SIDDAGANGA INSTITUTE OF TECHNOLOGY

TUMKUR - 572 103

ASSIGNMENT SHEET

Name Shreelakshmi A.N Roll No. ..... Reg. No. 1SI16CS102 Subject CNS Date .....

CNS ASSIGNMENT – 11

1] Using Fermat's theorm, find $3^{201} \bmod 11$

$a^{p-1} \equiv 1 \bmod p$

$3^{10} \equiv 1 \bmod 11 \Rightarrow 3^{10} \bmod 11 = 1$

$3^2 \bmod 11 = 9$

$3^4 \bmod 11 = 4$

$3^8 \bmod 11 = 5$

$3^{10} \bmod 11 = (5 \times 9) \bmod 11$

$= 1$

$3^{201} \bmod 11 = ((3^{10})^{20} - 3) \bmod 11$

$= 3^{2000} \bmod 11 \times 3 \bmod 11$

$= (2 \times 3) \bmod 11$

$3^{201} \bmod 11 \Rightarrow 3$

2] Use fermat's theorm to find a number a b/w 0 & 72 which a congruent to 9^{794} modulo 73

$a^p \bmod p \equiv a$

$9^{794} \bmod 73 = a$

$a \equiv 12$

3] Use fermat's theorm to find a number 'x' b/w 0 & 28 with x^{85} congruent to 6 modulo 29.

$x^{85} \equiv 6 \bmod 29 \Rightarrow x^{85} \bmod 29 = 6$

w.k.t $a^{p-1} \bmod p = 1$

$x^{28} \bmod 29 = 1$

$(x^{28})^2 \bmod 29 = 1$

$(x^{28})^3 \bmod 29 = 1$

$x^{35} \bmod 29 = (x^{34} \cdot x \bmod 29) = 6$

$1 \times x \bmod 29 = 6$

$x \bmod 29 = 6$

By substituting values for x between 1 & 28 we get $x = 6, 21$

i.e., $(6)^{85} \bmod 29 = 6$ & $(21)^{85} \bmod 29 = 1$

$6^{85} \bmod 29 \equiv 6 \bmod 29$ & $21^{85} \equiv 6 \bmod 29$.

4] Use Euler's theorm to find a number a between 0 & 9 such that it is congruent to 7^{1000} modulo 10.

By Euler's theorm we have,

number relatively prime to 10

$10 = \{1, 3, 7, 9\}$

$7^{\phi(n)} \equiv 1 \bmod n$

$7^{\phi(10)} \equiv 1 \bmod 10$

$7^4 \equiv 1 \bmod 10$

find for 7^{1000}

$\Rightarrow (7^4)^{250} \bmod 10 = 1$

5] Use Euler's theorm to find or number x b/w 0 & 28 with x^{85} congruent to 6 modulo 35

$x^{85} \equiv 6 \bmod 35$

Acc to Euler's theorm

$x^{\phi(n)} \equiv 6 \bmod n$

$x^{\phi(35)} \equiv 6 \bmod 35$

$x^{29} \equiv 6 \bmod 35$

$35^- = \{1, 2, 3, 4, 6, 8, 9, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20, 21, 22, 23, 24, 26, 27, 29, 30, 31, 32, 33, 34\}$

$\Rightarrow x = 6$

$(6)^{85} \equiv 6 \bmod 35$

SIDDAGANGA INSTITUTE OF TECHNOLOGY

TUMKUR - 572 103

ASSIGNMENT SHEET

Name ..... Roll No. ..... Reg. No. ..... Subject ..... Date .....

6] Perform Encryption & decryption using RSA algorithm, for the following.

a] $p=3,\ q=11,\ e=7,\ m=5$?-

$n = p \times q = 3 \times 11 = 33$

$\phi(n) = (p-1)(q-1) = 2 \times 10 = 20$

$d = e^{-1} \bmod (\phi(n))$

$= 7^{-1} \bmod 20$

$\boxed{d = 3}$

$C = M^e \bmod n$

$= (5)^7 \bmod 33$

$\boxed{C = 14}$

$M = (C)^d \bmod n$

$= (14)^3 \bmod 33$

$\boxed{m = 5}$

q	r_1	r_2	r	t_1	t_2	t
2	20	7	6	0	1	-2
1	7	6	1	1	-2	3
6	6	1	0	-2	3	-20
	1	0		3	-20	

