right) = 1$, so that

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

If $p \equiv 3 \bmod 4$, then $\left(\frac{-1}{p}\right) = -1$ and $\left(\frac{p}{3}\right) = -\left(\frac{3}{p}\right) = -1$, so that

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

8. If $\left(\frac{a}{p}\right) = 1$, then

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

Hence $2|(p-1)$, and 2 is a prime. It does not satisfy that for all q such that $q|(p-1), \alpha^{(p-1)/q} \equiv 1 \bmod p$.

Ex.4 Prime vs. irreducible

1. In an integral domain, in a commutative ring, we assume that a reducible prime element $p = mn$, where m, n are non-zero, non-invertible elements. $x = am$, $y = bn$, where a, $b \neq 0$. If $m \nmid b$, $n \nmid a$, then $p \nmid am$ and $p \nmid bn$, i.e., $p \nmid x$ and $p \nmid y$, which leads to a contradiction to (*).

2. In $\mathbb{Z}$, we assume that a irreducible integer p is not prime and $p > 1$, then p cannot be represented as $p = mn$, where m, $n > 1$. If $a|p$, then it implies $a = 1$ or $a = p$, which leads to a contradiction to (**).

3. According to (**), any irreducible integer in $\mathbb{Z}$ is prime. If $p \in \mathbb{Z}$ is prime, then for $a|p$, only $a = 1$ or $a = p$ satisfy. We assume that $p|(x, y)$ cannot imply $p|x$ or $p|y$. However, when $x = 1$, $y = p$ it satisfy, which leads to a contradiction to (*).

4. According to (*), any prime integer in $\mathbb{Z}$ is irreducible. If $p \in \mathbb{Z}$ is prime, then for all x, $y \in \mathbb{Z}$, $p|(x \cdot y)$ implies $p|x$ or $p|y$. We assume that there exist a, $b \in \mathbb{Z}$ so that $p = ab$ and a, $b > 1$. Then $p|(a, b)$ but neither $p|a$ nor $p|b$, which leads to a contradiction to (**).

   Both (**)$\Rightarrow$ (*) and (*)$\Rightarrow$ (**) stand for integers, hence $(*)$ and $(**)$ are equivalent for integers.

Ex.5 Primitive root mod 65537

1. $$\left(\frac{3}{65537}\right) \equiv 3^{32768} \bmod 65537$$

   According to modular exponentiation, calculated by online Modular exponentiation calculator

   $$3^{32768} \equiv -1 \bmod 65537$$

2. According to 1., $3^{32768} \not\equiv 1 \bmod 65537$.

3. Because 2 is a generator of $U(\mathbb{Z}/65537\mathbb{Z})$.