NETWORK SECURITY

ASSIGNMENT (T-4)

Name : Sheikh Mohd Sabir

Class : B.Tech Computer Engineering, 8th sem, 202

RollNo. : 19BCS058

Sol 1. Given, super-increasing tuple b = [7, 11, 19, 39, 79, 157, 313]

r = 37, n = 900 (modulus) and Permutation table = [4, 2, 5, 3, 1, 7, 6]

To encrypt & decrypt (ASCII value of "H") :-

⇒ tuple t = $[t_1, t_2, t_3, \ldots, t_7]$

where $t_i = r * b_i \bmod n$

$t_1 = 37 * 7 \bmod 900 = 259$
$t_2 = 37 * 11 \bmod 900 = 407$
$t_3 = 37 * 19 \bmod 900 = 703$
$t_4 = 37 * 39 \bmod 900 = 543$
$t_5 = 37 * 79 \bmod 900 = 223$
$t_6 = 37 * 157 \bmod 900 = 409$
$t_7 = 37 * 313 \bmod 900 = 781$

(1 2 3 4 5 6 7)

∴ t = [259, 407, 703, 543, 223, 409, 781]

tuple a = permute (t) = using $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 5 & 3 & 1 & 7 & 6 \end{pmatrix}$

= [543, 407, 223, 703, 259, 781, 409]

Now, a is publicly announced, n, r & b are secret.

"H" = 72 (ascii) = [1001000] = x

in 7-bits

Knapsack Sum (a, x)

$a = [543, 407, 223, 703, 259, 781, 409]$

$x = 1\ 0\ 0\ 1\ 0\ 0\ 0$

$sum = 543 + 0 + 0 + 703 + 0 + 0 + 0$

$\Rightarrow S = 1246$

Hence, Encryption done.

Now, Decrypting, $S = 1246$

$S' = S * r^{-1} \bmod n$

$= 1246 * 37^{-1} \bmod 900$

$= 1246 * 73 \bmod 900$

$= 58$

$\because 37 \bmod 900 = 73$

Now, $X' = inv\_knapsackSum(S', b)$

Iterations →

i	S'	b_i	x_i	
7	58	313	0	↑
6	58	157	0	
5	58	79	0	
4	58	39	1	
3	58 ≥ 39 → 58−39 = 19	19	1	X'
2	19 ≥ 19 → 19−19 = 0	11	0	
1	0	7	0	

$r = r - b_i * x_i$

$= 58 - 39 * 1$

$= 0$

```
inv_knapsackSum (S', b) →
{
  for (i = k down to 1)
  {
    if s ≥ bi
    {
      xi ← 1
      S ← s − bi
    }
    else xi ← 0
  }
  return x[1 ..... K]
}
```

$X' = \begin{matrix} 1234567 \\ 0011000 \\ 4253176 \end{matrix}$

$\therefore X = \text{permute}(X') = 1001000 = 64+8 = 72$
$= "H"$

Hence, decryption done.

sol 2. Given, Super-increasing tuple $b = [7, 11, 23, 43, 87, 173, 357]$, $r = 41$, modulus $n = 1001$ and permute = [7,6,5,1,3,2,4] table

Tuple, $t = [t_1, t_2, \ldots, t_7]$

where, $t_i = r * b_i \bmod n$

$t_1 = 41 * 7 \bmod 1001 = 287$
$t_2 = 41 * 11 \bmod 1001 = 451$
$t_3 = 41 * 23 \bmod 1001 = 943$
$t_4 = 41 * 43 \bmod 1001 = 762$
$t_5 = 41 * 87 \bmod 1001 = 564$
$t_6 = 41 * 173 \bmod 1001 = 86$
$t_7 = 41 * 357 \bmod 1001 = 623$

$\therefore$ tuple $t = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ [287, & 451, & 943, & 762, & 564, & 86, & 623] \\ 7 & 6 & 5 & 1 & 2 & 3 & 4 \end{matrix}$

$\Rightarrow$ tuple $a = \text{permute}(t) = [623, 86, 564, 287, 451, 943, 762]$

Now, a is publicly announced (n, r and b are secret)

"d" = 100 (ascii) = [1100100] = x

Knapsack Sum (a, x)

$a = [623, 86, 564, 287, 451, 943, 762]$
$x = [1\ 1\ 0\ 0\ 1\ 0\ 0]$
sum = 623 + 86 + 0 + 0 + 451 + 0 + 0
$\Rightarrow S = 1160$

∴, Ciphertext, S = 1160

Hence, Encryption done.

