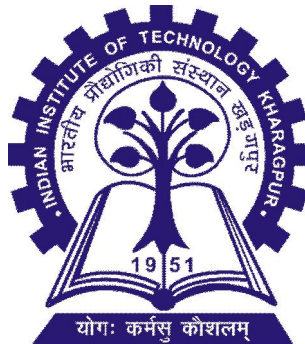


Cryptography and Network Security (CS60065) AUTUMN, 2021-2022

TA: Tapadyoti Banerjee

**Course Instructor: Prof. Dipanwita Roy Chowdhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur
West Bengal 721302, India**



**TUTORIAL: 3
DATE: 1st October 2021**

tapadyoti@iitkgp.ac.in

QUESTION : 1 (Fermat's theorem)

Using Fermat's theorem, find $3^{201} \bmod 11$.

$$(3^{10})^{20} \times 3 = 3 \pmod{11}$$

QUESTION : 2 (Euler's Totient Function)

Determine the following:

(a) $\Phi(41) = 40$

(b) $\Phi(231) = 120$

QUESTION : 3 (Euler's Theorem)

Suppose $a = 3$, $n = 10$, find $a^{\Phi(n)}$

For every a and n that are relatively prime:
 $a^{\phi(n)} \equiv 1 \pmod{n}$

$a=3, n=10$

$\phi(10)=\phi(5) \times \phi(2) = 4$

$3^4 =$

$a=2, n=11$

$2^{10} \equiv 1 \pmod{11}$

m_1, m_2, \dots, m_k
 a_1, a_2, \dots, a_k
modulo m , $m = m_1 m_2 \dots m_k$

QUESTION : 4 (The Chinese Remainder Theorem)

Solve the simultaneous congruences

$$x \equiv 6 \pmod{11}, x \equiv 13 \pmod{16}, x \equiv 9 \pmod{21}, x \equiv 19 \pmod{25}.$$

11, 16, 21, 25 are pairwise relatively prime

$$m = 11 \times 16 \times 21 \times 25 = 92400$$

4

$$m_1=11, m_2=16, m_3=21, m_4=25$$
$$a_1=6, a_2=13, a_3=9, a_4=19$$

$$z_1 = m/m_1 = m_2 \times m_3 \times m_4$$

$$z_2 = m/m_2 = m_1 \times m_3 \times m_4$$

$$z_3 = m/m_3 = m_1 \times m_2 \times m_4$$

$$z_4 = m/m_4 = m_1 \times m_2 \times m_3$$

$$y_1 = z_1^{-1} \pmod{m_1}$$

$$y_2 = z_2^{-1} \pmod{m_2}$$

$$y_3 = z_3^{-1} \pmod{m_3}$$

$$y_4 = z_4^{-1} \pmod{m_4}$$

$$w_1 = y_1 z_1 \pmod{m}$$

$$w_2 = y_2 z_2 \pmod{m}$$

$$w_3 = y_3 z_3 \pmod{m}$$

$$w_4 = y_4 z_4 \pmod{m}$$

$$x = a_1 w_1 + a_2 w_2 + a_3 w_3 + a_4 w_4 \pmod{m}$$

p prime,
 a a primitive element modulo p
 $b = Z_p^*$

$$b = a^i$$
$$0 \leq i \leq (p-2)$$

$$(p-1)/(\gcd(p-1, i))$$

QUESTION : 5 (Z_p^* and cyclic group)

Suppose $p = 13$. Find how many primitive elements are there in modulo 13.
And, examine it for 2.

$$2^0 \bmod 13 = 1$$

$$2^1 \bmod 13 = 2$$

$$2^2 \bmod 13 = 4$$

$$2^3 \bmod 13 = 8$$

$$2^4 \bmod 13 = 3$$

$$2^5 \bmod 13 = 6$$

$$2^6 \bmod 13 = 12$$

$$2^7 \bmod 13 = 11$$

$$2^8 \bmod 13 = 9$$

$$2^9 \bmod 13 = 5$$

$$2^{10} \bmod 13 = 10$$

$$2^{11} \bmod 13 = 7$$

$$2^{12} \bmod 13 = 1 = 2^0 \bmod 13$$

The element 2^i is primitive if and only if $\gcd(i, 12) = 1$

$$i = 1, 5, 7, 11$$

$$2^i$$

$$2, 6, 11, 7$$

2, 6, 7, 11 these are the primitive elements modulo 13

$$M = 88$$

$$C = 88^7 \bmod 187$$

$$= [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$$

$$88^1 \bmod 187 = 88$$

$$88^2 \bmod 187 = 77$$

$$88^4 \bmod 187 = 132$$

QUESTION : 6 (RSA Algorithm)

Consider the keys: public key $PU = \{7, 187\}$ and private key $PR = \{23, 187\}$.
Now, use these keys for a plaintext input of $M = 88$, determine the ciphertext and also decrypt it.

Select p, q : p, q both prime, $p \neq q$

Calculate $n = p \times q$

Calculate $\phi(n) = (p-1)(q-1)$

select integer e : $\gcd(\phi(n), e) = 1$; $1 < e < \phi(n)$

Calculate d : $d = e^{-1} \pmod{\phi(n)}$

Public key: $PU = \{e, n\}$

Private key: $PR = \{d, n\}$

Encryption: Plaintext: M

Ciphertext: $C = M^e \bmod n$

Decryption: Ciphertext: C

Plaintext: $C^d \bmod n = M$

$$C=11$$

$$M = 11^{23} \bmod 187 =$$

1
2
4
8
8