Tutorial - 4

Date

DELTA Pg No.

Q1 Given the super-increasing tuple $b = [7, 11, 19, 39, 79, 157, 313]$ $r = 37$ and modulus $n = 900$, encrypt and decrypt the letter "H" using the knapsack cryptosystem. Use $[4, 2, 5, 3, 1, 7, 6]$ as the permutation table. Use ASCII value for representing H.

Sol^n

Super increasing tuple $b = [7, 11, 19, 39, 79, 157, 313]$ $r = 37$
modulus $n = 900$ and permutation table $= [4\ 2\ 5\ 3\ 1\ 7\ 6]$

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

$$t_i = r \times b_i \bmod n$$

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

$\Rightarrow t = [259, 407, 703, 543, 223, 409, 781]$

tuple $\{a\}$ = permute (t) = (using

1	2	3	4	5	6	7
4	2	5	3	1	7	6

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

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

in ascii $H = 72$ ~~1000110~~

in 7 bits $= [1001000] = x$

$\Rightarrow$ knapsackSum (a, x) $= a\,[543, 407, 223, 703, 259, 781, 409]$
$\times$ 1 0 0 1 0 0 0

(cipher text) $S = 1246 \Leftarrow 543 + 0 + 0 + 703 + 0 + 0 + 0$

$37^{-1} \bmod 900 = 73$

now, decrypting $s = 1246$

$s' = s \times r^{-1} \bmod n = 1246 \times 37^{-1} \bmod 900$
$= (1246 \times 73) \bmod 900 = 58 = s'$

$x' =$ Inv_KnapsackSum (s', b)

Date
DELTA Pg No.

~~but it is 38+19~~ 58

589

inv-knapsacksum (s', b) → { for ($i = k$ to 1)
if $s' \geq b_i$
{ $x_i \leftarrow 1$
$s' \leftarrow s' - b_i$
}
else $x_i \leftarrow 0$
return $x[1 \ldots k]$
}

i	s'	b_i	x_i
7	58	313	0
6	58	157	0
5	58	79	0
4	58	39	1
3	19	19	1
2	0	11	0
1	0	7	0

$$x' = \begin{array}{c} 1\;2\;3\;4\;5\;6\;7 \\ [0\;0\;1\;1\;0\;0\;0] \\ 4\;2\;5\;3\;1\;7\;6 \end{array}$$

x = permute(x') = [1 0 0 1 0 0 0]

= 64 + 8 = 72 = "H"

Q2 b = [7, 11, 23, 43, 87, 173, 357]
r = 41, modulus n = 1001, encrypt/decrypt "d" (ASCII) using knapsack Cryptosystem, permutation table = [7 6 5 1 2 3 4]

tuple t = [t_1, t_2 ..., t_7]
t_1 = (41 × 7) mod 1001 = 287
t_2 = (41 × 11) mod 1001 = 451
t_3 = (41 × 23) mod 1001 = 943
t_4 = 41 × 43 mod 1001 = 762
t_5 = 41 × 87 mod 1001 = 564
t_6 = 41 × 173 mod 1001 = 86
t_7 = 41 × 357 mod 1001 = 623

tuple t = 287, 451, 943, 762, 564, 86, 623
(1 2 3 4 5 6 7)
(7 6 5 1 2 3 4)

tuple a = permute(t) = 623, 86, 564, 287, 451, 943, 762

tuple a is publicly announced →

Date
DELTA Pg No.

encryption

in ascii "d" = 100 = [1100100]

$x = [1\ 1\ 0\ 0\ 1\ 0\ 0]$

$a = [623\ 86\ 564\ 287\ 451\ 943,\ 762]$

Knapsack Sum $(a, x) = 1160 \Leftarrow 623 + 86 + 0 + 0 + 451 + 0 + 0$

cipher text $s = 1160$

decryption:- ~~inv knapsack~~

$s' = (1160 \times 41^{-1}) \bmod 1001$

$= (1160 \times 293) \bmod 1001$

$= 541$

$41^{-1} \bmod 900$
$= 293$

$x' = \text{Inv\_Knapsack}(s', b)$

i	s'	bi	xi
7	541	357	1
6	184	173	1
5	11	87	0
4		43	0
3		23	0
2	11	11	1
1	0	7	0

$$\Rightarrow x' = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ [\begin{matrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{matrix}] \\ \begin{matrix} 7 & 6 & 5 & 1 & 2 & 3 & 4 \end{matrix} \end{array}$$