Now, Decrypting S = 1160

$$S' = S * r^{-1} \bmod n$$
$$= 1160 * 41^{-1} \bmod 1001$$
$$= 159 * 293 \bmod 1001$$
$$= 541$$

Now, X' = inv_knapsack_sum (S', b)

i	S'	b_i	x_i
7	541	357	1
6	184	173	1
5	11	87	0
4	11	43	0
3	11	23	0
2	11	11	1
1	0	7	0

∴, X' = [0 1 0 0 0 1 1]
(1 2 3 4 5 6 7 ; 7 6 5 1 2 3 4)

= [1 1 0 0 1 0 0]

= 64 + 32 + 4

= 100

= "d"

Hence, Decryption done.

Sol 3. p = 11, q = 19 for RSA :-

1. public key = 9
2. private key = 9
3. Encrypt & Decrypt "TO".

∴, $n = p * q = 11 * 19 = 209$

$$\phi(n) = (p-1) * (q-1) = (11-1) * (19-1) = 180$$

Now, choose 2 exponents e & d from Z_{180} such that $1 < e < \phi(n)$ and e is coprime to $\phi(n)$.
and,

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

Let, $e = 13$ then, $d = 13^{-1} \bmod 180 = 97$
∴, (e, n) i.e., (13, 209) is public key and d = 97 is private key

Now, Encryption Process

Cipher text, $C = P^e \bmod n$, P = Plain Text
$= 19^{13} \bmod 209$ = "TO"
$= 171$ = "19 14"

&

$= 14^{13} \bmod 209$
$= 192$

Now, Decryption Process

Plain text, $P = C^d \bmod n$
$= (171)^{97} \bmod 209$
$= 19$ = "T"

&

$= (192)^{97} \bmod 209$
$= 14$ = "O"

Aniket
Date
Page

Sol 4. Given, $e = 17$, $n = 187$, $d = ?$

In RSA,

$$n = 187 = 11 * 17$$
$$\phi(n) = (11-1) * (17-1) = 160$$
$$d = e^{-1} \bmod \phi(n) = 17^{-1} \bmod 160 = 113$$

Sol 5. Given, $C = 10$, $e = 5$, $n = 35$

(e, n: public key pair)

In RSA,

$\because n = 35 = 5 * 7$

$\therefore \phi(n) = (5-1) * (7-1) = 24$

Plain Text, $m = C^d \bmod n$

$$\Rightarrow d = e^{-1} \bmod \phi(n) = 5^{-1} \bmod 24 = 5$$

$$\Rightarrow m = 10^5 \bmod 35$$
$$= 5$$

Sol 6. In Rabin Cryptosystem :-

Encrypt & decrypt $P = 24$ (Plain text) using this method where $p = 23$ & $q = 7$

{both are congruent to 3 mod 4}

$\because n = p * q = 23 * 7 = 161$

n is public key while p & q are kept secret

Aniket
Date
Page

Now,

Encryption

Cipher Text $C = P^e \bmod n = 24^2 \cdot \bmod 161$

$= 93$ ✓

Decryption

$a_1 = +(93^{(23+1)/4}) \bmod 23 \quad = +93^6 \bmod 23 = 1 \bmod 23$

$a_2 = -(93^{(23+1)/4}) \bmod 23 \quad = -93^6 \bmod 23 = 22 \bmod 23$

$b_1 = +(93^{(7+1)/4}) \bmod 7 \quad = +93^2 \bmod 7 = 4 \bmod 7$

$b_2 = -(93^{(7+1)/4}) \bmod 7 \quad = -93^2 \bmod 7 = 3 \bmod 7$

So, user A takes four possible answers (a_1, b_1), (a_1, b_2), (a_2, b_1) and (a_2, b_2) and uses Chinese Remainder Theorem (CRT).

