Assignment
On
Cryptography
&
Security

Scholar Id :- 16-1-5-011

Branch :- Computer Science & Engineering

Semester :- 8th Sem

Nit
Silchar

Q.

Let $p = 23, q = 31$, Bob chose $e = 83$. Compute d? if Alice wants to sent the text "NITS", the ASCII code is (78, 73, 84, 83). Find the cipher text for each ~~ASCII~~ ASCII code. Convert back the the cipher text to plain text using the private key 'd'

Soln

Step – 1

Key generation.

(i) $p = 23$ & $q = 31$

(ii) $n = p \times q = 23 \times 31 = 713$

(iii) $\phi(n) = (p-1)(q-1) = (23-1) \times (31-1) = 22 \times 30 = 660$

(iv) Given $e = 83$

$\gcd(\phi(n), e) = 1$

$\gcd(660, 83) = 1$

q	r_1	r_2	r	T_1	T_2	$T_1 - qT_2$
7	660	83	79	0	1	-7
1	83	79	4	1	-7	8
19	79	4	3	-7	8	-159
1	4	3	1	8	-159	167
3	3	1	0	-159	167	-645
	1	0		167	-645	

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

$= 83^{-1} \bmod 660$

$= \frac{1}{83} \bmod 660$

$= 167 \times 1 \bmod 660$

$= 167 \bmod 660$

$= 167$

$e = 83, \quad d = 167$

(vi) Public key

$KU = \{e, n\}$

$= \{83, 713\}$

(vii) Private key

$KR = \{d, n\}$

$= \{167, 713\}$

For

Step - 2

Encryption

Alice wants to sent the text "NITS"

The ASCII code is (78, 73, 84, 83).

For

plain text $M = 78 < n$

$\therefore$ Cipher text $C = M^e \pmod n$

$= 78^{83} \bmod 713$

$78 \to 78 \bmod 713$

$78^2 \to 6084 \bmod 713$

$\to 380$

$(78)^4 \to (380)^2 \bmod 713$

$\to 374$

$(78)^{16} = (374)^2 \bmod 713$

$= 128$

$(78)^{32} \to (128)^2 \bmod 713$

$= 698$

$(78)^{64} \to (698)^2 \bmod 713$

$\to 225$

$83 \to 1010011$

$78^{83} \to 78^{64+16+2+1}$

$\to (225)(128)(380)(78) \bmod 713$

$\Rightarrow 78^{83} \bmod 713$

$= 624$

Plain text $M = 73 < n$

$\therefore$ Cipher text $C = M^e \pmod n$

$= 73^{83} \bmod 713$

$73 \rightarrow 73 \bmod 713$

$73^2 \rightarrow 5329 \bmod 713$

$\rightarrow 338$

$(73)^4 \rightarrow (338)^2 \bmod 713$

$\rightarrow 164$

$(73)^8 \rightarrow (164)^2 \bmod 713$

$\rightarrow 515$

$(73)^{16} \rightarrow (515)^2 \bmod 713$

$\rightarrow 702$

$(73)^{32} \rightarrow (702)^2 \bmod 713$

$\rightarrow 121$

$(73)^{64} \rightarrow (121)^2 \bmod 713$

$\rightarrow 381$

$83 \rightarrow 64+16+2+1$

$73^{83} \rightarrow 73^{64+16+2+1}$

$\rightarrow (381)(702)(338)(73) \bmod 713$

$\rightarrow 508$

$\Rightarrow 73^{83} \bmod 713$

$= 508$

Plain text $M = 84 < n$

$\therefore$ Cipher text $c = M^e \pmod n$

$= 84^{83} \pmod{713}$

$84 \rightarrow 84 \bmod 713$

$84^2 \rightarrow 7056 \bmod 713$

$\rightarrow 639$

$(84)^4 \rightarrow (639)^2 \bmod 713$

$\rightarrow 485$

$(84)^{16} \rightarrow (485)^2 \bmod 713$

$\rightarrow 648$

$(84)^{32} = (648)^2 \bmod 713$

$= 660$

$(84)^{64} = (660)^2 \bmod 713$

$= 670$

$83 \rightarrow 64+16+2+1$

$84^{83} \rightarrow 84^{64+16+2+1}$

$= (670)(648)(639)(84) \bmod 713$

$= 84^{83} \pmod{713}$

$= 654$

Plain text $M = 83 < n$

$\therefore$ Ciphertext $C = M^e \pmod n$

$= 83^{83} \bmod 713$

$= 296$

Plain text = (78 , 73 , 84 , 83)

Cipher text = (624 , 508 , 654 , 296)

For Decryption

Convert back the cipher text to plain text using the private key 'd'

(i) Ciphertext $c = 624$

$\therefore$ Plain Text $M = c^d \pmod n$

$= 624^{167} \pmod{713}$

$= 78$

(ii) Cipher text $c = 508$

$\therefore$ plain text $M = c^d \pmod n$

$= 508^{167} \pmod{713}$

$= 73$

(iii) cipher text $c = 654$

$\therefore$ plain text $M = c^d \pmod n$

$= 654^{167} \mod 713$

$= 84$

(iv) cipher text $c = 296$

$\therefore$ plain text $M = c^d \pmod{n}$

$= 296^{167} \bmod 713$

$= 83$

$\therefore$ cipher text $\rightarrow$ (624, 508, 654, 296)

$\Downarrow$

$\therefore$ plain text $\rightarrow$ (78, 73, 84, 83)