$x = \text{permute}(x') = [1\ 1\ 0\ 0\ 1\ 0\ 0]$

$= 64 + 32 + 4$

$= 100 = $ "d"

Q3 Using value of $p = 11$ and $q = 19$, for RSA

(i) Find the value of public key (ii) Find the value of private key

(iii) Encrypt and Decrypt the message "TO" using the key generated in (i) and (ii)

Sol (i)

$p = 11,\ q = 19 \Rightarrow n = p \times q = 209$

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

Now choose 2 exponents e and 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 $e = 13 \Rightarrow d = 13^{-1} \bmod 180 = 97$

$(e, n) \to$ public key $\boxed{e = 13}$ publicly announced $n = 209$

$\boxed{d = 97} \Leftarrow$ private key
secret

Date
DELTA Pg No.

(iii) Encryption :- Cipher text = (plaintext^e) mod n

~~Ba~~ plaintext = "TO" = 84 79 (in ASCII)

⇒ Cipher text = $84^{13} \bmod 209$, $79^{13} \bmod 209$

= ~~84 mod~~ 46 52

Decryption: Cipher text = 46 52

plaintext = ~~46~~ $\text{ciphertext}^{d} \bmod n$

De~~cryption~~:- ~~Cipherd~~ = $46^{97} \bmod 209$ $52^{97} \bmod 209$

= 84 79

= "T O"

Q4 In RSA cryptography find d if you know e = 17 and n = 187

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

$d = 17^{-1} \bmod 187$ gcd (17, 187) = 17 ≠ 1

$x \times 17 \bmod 187 = 1$ ⇒ no inverse possible

~~17, 170, 187,~~

Q5 $c = 10$, $\underbrace{e = 5 , n = 35}_{\text{public key}}$, In RSA eve intercept ciphertext c

find plaintext

$p = c^{d} \bmod 35$

$d = 5^{-1} \bmod 35$ again gcd (5, 35) = 5 ≠ 1

⇒ no plain text found. ⇒ no inverse possible.

Q6 In Rabin cryptosystem, user A chooses two prime nos. p = 23, q = 7
encrypt and decrypt plaintext P = 24 using this method

n bada chahiye 1914 se

(iii) encryption
ciphertext = $C = P^e \bmod n$
plaintext = "TO" = 1914
$C = 1914^{13} \bmod 209$ = 131

now 1914 > 209
(Text) > n
and C < n
P < n

$19^{13} \bmod 209 = 171$
$14^{13} \bmod 209 = 192$

decryption
$171^{97} \bmod 209 = 19 = T$
$192^{97} \bmod 209 = 14 = O$

plaintext $P = C^d \bmod n$
$P = 154^{97} \bmod 209$
$= 833$?

ans nahi nikal raha 833 hi aa raha

~~Ans 6~~

i) Key generation ∴ p and q in the form 4K+3 and p ≠ q
p = 23, q = 7
$n = 23 \times 7$
(public key) $n = 161$ private key = (23, 7) ← (p, q)
publicly announce

ii) Encryption $C = P^2 \bmod n$
$C = 24^2 \bmod 161$
ciphertext $C = 93$ → sent

iv) Decryption B receives 93 as ciphertext
$a_1 = +93^{(23+1)/4} \bmod 23 = 1 \bmod 23 = 1$
$a_2 = -93^{(23+1)/4} \bmod 23 = 22 \bmod 23 = 22$
$b_1 = +93^{(7+1)/4} \bmod 7 = 4 \bmod 7 = 4$
$b_2 = (-93)^{(7+1)/4} \bmod 7 = 3 \bmod 7 = 3$

⇒ $p1 = (a_1, b_1) = 116$ $p3 = (a_2, b_1) = 137$
$p2 = (a_1, b_2) = 24$ $p4 = (a_2, b_2) = 45$

(according to chinese remainder theorem) search it

Q7 In ElGamal, given the prime $p = 31$:
a) Chose an appropriate e1 and d, then calculate e2.
b) Encrypt the message "HELLO", use 00 to 25 for encoding.
c) Decrypt the cipher text to obtain plaintext.