The final possible plain-texts are 116, 24, 137 and 45.

$(116^2 \bmod 161 = 93)$ ✓

$(24^2 \bmod 161 = 93)$ ✓

$(137^2 \bmod 161 = 93)$ ✓

$(45^2 \bmod 161 = 93)$ ✓

116 calc.

(a_1, b_1) set 1

$M = m_1 * m_2 = 23 * 7 = 161$

$M_1 = 7, \quad M_2 = 23$

$M_1^{-1} = 7^{-1} \bmod 23 \quad = 10$

$M_2^{-1} = 23^{-1} \bmod 7 \quad = 4$

for set 1, $x = (1 * 7 * 10 + 4 * 23 * 4) \bmod 161$

$= 438 \bmod 161 = 116 \Rightarrow$ Plaintext.

Similar calculations will be done for other sets.

Aniket
Date
Page

Sol 7. In ELGamal :-

we choose, $G = \langle Z_{31}^*, n \rangle$

$\phi(31) = 30$

elements $= \{1, 2, 3, \ldots\ldots, 31\}$
$d = 5$

check for 2 :- $2^1 \bmod 31 = 2$, $2^2 \bmod 31 = 4$, $2^3 = 8$, $2^4 = 16$
$2^5 \bmod 31 = 1$
↑ stop

check for 3 :- $3^1 \bmod 31 = 3$, $3^2 = 9$, $3^3 = 27$, $3^4 = 19$
$3^5 = 26$, ..., $3^{28} = 7$, $3^{29} = 21$
, $3^{30} \bmod 31 = 1$

Hence, 3 is the primary root of 31 (as $ord(3) = \phi(n)$)

∴, $e_1 = 3$, $d = 5$

(a.) $e_2 = e_1^d \bmod p = 3^5 \bmod 31 = 26$

Public key = $(3, 26, 31) \Rightarrow (e_1, e_2, p)$
Private key = $5 \Rightarrow (d)$

Let $r = 6$
$C_1 = e_1^r \bmod p$
$C_2 = (P * e_2^r) \bmod p$

, $p = 31$
$e_1 = 3$
$e_2 = 26$

Aniket
Date
Page

Encryption

Plaintext (P)	C_1	C_2	
H = 7	$3^6 \bmod 31 = 16$	$(7 * 26^6) \bmod 31 = 07$	→ (16, 07)
E = 4	16	04	→ (16, 04)
L = 11	16	11	→ (16, 11)
L = 11	16	11	→ (16, 11)
O = 14	16	14	→ (16, 14)

Decryption

C_1	C_2	Plaintext $(P = (C_2 (C_1^d)^{-1}) \bmod p)$	
16	07	$(7.(16^5)^{-1}) \bmod 31 = 07$	→ H
16	04	04	→ E
16	11	11	→ L
16	11	11	→ L
16	14	14	→ O

Sol 8. $P_1 = 17$, $P_2 = 37$, $r = 9$, $e_1 = 2$, $p = 53$

Eve knows $P_1 = 17$

$P \rightarrow P_1$

$P' \rightarrow P_2$

~~$C_2 = P_1 * e_2^r \bmod 53$~~

$= 17 *$

$C_2 = P * (e_2^r) \bmod p$, $C_2' = P' (e_2^r) \bmod p$

$e_2^r = C_2 P^{-1} \bmod p$, $P' = C_2' (e_2^r)^{-1} \bmod p$

Aniket
Date
Page

$P_1 = 17$

$e_2 = e_1^d \bmod p$
$= 2^3 \bmod 53 = 8$
$\Rightarrow C_2 = (17 * 8^9) \bmod 53$
$= 228170376 \bmod 53$
$= 19$

$P_2 = 37$

$C_2' = (37 * 8^9) \bmod 53$
$= 32$

Eve intercepts $C_2 = 19$ & $C_2' = 32$ & she knows $P_1 = 17$.

