Nama: Montana Gurning
Nim : 1113g017

8. in a pubric-key system using RSA, you intercept the Ciphertext C=10 sent to a user whose pubric key is e=5, n=35. what is the plaintext?

Pembahasan:

Dik: C = 10
e = 5
n = 35

Dit: M

Jwb: $M = C^d \bmod n$

① Select primes: p=5 & q=7
② Hitung N = p.q
= 5.7 = 35
③ Hitung $\phi(n)$: (p-1) (q-1)
= (5-1) (7-1)
= 4.6
= 24
④ Select e : gcd (e, 24) = 1 , choose = 5
⑤ Tentukan d ; d.e = 1 mod 24 dan d<24
maka d = 5 → karena 5x5 = 25 → 4.6 + 1
⑥ pubric key KU = {e, N}
= {5, 35}
⑦ Private key KR = {d, p, q}
= {5, 5, 7}

✱ M = $C^d \bmod N$
= $10^5 \bmod 35$
= 100.000 mod 35
= 5

Maka plaintext (M) = 5

✱ Pembuktí bahwa Ciphertext C=10
C = $M^e \bmod N$
= $5^5 \bmod 35$
= 3125 mod 35
= 10 (terbuktí Ciphertext =10) //