b] $p=5,\ q=11,\ e=3,\ m=9$

$n = p \times q = 5 \times 11 = 55$

$\phi(n) = (p-1)(q-1) = 4 \times 10 = 40$

$d = e^{-1} \bmod (\phi(n))$

$= 3^{-1} \bmod 40$

$d = -13 \Rightarrow (-13 + 40 \bmod 40) \Rightarrow 27$

$C = m^e \bmod n$

$= (9)^3 \bmod 55$

$\boxed{C = 14}$

$M = (C)^d \bmod n = 14^{27} \bmod 55$

$\boxed{M = 9}$

q	r_1	r_2	r	t_1	t_2	t
13	40	3	1	0	1	-13
3	3	1	0	1	-13	40
	1	0		-13	40	

$14 \bmod 55 = 14$

$14^2 \bmod 55 = 31$

$14^4 \bmod 55 = 26$

$14^8 \bmod 55 = 16$

$14^{16} \bmod 55 = 36$

$14^{27} \bmod 55 = 9$

c] $p = 7,\ q = 11,\ e = 17\quad m = 8$

$n = p \times q = 7 \times 11 = 77$

$\phi(n) = (p-1)(q-1) = 6 \times 10 = 60$

$d = e^{-1} \bmod \phi(n)$

$= (17)^{-1} \bmod 60$

$d = -7$

$d = (-7+60) \bmod 60 = 53$

q	r_1	r_2	r	t_1	t_2	t
3	60	17	9	0	1	-3
1	17	9	8	1	-3	4
1	9	8	1	-3	4	-7
8	8	1	0	4	-7	60
	1	0		-7	60	

$C = M^e \bmod n$

$= (8)^{17} \bmod 77$

$C = 57$

$8^2 \bmod 77 = 64$

$8^4 \bmod 77 = 15$

$8^8 \bmod 77 = 71$

$8^{16} \bmod 77 = 36$

$8^{17} \bmod 77 = (36 \times 8) \bmod 77$

$= 57$

$M = C^d \bmod n$

$= (57)^{53} \bmod 77$

$M = 8$

$57^2 \bmod 77 = 15$

$57^4 \bmod 77 = 71$

$57^8 \bmod 77 = 36$

$57^{16} \bmod 77 = 64$

$57^{32} \bmod 77 = 15$

$57^{48} \bmod 77 = (15 \times 36) \bmod 77 = 1$

$57^{49} \bmod 77 = (1 \times 36) = 36$

$57^{50} \bmod 77 = (36 \times 15) \bmod 77 = 1$

$57^{53} \bmod 77 = (1 \times 15 \times 57) \bmod 77 = 8$

d] $p = 11,\ q = 13,\ e = 11,\ m = 7$

$n = p \times q = 11 \times 13 = 143$

$\phi(n) = (p-1)(q-1) = 10 \times 12 = 120$

$d = e^{-1} \bmod \phi(n)$

$= (11)^{-1} \bmod 120$

$d = 11$

q	r_1	r_2	r	t_1	t_2	t
10	120	11	10	0	1	-10
1	11	10	1	1	-10	11
10	10	1	0	-10	11	-120
	1	0		11	-120	

$C = M^e \bmod n$

$= (7)^{11} \bmod 143$

$C = 106$

$M = C^d \bmod n$

$= (106)^{11} \bmod 143$

$M = 7$

$(106)^2 \bmod 143 = 82$

$(106)^4 \bmod 143 = 3$

$(106)^8 \bmod 143 = 9$

$(106)^{10} \bmod 143 = 23 \times 106 \bmod 143 = 7$

Scanned by CamScanner

SIDDAGANGA INSTITUTE OF TECHNOLOGY
TUMKUR - 572 103
ASSIGNMENT SHEET

Name .... Roll No. .... Reg. No. .... Subject .... Date ....

c) $p = 17$, $q = 31$, $e = 7$ $m = 2$

$n = p \times q = 17 \times 31 = 527$

$\phi(n) = (p-1)(q-1) = 16 \times 30 = 480$

$d = e^{-1} \bmod \phi(n)$

$= 7^{-1} \bmod 480$

$d = -137$

$d = (-137 + 480) \bmod 480$

$d = 343$

$C = M^e \bmod n$

$= 2^7 \bmod 527$

$C = 128$

$M = C^d \bmod n$

$= (128)^{343} \bmod 527$

$M = 2$

q	r_1	r_2	r	t_1	t_2	t
68	480	7	4	0	1	-68
1	7	4	3	1	-68	69
1	4	3	1	-68	69	-137
3	3	1	0	69	-127	
	1	0		-137		

$(128)^2 \bmod 527 = 47$

$(128)^4 \bmod 527 = 101$

$(128)^8 \bmod 527 = 188$

$(128)^{16} \bmod 527 = 35$

$(128)^{32} \bmod 527 = 171$

$(128)^{64} \bmod 527 = (256 \times 188) \bmod 527 = 171$

$(128)^{80} \bmod 527 = 171 \times 188 \bmod 527 = 1$

$(128)^{212} = (128)^{180} \cdot (128)^{153}$

$= (1 \times 171) \bmod 527 = 171$

$(128)^{320} = (171 \times 188) \bmod 527 = 1$

$(128)^{343} = 1 \times 35 \times 101 \times 47 \times 128$

$= 373 \times 47 \times 128$

$= (140 \times 128) \bmod 527$

$(128)^{343} = 2$

Scanned by CamScanner

7] In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5$, $n = 35$. What is plaintext M?