$e_2^\gamma = (19 * 17^{-1}) \bmod 53$
$= 19 * 25 \bmod 53$
$= 51$

$P' = C_2' (e_2^\gamma)^{-1} \bmod p$
$= (32 * 51^{-1}) \bmod 53$
$= (32 * 26) \bmod 53$
$= 37$

Hence, Eve knows what P_2 was.
(Plaintext P_2 can be found)

sol 9. Elliptical curve $E_{23}(1,1)$, $P(3,10)$, $Q(9,7)$

(i) value of $P+Q = ?$

$\lambda = (y_2 - y_1) * (x_2 - x_1)^{-1} \bmod 23$

$= (7-10) * (9-3)^{-1} \bmod 23$
$= (-3) * (6)^{-1} \bmod 23$
$= (-3 * 4) \bmod 23$
$= (-12) \bmod 23$
$= 11$

$$x_3 = (\lambda^2 - x_1 - x_2) \bmod 23$$

$$= (121 - 3 - 9) \bmod 23$$

$$= 109 \bmod 23$$

$$= 17$$

$$y_3 = [\lambda(x_1 - x_3) - y_1] \bmod 23$$

$$= (11(3 - 17) - 10) \bmod 23$$

$$= -154 - 10$$

$$= -164 \bmod 23 = 20$$

$$\Rightarrow P + Q = (x_3, y_3) = (17, 20)$$ Ans

(ii) ∞P

$(P + P + P + P$ (adding Points)) $\quad (P = (3, 10))$

$$R = P + P = 2P$$

$$\lambda = (3x_1^2 + a)/2y_1 = (3 \cdot 9 + 1)/20 = 28 * 20^{-1} \bmod 23$$

$$= 5 * 15 \bmod 23 = 6$$

$$x_3 = \lambda^2 - x_1 - x_2 = (36 - 3 - 3) \bmod 23$$

$$= 7$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = (6(3 - 7) - 10) \bmod 23$$

$$= -11 \bmod 23 = 12$$

$$R = (x_3, y_3) = (7, 12)$$

Aniket
Date
Page

$R' = 2R = R+R = 4P$ $\quad (R = (7, 12))$

$\lambda' = ((3 \cdot 7^2 + 1)/24) \bmod 23$

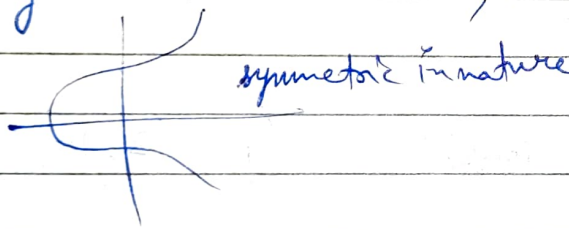
$= 10$

$x_3' = (10^2 - 7 - 7) \bmod 23 = 86 \bmod 23 = 17$

$y_3' = (10 \cdot (7 - 17) - 12) \bmod 23 = -112 \bmod 23 = 3$

$\therefore, \quad R' = 4P = (17, 3)$

sol 10. $y^2 = x^3 + 2x + 9 \quad , \bmod p = 37$



To find the points on the elliptic curve, we can start by substituting different values of x into the equation & solving for y.

$x = 0$

$y^2 = 0^3 + 2.0 + 9 = 0 + 0 + 9 = 9$

$(9)^{18} \bmod 37 = 1$

we check for whether y^2 is a Q.R or not

$y^2 = 9 \bmod 37$ (checking)

i	x	y = 1	a = 9
0	0		7
1	1	7	12
2	0		33
3	0		16
4	1	1	

Hence, 9 is Q.R.

