COMP 2711 Discrete Mathematical Tools for Computer Science
2022 Fall Semester – Tutorial 9

Question 1: Evaluate $1819^{13} \pmod{2537}$). Show the steps of fast modular exponentiation.

Solution : By repeated squaring method, we have

$$\begin{aligned} 1819^{2^0} \bmod 2537 &= 1819 \\ 1819^{2^1} \bmod 2537 &= 1819^2 \bmod 2537 = 513 \\ 1819^{2^2} \bmod 2537 &= 513^2 \bmod 2537 = 1858 \\ 1819^{2^3} \bmod 2537 &= 1858^2 \bmod 2537 = 1844 \end{aligned}$$

Note that $13 = 2^0 + 2^2 + 2^3$. Therefore, $1819^{13} \equiv 1819^{2^3} \cdot 1819^{2^2} \cdot 1819^{2^0} \equiv 1844 \cdot 1858 \cdot 1819 \equiv 2081 \pmod{2537}$.

Question 2: Compute each of the following. Show or explain your work. Do not use a calculator or computer.

1) $15^{96} \bmod 97$.
2) $67^{72} \bmod 73$.
3) $67^{73} \bmod 73$.

Solution : 97 and 73 are prime numbers. Use Fermat's Little Theorem to get the following:

1) $15^{96} \bmod 97 = 1$.
2) $67^{72} \bmod 73 = 1$.
3) $67^{73} \bmod 73 = 67 \cdot 67^{72} \bmod 73 = 67 \cdot 1 = 67$.

Question 3: (a) Use Fermat's Little Theorem to show that, if an integer a is not divisible by any of 3, 5, and 7, then

$$a^{49} \equiv a \pmod{105}.$$

(b) Use part (a) to calculate

$$4^{385} \bmod 105.$$

Solution : (a) Note that $105 = 3 \times 5 \times 7$.

$a^{49} \equiv a^{24*(3-1)+1} \equiv a \pmod 3$ by Fermat's Little Theorem;

$a^{49} \equiv a^{12*(5-1)+1} \equiv a \pmod 5$ by Fermat's Little Theorem;

$a^{49} \equiv a^{8*(7-1)+1} \equiv a \pmod 7$ by Fermat's Little Theorem;

Use a simple property of prime numbers: if q and q are both primes and $p|z$, $q|z$, then $pq|z$.

From the first two equations, we have

$$\begin{aligned} a^{49} &\equiv a \pmod{3 \times 5} \\ &\equiv a \pmod{15}. \end{aligned}$$

Similarly, from the third equation and the above derived equation, we have

$$\begin{aligned} a^{49} &\equiv a \pmod{15 \times 7} \\ &\equiv a \pmod{105}. \end{aligned}$$

(b) By the result of (a),

$$\begin{aligned} 4^{385} \bmod 105 &= 4^{7*49+42} \bmod 105 \\ &= ((4^{7*49} \bmod 105) \times 4^{42}) \bmod 105 \\ &= (4^7 \times 4^{42}) \bmod 105 \\ &= 4^{49} \bmod 105 \\ &= 4 \bmod 105 = 4. \end{aligned}$$

Question 4: This problem is on the RSA algorithm for public key cryptography. To generate his keys, Bob starts by picking $p = 37$ and $q = 31$. So, $n = pq = 1147$ and $T = (p-1)(q-1) = 1080$.

(a) Bob's public key is a pair $(e, 1147)$. Which of the following integers can Bob use for e? Why?

(i) 17; (ii) 5; (iii) 49; (iv) 21.

(b) Suppose Bob chooses $e = 47$. Compute his private key d by running the extended GCD algorithm. Show all the steps.

Solution : (a) (i),(iii). This is because they are the only ones that are relatively prime to T, that is, $gcd(e, T)$ must be 1. (ii) fails because 1080 and 5 are both divisible by 5. (iv) fails because 1080 and 21 are both divisible by 3.

