CHRIST
(DEEMED TO BE UNIVERSITY)
BANGALORE · INDIA

CIA-3

PROBLEM SOLVING

BCA331

SUBMITTED BY:

Rushaan Anwar

3BCA 'B'

2241151

SUBMITTED TO:

DEPARTMENT OF MATHEMATICS

Question 1

Suppose Alice RSA Cryptosystem with key $(n=2537, e=13)$, note that 2537 is equal to $43 * 59$. Alice wants to send the message " MEET AT NOON " to her friends. What should she send? Also help Alice's friends to decrypt the received messages that they received from Alice.

Solution :

key $(n,e) = 2537, 13$

$\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$

MEET AT NOON

Translating the letters into numerical equivalent,

12040419 0019 13141413

Grouping them into fours,

1204 0419 0019 1314 1413

Encrypting each block with,

$C = M^e \bmod n$

$\underline{1204}$

1204^{13} mod 2537

$13 = (1101)_2$, $x = 1$

$i = 0$, $a_0 = 1$, $x = 1 \cdot 1204$, power $= 1204^2$ mod $2537 = 989$

$i = 1$, $a_1 = 0$, $x = 1204$, power $= 989^2$ mod $2537 = 1376$

$i = 2$, $a_2 = 1$, $x = 1204 \cdot 1376$ mod $2537 = 43$, power $= 1376^2$ mod 2537
$= 774$

$i = 3$, $a_3 = 1$, $x = 43 \cdot 774$ mod $2537 = \underline{\underline{301}}$

Similarly applying for 0419, 0019, 1314 and 1413 we get,

1204	—	301
0419	—	2017
1314	-	2431
1413	-	1155

The Encrypted message is :

301 2017 2431 1151

To decrypt the message that Alice sent,

$\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$

$\gcd(13, 2436) = 1$

$13x = 1 \mod 2436$

Finding Inverse of 13 mod 2436,

$13(937) \equiv 1 \mod 2436$

Since inverse of 13 mod 2436 = 937, $\underline{d = 937}$

Using $d = 937$ as our decryption exponent,

$M = C^{937} \mod 2537$

$\underline{301}$

$(0301)^{937} \mod 2537 = 1204 \quad [1204]$

$\underline{2017}$

$(2017)^{937} \mod 2537 = 419 \quad [0419]$

$\underline{2431}$

$(2431)^{937} \mod 2537 = 1314 \quad [1314]$

$\underline{1155}$

$(1155)^{937} \mod 2537 = 1413 \quad [1413]$

Hence, the decrypted message is:

1204 0419 1314 1413

⇒ "MEET AT NOON"

Question 2

Suppose Alice and Bob RSA cryptosystem with keys $(n_{Alice}, e_{Alice}) = (2867, 7) = (61 \cdot 47, 7)$ and $(n_{Bob}, e_{Bob}) = (3127, 21) = (59 \cdot 53, 21)$.

(i) Alice wants to send all her friends including Bob "SELL EVERYTHING" so that he knows she sent it. What should she sent her friends?

(ii) Alice wants to send Bob the message "BUY NOW" so that he knows that she sent it and so that so that only Bob can read it. What should she send Bob, assuming she signs the message and then encrypts it using Bob's public key?

Solution

$$(n_{Alice}, e_{Alice}) = (2867, 7) = (61 \cdot 47, 7)$$

$$d_{Alice} = 1183$$

$$(n_{Bob}, e_{Bob}) = (3127, 21) = (59 \cdot 53, 21)$$

$$d_{Bob} = 1149$$

Message = "SELL EVERYTHING"

18041111 04210417241907081306

Grouping into blocks of 4,

1804 1111 0421 0417 2419 0708 1306

Alice using her decryption to send and decrypt each block,

$$D_{(2867,7)} = D_{(n,e)} = x^{d} \bmod n = x^{1183} \bmod 2867$$

$1804^{1183} \bmod 2867 = 2186$

$1111^{1183} \bmod 2867 = 2087$

$0421^{1183} \bmod 2867 = 1279$

$0417^{1183} \bmod 2867 = 1251$

$2419^{1183} \bmod 2867 = 0326$

$0708^{1183} \bmod 2867 = 0816$

$1306^{1183} \bmod 2867 = 1948$

The message that Alice sends would be,

2186 2087 1279 1251 0326 0816 1948

Message = "BUY NOW"

Converting into blocks of 4,

012024 131422

↓

0120 2413 1422

Encrypting,

$E_{(3127,21)} = D_{(n,e)} = x^e \bmod n = x^{21} \bmod 3127$

$0120^{21} \bmod 3127 = 2711$

$2413^{21} \bmod 3127 = 2080$

$1422^{21} \bmod 3127 = 0280$

The message Alice sends so that Bob can read it is,

2711 2080 0280