Metoda direkte - Shifrimit RSA (Rivest–Shamir–Adleman)

$$c \equiv b^e \ mod \ m$$

Formula përdoret për të shifruar një mesazh (c) duke përdorur një çelës publik të një sistemi RSA. Ky çelës publik përbëhet nga dy pjesë, një eksponent publik (e) dhe një modulo (m)

Ku:

c është mesazhi i shifruar,

b është mesazhi i lexueshëm,

e është eksponenti publik,

m është moduli.

Detyra 1

Jane dhënë b=4, e=13 m=497 enkriptoni(shifroni) c

$c \equiv b^e \ mod \ m$

$c \equiv 4^{13} \ mod \ 497$

$c \equiv 67108864 \ mod \ 497$

$c = 445$

Detyra 2

A plaintext message **m** is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.

To find ciphertext from the plain text following formula is used to get ciphertext C.

$C = m^e \bmod n$

$C = 9^7 \bmod 77$

C = 37

Detyra 3:

A ciphertext message **c** is decrypted using private key <d, n>. To calculate plain text **m** from the ciphertext c following formula is used to get plain text m.

$m = c^d \bmod n$

$m = 37^{43} \bmod 77$

m = 9

In this example, Plain text = 9 and the ciphertext = 37

Detyrë:

Supozojmë se P = 41 dhe Q = 59.

n= p*q

n=41*59

n=2419

Supozojmë e = 3

Φ(n) = (p-1)(q-1)

Φ(n) = (41-1)(59-1)

Rezultati Φ(n)=2320

d = (k*Φ(n) + 1) / e për k = 2

d = (2*2320+1)/3

Rezultati d = 1547

Për Enkriptim

Supozoni se Mesazhi është "m". Atëherë teksti i shifruar-ciphertext është:

$c = m^e \ mod \ n$

$c = m^3 \ mod$ 2419.

Për deshifrim

Supozoni se mesazhi me tekst i kodit është "C". Atëherë plaintext është:

$m = C^d \ mod \ n$

$m = C^{1547} \ mod \ 2419$