Network Security Technology Spring, 2019
Tutorial 2, Week 3 (March 13) LIU Zhen
Due Date: March 20

Questions:

1. **Euclidean Algorithm (15 points)**:

   (a) Determine whether 227 and 79 are relatively prime.

   (b) Determine whether 22337 and 17241 are relatively prime.

   Solution

   (a) We use the Euclidean algorithm to calculate the greatest common divisor:

$$\begin{aligned}227 &= 2 \cdot 79 + 69\\ 79 &= 1 \cdot 69 + 10\\ 69 &= 6 \cdot 10 + 9\\ 10 &= 1 \cdot 9 + 1\\ 9 &= 9 \cdot 1 + 0\end{aligned}$$

   We have $\gcd(227, 79) = 1$ and 227 and 79 are thus relativey prime.

   (b) Using the Euclidean algorithm:

$$\begin{aligned}22337 &= 1 \cdot 17241 + 5096\\ 17241 &= 3 \cdot 5096 + 1953\\ 5096 &= 2 \cdot 1953 + 1190\\ 1953 &= 1 \cdot 1190 + 763\\ 1190 &= 1 \cdot 763 + 427\\ 763 &= 1 \cdot 427 + 336\\ 427 &= 1 \cdot 336 + 91\\ 336 &= 3 \cdot 91 + 63\\ 91 &= 1 \cdot 63 + 28\\ 63 &= 2 \cdot 28 + 7\\ 28 &= 4 \cdot 7 + 0\end{aligned}$$

   We find that $\gcd(22337, 17241) = 7$, and thus 22337 and 17241 are not relatively prime.

2. **Extended Euclidean Algorithm (15 points)**:

   (a) Find the multiplicative inverse of $4565 \mod 15447$.

   (b) Without calculating anything, by simply looking at the numbers, can you tell whether $7932 \mod 11458$ has a multiplicative inverse? Explain.

   Solution

(a) We use the Extended Euclidean Algorithm:

$$\begin{aligned}
15447 &= 3 \cdot 4565 + 1752 \\
4565 &= 2 \cdot 1752 + 1061 \\
1752 &= 1 \cdot 1061 + 691 \\
1061 &= 1 \cdot 691 + 370 \\
691 &= 1 \cdot 370 + 321 \\
370 &= 1 \cdot 321 + 49 \\
321 &= 6 \cdot 49 + 27 \\
49 &= 1 \cdot 27 + 22 \\
27 &= 1 \cdot 22 + 5 \\
22 &= 4 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

We have $\gcd(15447, 4565) = 1$ and a multiplicative inverse exists. We then reverse the process:

$$\begin{aligned}
1 &= 5 - 2 \cdot 2 = 5 - 2 \cdot (22 - 4 \cdot 5) = 9 \cdot 5 - 2 \cdot 22 \\
&= 9 \cdot (27 - 1 \cdot 22) - 2 \cdot 22 = 9 \cdot 27 - 11 \cdot 22 \\
&= 9 \cdot 27 - 11 \cdot (49 - 1 \cdot 27) = 20 \cdot 27 - 11 \cdot 49 \\
&= 20 \cdot (321 - 6 \cdot 49) - 11 \cdot 49 = 20 \cdot 321 - 131 \cdot 49 \\
&= 20 \cdot 321 - 131 \cdot (370 - 1 \cdot 321) = 151 \cdot 321 - 131 \cdot 370 \\
&= 151 \cdot (691 - 1 \cdot 370) - 131 \cdot 370 = 151 \cdot 691 - 282 \cdot 370 \\
&= 151 \cdot 691 - 282 \cdot (1061 - 1 \cdot 691) = 433 \cdot 691 - 282 \cdot 1061 \\
&= 433 \cdot (1752 - 1 \cdot 1061) - 282 \cdot 1061 = 433 \cdot 1752 - 715 \cdot 1061 \\
&= 433 \cdot 1752 - 715 \cdot (4565 - 2 \cdot 1752) = 1863 \cdot 1752 - 715 \cdot 4565 \\
&= 1863 \cdot (15447 - 3 \cdot 4565) - 715 \cdot 4565 = 1863 \cdot 15447 - 6304 \cdot 4565
\end{aligned}$$

The modular inverse of $4565 \mod 15447$ is -6304 which is equivalent to **9143**.

(b) We can see that both numbers are even, this means that both of them have at least 2 as a divisor and are therefore not relatively prime. Thus no multiplicative inverse exists.

3. **Euler Phi Function (10 points)**:

   (a) Show the steps of how to calculate $\phi(210)$.

   Solution

   (a) It is easily observable that 210 is not a prime number (an obvious prime factor is 5), and we determine the prime factors to be $2 \cdot 3 \cdot 5 \cdot 7 = 210$. Using the properties of the Euler Phi function, we calculate:

$$\phi(210) = \phi(2) \cdot \phi(3) \cdot \phi(5) \cdot \phi(7) = 1 \cdot 2 \cdot 4 \cdot 6 = 48$$

4. **Fermat's Little Theorem/Euler's Generalization (15 points)**:

(a) Show how to calculate $227^{54996213} \mod 21$ using Euler's generalization.

