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} mod 11.

(3^(10))^(20) x 3 = 3 (mod 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))= 1(mod n)

a=2, n=11

1 (mod 11)

a=3, n=10
phi(10)=phi(5)x phi(2) = 4

3^4 =

$m1, m2, \ldots mk$
$a1, a2, \ldots ak$
modulo m, $m = m1m2 \ldots mk$

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
$m1=11$, $m2=16$, $m3=21$, $m4=25$
$a1=6$, $a2=13$, $a\,3=9$, $a4=19$

$z1 = m/m1 = m2 \times m3 \times m4$
$z2 = m/m2 = m1 \times m3 \times m4$
$z3 = m/m1 = m1 \times m2 \times m4$
$z4 = m/m4 = m1 \times m2 \times m3$

$y1 = z1\text{^}(-1) \pmod{m1}$
$y2 = z2\text{^}(-1) \pmod{m2}$
$y3 = z3\text{^}(-1) \pmod{m3}$
$y4 = z4\text{^}(-1) \pmod{m4}$

$w1 = y1z1 \pmod{m}$
$w2 = y2z2 \pmod{m}$
$w3 = y3z3 \pmod{m}$
$w4 = y4z4 \pmod{m}$

$x = a1w1 + a2w2 + a3w3 + a4w4 \pmod{m}$

p prime,
a primitive element modulo p
b = Zp*

b=a^i
0<=i<=(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 mod 13 = 1
2^1 mod 13 = 2
2^2 mod 13 = 4
2^3 mod 13 = 8
2^4 mod 13 = 3
2^5 mod 13 = 6
2^6 mod 13 = 12
2^7 mod 13 = 11
2^8 mod 13 = 9
2^9 mod 13 = 5
2^10 mod 13 = 10
211 mod 13 = 7
2^12 mod 13 = 1 = 2^0 mod 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 mod 187
= [(88^4 mod 187) x (88^2 mod 187) x (88^1 mod 187)] mod 187

88^1 mod 187 = 88
88^2 mod 187 = 77
88^4 mod 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!= q
Calculate n = p x 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) (mod phi(n))

Public key: PU = {e, n}
Private key: PR = {d, n}

Encryption: Plaintext: M
Ciphertext: C = M^e mod n

Decryption: Ciphertext: C
Plaintext: C^d mod n = M

C=11

M = 11^23 mod 187 =

1
2
4
8
8