Q. 7

1) Key generation select large prime $p = 31$ (given)

e_1 = given primitive root of 31 such that $e_1^i \bmod 31 = \{1 \text{ to } 30\}$

we have 8 primitive roots of 31

e_1: 3, 11, 12, 13, 17, 21, 22 and 24

$\Rightarrow e_1 = 3$

$d = 10, 0 < d < p-2$

$\Rightarrow$

$e_2 = 3^{10} \bmod 31 = 25$

public key $(e_1, e_2, p) = 3, 25, 31$

private key $(d) = 10$

2) encryption :- select random r in group $G = \langle Z_{31}^*, \times \rangle$

let $r = 7$

$\Rightarrow C_1 = e_1^r \bmod p = 3^7 \bmod 31 = 17$

$C_2 = (P \times e_2^r) \bmod p$ for C_2 $e^7 \bmod 21 = 25^7 \bmod 31 = 25$

	Plaintext	$C(C_1, C_2)$		
H	7	17, 20	← for P = H	$C_2 = (7 \times 25^7) \bmod 31 = 20$ $7 \times 25 \bmod 31 = 20$
E	4	17, 7	← P = E	$C_2 = (4 \times 25^7) \bmod 31 = 7 = 4 \times 25 \bmod 31 = 7$
L	11	17, 27	← P = L	$C_2 = (11 \times 25^7) \bmod 31 = (11 \times 25 \bmod 31) = 27$
L	11	17, 27	← P = L	$C_2 = (11 \times 25^7) \bmod 31 = (11 \times 25 \bmod 31) = 27$
O	14	17, 9	← P = O	$C_2 = (14 \times 25^7) \bmod 31 = (14 \times 25 \bmod 31) = 9$

~~$(17^{10})^{-1} \bmod 31 = 25$~~

decryption :-

$P = [C_2 (C_1^{d})^{-1}] \bmod p$

C	P	text
17, 20	$20 \times (17^{10})^{-1} \bmod 31 = 7$	H
17, 7	$7 \times (17^{10})^{-1} \bmod 31 = 4$	E
17, 27	$27 \times (17^{10})^{-1} \bmod 31 = 11$	L
17, 27	$27 \times (17^{10})^{-1} \bmod 31 = 11$	L
17, 9	$9 \times (17^{10})^{-1} \bmod 31 = 14$	O

Date
DELTA Pg No.

Q8 Assume that Alice uses Bob's ElGamal public key ($e1 = 2$) to send two messages $P1 = 17$ and $P2 = 37$ using same random integer $r = 9$. Eve Intercepts the cipher text and somehow finds the value of $P1 = 17$. Show how Eve can use a known plain text attack to find the value of P2. Assume the value of modulus $p = 53$ and $d = 3$

Sol^n

Known-Plaintext Attack :- if Alice uses same random exponent r, to encrypt 2 plain texts P and P', Eve discovers P' if she knows P.

Assume, that $C_2 = P \times e_2^r \bmod p$ and $C_2' = p' \times e_2^r \bmod p$.

Eve finds P' using following steps:

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

Alice should use new r value to thwart the known-plaintext attack

$\Rightarrow$ $P_1 = 17$, $P_2 = 37$, $r = 9$, $e1 = 2$, $p = 53$

even knows $P_1 = 17$

$\Rightarrow$ $C_2 = P_1 \times 2^9 \bmod 53$ and $C_2' = P_2 \times 2^9 \bmod 53$

$C_2 = 17 \times 2^9 \bmod 53 = 12$ $\qquad$ $= 37 \times 2^9 \bmod 53 = 23$

eve intercepts

$\Rightarrow C_2 = 23$

$C_2' = 23$

Step 1 :- $e_2^9 = C_2 \times P_1^{-1} \bmod p$

$= 12 \times 17^{-1} \bmod 53$

$= 12 \times 25 \bmod 53$

$= 35$

Step 2 $P_2 = C_2' \times (35)^{-1} \bmod 53$

$= 23 \times (35)^{-1} \bmod 53$

$P_2 = 23 \times 50 \bmod 53$

$\boxed{P_2 = 37}$ ← Now eve knows what P_2 was.