Solution

(a) Euler's generalization says $a^{\phi(n)} \equiv 1 \mod n$ if a is relatively prime to n. This means that for $a^x \mod n$, when a is relatively prime to n, we can calculate $a^{x \mod \phi(n)} \mod n$ instead. To illustrate this, consider $3^6 \mod 5$:

$$\begin{aligned} 3^6 \mod 5 &= (3^4 \cdot 3^2) \mod 5 = (3^{\phi(5)} \cdot 3^2) \mod 5 \overset{\overset{\text{Euler}}{\downarrow}}{=} (1 \cdot 3^2) \mod 5 \\ &= 3^2 \mod 5 = 9 \mod 5 = 4 \end{aligned}$$

We can indeed verify that $3^6 \mod 5 = 729 \mod 5 = 4$.
Coming back to the present example, we have:

$$54996213 \mod \phi(21) = 54996213 \mod 12 = 9$$

and thus

$$17^{54996213} \mod 21 = 17^9 \mod 21 = 118'587'876'497 \mod 21 = 20$$

5. **Modular Exponentiation (20 points)**

(a) Calculate $17^{27} \mod 23$ using the square and multiply method.

(b) Consider the following two cases of raising a number to a certain exponent:

- $a^{65535} \mod b$
- $a^{65537} \mod b$

Using the square and multiply method, which one of these two exponentiations will be significantly more expensive? Why? Calculate the total number of modular multiplications required for each case (counting a squaring operation as a modular multiplication).

Solution

(a) We first square 17 several times mod 23:

$$\begin{aligned} 17^2 &\mod 23 = 13 \\ 17^4 &\mod 23 = (17^2)^2 \mod 23 = (13)^2 \mod 23 = 8 \\ 17^8 &\mod 23 = (17^4)^2 \mod 23 = (8)^2 \mod 23 = 18 \\ 17^{16} &\mod 23 = (17^8)^2 \mod 23 = (18)^2 \mod 23 = 2 \end{aligned}$$

Putting appropriate terms together we get:

$$\begin{aligned} 17^{27} \mod 23 &= 17^{16} \cdot 17^8 \cdot 17^2 \cdot 17 \mod 23 \\ &= 2 \cdot 18 \cdot 13 \cdot 17 \mod 23 = \mathbf{21} \end{aligned}$$

(b) To answer this question let's look at the binary form of the two exponents:

$$\begin{aligned} 65535 &= \{1111\ 1111\ 1111\ 1111\}_b \\ 65537 &= \{1\ 0000\ 0000\ 0000\ 0001\}_b \end{aligned}$$

With the square and multiply method, the total number of modular multiplications depends on the number of 1 bits in the exponent. As we can see, 65535 has 16 bits set to 1, 65537 only 2. Taking the modular exponentiation with 65535 as the exponent is thus more expensive.
To calculate the total number of modular multiplications necessary we have to include the multiplications for the squaring operations and the multiplications of the individual terms. For the exponent 65535 we need 30 modular multiplications (15 for squaring and 15 for collecting the terms). For the exponent 65537 we only need 17 multiplications (16 for squaring and 1 for collecting the terms).

6. **Group (10 points)**

   (a) Which of the following sets form a multiplicative group? How can you tell?

   - $\mathbb{Z}_{11} \setminus \{0\}$
   - $\mathbb{Z}_{15} \setminus \{0\}$
   - $\mathbb{Z}_{69} \setminus \{0\}$
   - $\mathbb{Z}_{79} \setminus \{0\}$

   Solution

   (a) For sets of the form $\mathbb{Z}_n \setminus \{0\}$ it is enough to check whether n is prime or not.

   - $\mathbb{Z}_{11} \setminus \{0\}$: Yes (11 is prime)
   - $\mathbb{Z}_{15} \setminus \{0\}$: No (15 is not prime)
   - $\mathbb{Z}_{69} \setminus \{0\}$: No (69 is not prime)
   - $\mathbb{Z}_{79} \setminus \{0\}$: Yes (79 is prime)

7. **Cyclic Group (15 points)** Determine whether the following groups are cyclic. If they are, give a generator of the group.

   - $(\mathbb{Z}_5, +)$ (i.e., the set of numbers modulo 5 with addition as the group operation)
   - $(\mathbb{Z}_8^*, *)$
   - $(\mathbb{Z}_{13}^*, *)$

   Solution

   - $(\mathbb{Z}_5, +)$ is a cyclic group, as 1 generates all elements of the group, i.e.,

$$
\begin{aligned}
1 &= 1 \\
2 &= 1 + 1 \\
3 &= 1 + 1 + 1 \\
4 &= 1 + 1 + 1 + 1 \\
0 &= 1 + 1 + 1 + 1 + 1
\end{aligned}
$$

   In fact, every non-zero element of the group is a generator.

- $\mathbb{Z}_8^*$ is not a cyclic group. We know that $\mathbb{Z}_8^*$ consists of $\{1, 3, 5, 7\}$, but we have

  $$\begin{aligned} \langle 1 \rangle &= \{1\} \\ \langle 3 \rangle &= \{1, 3\} \\ \langle 5 \rangle &= \{1, 5\} \\ \langle 7 \rangle &= \{1, 7\} \end{aligned}$$

  Because none of the elements of $\mathbb{Z}_8^*$ is a generator, $\mathbb{Z}_8^*$ is not a cyclic group.
- $\mathbb{Z}_{13}^*$ must be cyclic because 13 is prime. We are left to find at least one generator, for example 2, which creates the group: $\{2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1\}$.