NAMA : Montana Guming
NIM : 11519017

9.2 perform encryption and decryption using the RSA algorithm, as in figure 9.5, for the followings :

a) $p = 3$; $q = 11$, $e = 7$; $M = 5$

① select primes : $p = 3$ & $q = 11$
② lakukan komputasi : $N = p.q = 3.11 = 33$
③ lakukan komputasi : $\phi(n) = (p-1)(q-1) = (3-1)(11-1) = 2.10 = 20$
④ select e ; gcd $(e, 20) = 1$; choose $e = 7$
⑤ Tentukan d ; $d.e = 1 \bmod 20$ dan $d < 20$,
maka $d = 3$, karena : $3 \times 7 = 21 = 2 \times 10 + 1$
⑥ publish public key $KU = \{7, 33\}$
⑦ keep secret private key $KR = \{3, 3, 11\}$

Proses enkripsi dan deskripsi :
① Message $M = 5$ $(5 < 33)$
② Encryption
$C = 5^7 \bmod 33 = 78125 \bmod 33 = 14$
③ Descryption
$M = 14^3 \bmod 33 = 2744 \bmod 33 = 5$ (terbukti)

b) $p = 5$; $q = 11$; $e = 3$; $M = 9$

① select primes : $p = 5$ & $q = 11$
② lakukan komputasi : $N = p.q = 5 \times 11 = 55$
③ lakukan komputasi : $\phi(n) = (p-1)(q-1) = (5-1)(11-1) = 4.10 = 40$
④ select e ; gcd $(e, 40) = 1$; choose $e = 3$
⑤ Tentukan d ; $d.e = 1 \bmod 40$ dan $d < 40$,
maka $d = 27$, karena $3 \times 27 = 81 = 2 \times 40 + 1$
⑥ publish public key $KU = \{3, 55\}$
⑦ keep secret private key $KR = \{13, 5, 11\}$

$d = ((\phi(n) * i) + 1) / e$
(i=1) $d = [40 \cdot 1) + 1 / 3 = 41/3$
$= 13,67 \rightarrow$ bukan integer
(i=2) $d = (40.2) + 1/3 = 81/3$
$= 27 \rightarrow$ integer

Proses enkripsi dan dekripsi :
① Message $M = 9$ $(9 < 55)$
② Encryption
$C = M^E \bmod N = 9^3 \bmod 55 = 729 \bmod 55 = 14$
③ Decryption
$M = C^d \bmod N = 14^{27} \bmod 55 = 9$ (terbukti)

Nama: Montana Guming
Nim : 11519017

Date

9.3 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 the plainteks M?

Pembahasan:

Dik: C = 10
e = 5
N = 35

Dit: M .... ?

Jwb:

$$C = M^e \bmod N$$
$$10 = M^5 \bmod 35$$

- select primes : p = 5 & q = 7
- lakukan komputasi : $N = p.q = 5.7 = 35$
- lakukan komputasi : $\emptyset(n) = (p-1)(q-1) = (5-1)(7-1) = 4.6 = 24$
- select e ; gcd(e, 24) = 1 , choose e = 5
- Tentukan d ; $d.e = 1 \bmod 24$ dan $d < 24$

$d = ((\emptyset(n)).i + 1)/e$,

$[i=1] \rightarrow d = (24.1 + 1)/5 = 25/5 = 5$ (integer)

maka d = 5 → karena $5 \times 5 = 25 = 4 \times 6 + 1$

- publish public key KU = {5, 35}
- secret private key KR = {5, 5, 7}

do encryp & decryp :

- M = ?
- C = 10
- $M = C^d \bmod N$

$M = 10^5 \bmod 35$

$M = 100.000 \bmod 35$

M = 5 (maka plainteksnya adalah 5)

Pembuktian bahwa ciphertext C = 10 ⇓

- $C = M^e \bmod N$

$C = 5^5 \bmod 35$

$C = 3125 \bmod 35$

C = 10 (terbukti ciphertext / C = 10)

NAMA : MONTANA BURNING
NIM : 11S19017

Date

9.4. In RSA system, the public key of a given user is $e = 31$, $n = 3599$. What is the private key of this user? Hint: First use trial-and-error to determine p and q; then use the Extended Euclidean algorithm to find the multiplicative inverse of 31 modulo $\phi(n)$.

Pembahasan

⊙ $KU = \{e, N\}$

$KU = \{31, 3599\}$

⊙ $p = 59$ & $q = 61$

⊙ $\phi(n) = (p-1).(q-1)$

$= (59-1).(61-1)$

$= 58.60$

$= 3480$

⊙ $e.d = 1 \mod \phi(n)$

$31.d = 1 \mod 3480$

$$d = \frac{1 + k\phi(n)}{e}$$

$$d = \frac{1 + 3480k}{31}$$

$(k=0) \rightarrow d = \frac{1 + 3480(0)}{31} = \frac{1}{31}$

$(k=1) \rightarrow d = \frac{1 + 3480(1)}{31} = \frac{3481}{31}$

$(k=2) \rightarrow d = \frac{1 + 3480(2)}{31} = \frac{6961}{31}$

⋮

$(k=27) \rightarrow d = \frac{1 + 3480(27)}{31} = 3031 \left(\frac{93961}{31}\right)$

Jadi private key $KR = [d, p, q]$

$KR = [3031, 59, 61]$