$C = 10$, $e = 5$ $n = 35$, $m = ?$

$C = M^e \bmod n$

$10 = m^5 \bmod 35$

$m = c^d \bmod n$

$m = m^{ed} \bmod n$

Relationship b/w e & d can be Expressed as

$ed \bmod \phi(n) = 1$

$ed \equiv 1 \bmod \phi(n)$

find P & q where $n = 35 = 5 \times 7 \Rightarrow p = 5, q = 7$

$\phi(n) = (p-1)(q-1) = 4 \times 6 = 24$

$\{gcd(24, 5) = 1\}$

$d = e^{-1} \bmod \phi(n)$

$= 5^{-1} \bmod 24$

$\boxed{d = 5}$

$m = e^d \bmod 35$

$= (10)^5 \bmod 35$

$\boxed{m = 5}$

$C = m^e \bmod n$

$= (5)^5 \bmod 35$

$\boxed{C = 10}$

TUMKUR - 572 103

ASSIGNMENT SHEET

Name ..... Roll No. ..... Reg. No. ..... Subject ..... Date .....

GY

8] In an RSA System, the public key of a User is e = 31, n = 3599. What is the private key of this User?

e = 31, n = 3599 d = ?

Prime no. are

$n = p \times q = 59 \times 61 = 3599$

$\phi(n) = (p-1)(q-1) = 3480$

$gcd(3480, 31) = 1$

$d = e^{-1} \bmod \phi(n)$

$= (31)^{-1} \bmod 3480$

$d = -449$

$d = (-449 + 3480) \bmod 3480$

$\boxed{d = 3031}$

q	r_1	r_2	r	t_1	t_2	t
112	3480	31	8	0	1	-112
3	31	8	7	1	-192	337
1	9	7	1	-112	337	-449
7	7	1	0	337	-449	3480
	1	0		-449		

9] Users A & B use the Diffie-Hellman key Exchange technique with a common prime q = 71 and a primitive root a = 7

a) If User A has private key $X_A = 5$, what is A's public key Y_A?

b) If User B has private key $X_B = 12$, what is B's public key Y_B?

c) what is Shared Secret key!

a] $q = 71$, $a = 7$ $X_A = 5$ $Y_A = ?$

$Y_A = a^{kA} \bmod q$

$= (7)^5 \bmod 71$

$\boxed{Y_A = 51}$

b] $q = 71$, $a = 7$ $x_B = 12$, $Y_B = ?$

$Y_B = a^{x_B} \bmod q$

$= (7)^{12} \bmod 71$

$Y_B = 4$

$7^2 \bmod 71 = 49$

$7^4 \bmod 71 = 58$

$7^8 \bmod 71 = 27$

$7^{12} \bmod 71 = 4$

$k = (Y_B)^{k_A} \bmod P$

$= (4)^5 \bmod 71$

$\boxed{k = 30}$

$k = (Y_A)^{k_B} \bmod P$

$= (51)^{12} \bmod 71$

$\boxed{k = 30}$

$(51)^2 \bmod 71 = 45$

$(51)^4 \bmod 71 = 37$

$(51)^8 \bmod 71 = 20$

$(51)^{12} \bmod 71 = 30$

10] Consider a diffie-Hellman Scheme with a common prime $q = 11$ & a primitive root $a = 2$

a) Show that 2 is a primitive root of 11

b) If User A has public key $Y_A = 9$ what is A's private key X_A?

c) If User B has public key $Y_B = 3$ & what is the Secret key k shared with A?

a) 2^i $i = 1, 2, 3 \ldots 10$

no. are 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024 - nos, there no when mod 11 will be 2, 4, 8, 5, 10, 9, 7, 3, 6, 1 respectively.

then no are b/w 1 & 10

b) $Y_A = 9$ $k_A = ?$

$X_A = (\log_2 Y_A) \bmod P$

$= (\log_2 9) \bmod 11$

$\boxed{X_A = 6}$

c) $Y_B = 3$ & $k = ?$

$k = (Y_B)^{X_A} \bmod P$

$= (3)^6 \bmod 11$

$\boxed{k = 3}$