VE475 Introduction to Cryptography
Homework 4

Jiang, Sifan
jasperrice@sjtu.edu.cn
515370910040

June 14, 2019

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 $i \equiv 0 \mod 4$, $K(i) = K(i-4) \oplus T(K(i-1))$.

Ex. 3 - Simple questions

Ex. 4 - Prime vs. irreducible

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.