(b) The private key should satisfy $(ed) \bmod T = 1$. i.e. d is multiplicative inverse of e in Z_T. Run the extended GCD algorithm to find d:

$$\begin{aligned} 1080 &= 47 \cdot 22 + 46 \\ 47 &= 46 \cdot 1 + 1 \end{aligned}$$

Then,

$$\begin{aligned} 1 &= 47 - 46 \\ &= 47 - (1080 - 47 \cdot 22) \\ &= 23 \cdot 47 + 1080 \cdot (-1) \end{aligned}$$

Thus, $d = 23$.

Question 5: Consider the following simplified version of the RSA algorithm for public cryptography:

(i) Bob's public key is a pair (n, e), where n is a prime number and e is a positive integer that is smaller than n and is relatively prime with $n - 1$.

(ii) Bob's private key is $d = e^{-1} \bmod (n - 1)$.

(iii) Alice encrypts a message m $(0 < m < n - 1)$ by calculating $c = m^e \bmod n$, and sends the ciphertext c to Bob.

(iv) Bob decrypts the ciphertext c by calculating $c^d \bmod n$.

Suppose $n = 251$ and $e = 137$.

(a) Calculate d using the extended GCD algorithm. Show the computational steps.

(b) Suppose $m = 200$. Calculate $c = m^e \bmod n$ using repeated squaring. Show the computational steps.

(c) Is the system secure? Explain why or why not.

Solution : (a) Note that $n - 1 = 250$ and $e = 137$. We use the extended GCD algorithm.

$$\begin{aligned} 250 &= 137 \cdot 1 + 113 \\ 137 &= 113 \cdot 1 + 24 \\ 113 &= 24 \cdot 4 + 17 \\ 24 &= 17 \cdot 1 + 7 \\ 17 &= 7 \cdot 2 + 3 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

So, gcd(250, 137) = 1. Thus, 250 and 137 are relatively prime.
Rewriting:

$$\begin{aligned}
113 &= 250 - 137 \cdot 1 \\
24 &= 137 - 113 \cdot 1 \\
17 &= 113 - 24 \cdot 4 \\
7 &= 24 - 17 \cdot 1 \\
3 &= 17 - 7 \cdot 2 \\
1 &= 7 - 3 \cdot 2
\end{aligned}$$

Substituting:

$$\begin{aligned}
1 &= 7 - (17 - 7 \cdot 2) \cdot 2 \\
&= 7 \cdot 5 - 17 \cdot 2 \\
&= (24 - 17 \cdot 1) \cdot 5 - 17 \cdot 2 \\
&= 24 \cdot 5 - 17 \cdot 7 \\
&= 24 \cdot 5 - (113 - 24 \cdot 4) \cdot 7 \\
&= 24 \cdot 33 - 113 \cdot 7 \\
&= (137 - 113 \cdot 1) \cdot 33 - 113 \cdot 7 \\
&= 137 \cdot 33 - 113 \cdot 40 \\
&= 137 \cdot 33 - (250 - 137 \cdot 1) \cdot 40 \\
&= 137 \cdot 73 + 250 \cdot -40
\end{aligned}$$

Therefore the linear combination is $1 = 137 \cdot 73 + 250 \cdot -40$. The inverse of 137 in Z_{250} is 73 mod 250 = 73. Thus, $d = 73$.

(b) $200^{2^0} \bmod 251 = 200$
$200^{2^1} \bmod 251 = 200^2 \bmod 251 = 91$
$200^{2^2} \bmod 251 = 91^2 \bmod 251 = 249$
$200^{2^3} \bmod 251 = 249^2 \bmod 251 = 4$
$200^{2^4} \bmod 251 = 4^2 \bmod 251 = 16$
$200^{2^5} \bmod 251 = 16^2 \bmod 251 = 5$
$200^{2^6} \bmod 251 = 5^2 \bmod 251 = 25$
$200^{2^7} \bmod 251 = 25^2 \bmod 251 = 123$
Note that $137 = 2^0 + 2^3 + 2^7$.
Therefore, $200^{137} \equiv 200^{2^0} \cdot 200^{2^3} \cdot 200^{2^7} \equiv 200 \cdot 4 \cdot 123 \equiv 8 \pmod{251}$.

(c) No. The system is not secure. As the public key is (n, e), the attacker could compute $n - 1$ from n, then compute d as the inverse of e in Z_n.