$y^2 = 9 \bmod 37$

$\Rightarrow y = \pm 3 \bmod 37$

for $x = 0$, $y = 3$, $y = 34$

$x = 1$

$y^2 = 1^3 + 2.1 + 9 = 12$

$(12)^{18} \bmod 37 = 1 \longrightarrow$ QR

i	x	y=1	a=12
0	0		33
1	1	33	16
2	0		34
3	0		9
4	1	1	

$y^2 = 12 \bmod 37$

$\Rightarrow y = \pm 7 \bmod 37$

for $x = 1$, $y = 7$, $y = 30$

$x = 2$

$y^2 = 2^3 + 2.2 + 9 = 8 + 4 + 9 = 21$

$(21)^{18} \bmod 37 = 1 \longrightarrow$ QR.

i	x	y=1	a=21
0	0		34
1	1	34	9
2	0		7
3	0		12
4	1	1	33

$y^2 = 21 \bmod 37$

$\Rightarrow y = \pm 13 \bmod 37$

for $x = 2$, $y = 13, y = 24$

Hence, points on the curve are $(0,3), (0,34), (1,7), (1,30), (2,13), (2,24)$.

Sol 11. $y^2+xy = x^3+g^3x^2+b$ is defined over G.F.(2^3) with I.P. $f(x) = x^3+x+1$

$$f(g)=0 \Rightarrow g^3+g+1=0$$
$$\Rightarrow \boxed{g^3 = g+1}, \quad b=1$$

elements $x, y \in \{0, 1, g, g^2, g^3, g^4, g^5, g^6\}$

$(x,y) = \{(0,0), (0,1), (0,g), (0,g^2), (0,g^3), (0,g^4), (0,g^5), (0,g^6),$
$(1,0), (1,1), \ldots$

$(g^6,0), (g^6,1), (g^6,g), (g^6,g^2), (g^6,g^3), (g^6,g^4), (g^6,g^5), (g^6,g^6)$

~~$x=0, y=0$ $\quad y^2+xy = x^3+g^3x^2+1$~~

$x=0, y=0$	$y^2+xy = x^3+g^3x^2+1$	yes/No
0, 0	$0+0.0 = 0+0+1$ ✗	No
0, 1	$1+0 = 0+0+1$ ✓	Yes
1, 0	$0+0 = 1+g^3+1 = g+1$ ✗	No
1, 1	$1+1 = 1+g^3+1 = g+1$ ✗	No
1, g	$g^2+g = 1+g^3+1 = g+1$ ✗	No
1, g^2		
1, g^3		

take all points with "yes"

All the points exist on this curve are :-

$(0,1)$ $(0,1)$
$(g^2,1)$ (g^2,g^6)
(g^3,g^2) (g^3,g^5)
$(g^5,1)$ (g^5,g^4)
(g^6,g) (g^6,g^5)

~~$y^2+xy=x^3+g^3x^2$~~

Sol 12 $y^2+xy=x^3+ax^2+1$ is defined over G.F.(2^3) with I.P. $f(x)=x^3+x+1$

$a=g^3$
$b=1$

$f(g)=0$
$g^3+g+1=0$
$\boxed{g^3=g+1}$

elements $x,y \in \{0,1,g,g^2,g^3,\dots,g^6\}$

$(x,y) = \{(0,0),(0,1),(0,g),(0,g^2),(0,g^3),(0,g^4),(0,g^5),(0,g^6),$
$(1,0),(1,1),(1,g),(1,g^2),(1,g^3),(1,g^4),(1,g^5),(1,g^6),$
$(2,0),\dots$

$(g^6,0),(g^6,1),(g^6,g),(g^6,g^2),(g^6,g^3),(g^6,g^4),(g^6,g^5),(g^6,g^6)\}$

Aniket
Date
Page

$x=0, y=0$	$y^2+xy = x^3+g^3x^2+1$		Yes/No
$0,0$	$0+0 = 0+0+1$	✗	No
$0,1$	$1+0 = 0+0+1$	✓	Yes
$0,g$	$g^2+0 = 0+0+1$	✗	No
$0,g^2$	$g^4+0 = 0+0+1$	✗	No
$0,g^3$	$g^6+0 = 0+0+1$	✗	No
$0,g^4$	$g^8+0 = 0+0+1$	✗	No
$0,g^5$	$g^{10}+0 = 0+0+1$	✗	No
$0,g^6$	$g^{12}+0 = 0+0+1$	✗	No
$1,0$	$0+0 = 1+g^3+1$	✗	No
$1,1$	$1+1 = 1+g^3+1$	✗	No
$1,g$	$g^2+g = 1+g^3+1$	✗	No
$1,g^2$	$g^4+g^2 = 1+g^3+1$	✗	No

$g^2+g = 1+g^3+1 \rightarrow (g+1)$

$g^4+g^2 = 1+g^3+1 \rightarrow g+1$

$(g+1).g+g^2 \rightarrow g+1$

g^2+g^2+1

All the points exists on this curve are :-

$(0,1)$
$(g^2,1)$
(g^3,g^2)
$(g^5,1)$
(g^6,g)

$(0,1)$
(g^2,g^6)
(g^3,g^5)
(g^5,g^4)
(g^6,g^5)

Aniket
Date
Page

Sol 13. $y^2 + xy = x^3 + ax^2 + b$ is defined over $GF(2^4)$ with I.P. $f(x) = x^4 + x + 1$, $a = g^4$, $b = g^0 = 1$

$\Rightarrow f(x) = 0$

$\Rightarrow g^4 + g + 1 = 0$

$\Rightarrow \boxed{g^4 = g + 1}$

The element $g = (0010$ is a generator for the field.

$g^0 = (0001)$

$g^1 = (0010)$

$g^2 = (0100)$

$g^3 = (1000)$

$g^4 = g + 1 = 0010 + 0001 = (0011)$

$\vdots$

$g^{15} = (g^4)^3 \cdot g^3 = (g+1)^3 \cdot g^3 = (g^3 + 1 + g^2 + g) \cdot g^3$

$= g^6 + g^3 + g^5 + g^4 = (g^4 + 1) \cdot g^2 + g^3 + (g+1) \cdot g + g + 1$

$= g^3 + g^2 + g^3 + g^2 + g + g + 1 = 1 = (0001)$

elements $x, y \in \{0, 1, g, g^2, g^3, \ldots, g^{14}\}$

$(x, y) \in \{(0,0), (0,1), (0,g), \ldots, (0, g^{14}),$
$(1,0), (1,1), (1,g), \ldots, (1, g^{14}),$
$\vdots$
$(g^{14}, 0), (g^{14}, 1), (g^{14}, g), \ldots, (g^{14}, g^{14})\}$

Aniket

Date

Page

$x=0, y=0$	$y^2+xy = x^3+g.x^2+1$	L.H.S = R.H.S Yes/No
0,0	$0+0 = 0+0+1$ ✗	No
0,1	$1+0 = 0+0+1$ ✓	Yes
0,g	$g^2+0 = 0+0+1$ ✗	No
		No
		No
$0, g^{14}$	✗	No
1,0	$0+0 = 1+g^4+1$ ✗	No
1,1	$1+1 = 1+g^4+1$ ✗	No
1,g	$g^2+g = 1+g^4+1$ ✗ ($g^4 \to g+1$)	No
$1, g^{12}$		
$1, g^{13}$	$g^{26}+g^{13} = 1+g^4+1$	
	$\Rightarrow (g^4)^6 \cdot g^2 + (g^4)^3 \cdot g = g+1$	
	$\Rightarrow (g+1)^6 \cdot g^2 + (g+1)^3 \cdot g = g+1$	

Aniket
Date
Page

$\Rightarrow g^{260/15} + g^{130/15} = 1 + g^4 + 1$

$\Rightarrow g^{11} + g^{13} = g^4$

$\Rightarrow (1110) + (1101) = (0011)$
(XOR)

$\Rightarrow 0011 = 0011$ ✓ Yes

do for all this

∴, Seven points exists on this curve are :-

$(0, 1)$
$(1, g^{13})$
$(1, g^6)$
(g^3, g^8)
(g^3, g^{13})
(g^5, g^3)
(g^5, g^{11}) ✓