Assignment NO: 02

Computer Security

Name: ASHFAQ AHMAD

Reg NO: 19PWCSE1795

Section: A

Submitted to:

Dr. Sadeeq Jan Sab

DCSE, UET Peshawar

Q NO: 01

Solve the following using RSA cryptosystem.

a) $P = 13$, $q = 17$ Public key $= e = 35$

Private key $= d = ?$

Sol

* first we will find system modulus

$$N = P \times q = 13 \times 17$$

$$\boxed{N = 221}$$

* Now we will find toshen function.

$$\phi(N) = (P-1)(q-1)$$
$$= (13-1)(17-1)$$
$$= (12)(16)$$
$$\boxed{\phi(N) = 192}$$

Now for finding d, there are two pre-requisites

→ $e \cdot d \bmod \phi(N) = 1$

→ $0 \leq d \leq N$

formula for finding d is,

$$d = \frac{K \cdot \phi(N) + 1}{e}$$

we will put the value of $K = 0, 1, 2, 3 \ldots$ so we get the value of d as a whole number

so by putting $K = 2$

$$d = \frac{2 \times 192 + 1}{35}$$

$d = 11$

(b) $P = 13$, $q = 23$, Public key $e = 23$

Private key $= d = ?$

Sol

* first we will find system modulus.

$N = P \times q$

$N = (13)(23)$

$N = 299$

* Now to chen function,

$\phi(N) = (P-1)(q-1)$

$\phi(N) = (13-1)(23-1)$

$\phi(N) = (12)(22)$

$\phi(N) = 264$

Now to find d, Two Pre-requisites,

$e \cdot d \bmod \phi(N) = 1$

$0 \leq d \leq N$

Formula for finding d is,

$$d = \frac{K \cdot \phi(N) + 1}{e}$$

$K = 0, 1, 2, 3, \ldots$ for getting d as a whole number

for $K = 2$

$$d = \frac{2 \times 264 + 1}{23}$$

$d = 23$ Ans

c) Encrypt the following message using the Public Key in Part a and b.

18, 22, 9, 17

Sup = encryption is done using public key of reciver.

So Public key in Part a is,

$KU = \{e, N\}$

$KU = \{35, 221\}$

Public key in Part b is,

$KU = \{e, N\}$

$KU = \{23, 299\}$

* **M = 18** (Part a)

As

$C = M^e \bmod N$

$C = 18^{35} \bmod 221$

$C = 18^{34} \bmod 221 \cdot 18^{1} \bmod 221$

$C = 18^{32} \bmod 221 \cdot 18^{2} \bmod 221 \cdot 18^{1} \bmod 221$

$C = 18^{16} \bmod 221 \cdot 18^{16} \bmod 221 \cdot 18^{2} \bmod 221 \cdot 18^{1} \bmod 221$

~~C = 18~~

$C = 18^{8} \bmod 221 \cdot 18^{8} \bmod 221 \cdot 18^{8} \bmod 221 \cdot 18^{8} \bmod 221 \cdot 18^{2} \bmod 221 \cdot 18^{1} \bmod 221$

As $18^{8} \bmod 221 = 1$ So

$C = 1 \times 1 \times 1 \times 1 \times 18^{2} \bmod 221 \cdot 18^{1} \bmod 221$

$C = 103 \times 18 \bmod 221$

$C = 86$ Ans

M = 18 (For Part b)

$c = 18^{23} \bmod 299$

$c = 18^{22} \bmod 299 \cdot 18 \bmod 299$

$c = 18^{8} \bmod 299 \cdot 18^{8} \bmod 299 \cdot 18^{6} \bmod 299 \cdot 18 \bmod 299$

~~$c = (240)(240)(48)(18) \bmod 299$~~

~~$c = 49766400 \bmod 299$~~

$c = (131)(131)(77)(18) \bmod 299$

$c = 23785146 \bmod 299$

$\boxed{c = 294}$

* M = 22 (Part a)

$c = 22^{35} \bmod 221$

From previous encryption we get

$c = 22^{8} \bmod 221 \cdot 22^{8} \bmod 221 \cdot 22^{8} \bmod 221 \cdot 22^{8} \bmod 221 \cdot 22^{2} \bmod 221 \cdot 22 \bmod 221$

$c = (16)(16)(16)(16)(42)(22) \bmod 221$

$c = 60555264 \bmod 221$

$\boxed{c = 159}$

For Part (b)

$c = 22^{23} \bmod 299$

From previous,

$c = 22^{8} \bmod 299 \cdot 22^{8} \bmod 299 \cdot 22^{6} \bmod 299 \cdot 22 \bmod 299$

$c = (185)(185)(1)(22) \bmod 299$

$c = 752950 \bmod 299$

$\boxed{c = 68}$

* **M = 9:**

(for part a)

$c = 9^{35} \bmod 221$

From previous eq,

$c = 9^8 \bmod 221 \cdot 9^8 \bmod 221 \cdot 9^8 \bmod 221 \cdot 9^8 \bmod 221 \cdot 9^2 \bmod 221 \cdot 9 \bmod 221$

$c = (120)(120)(120)(120)(81)(9) \bmod 221$

$c = 151165440000 \bmod 221$

$\boxed{c = 185}$

(for part b)

$c = 9^{23} \bmod 299$ from previous eq,

$c = 9^8 \bmod 299 \cdot 9^8 \bmod 299 \cdot 9^6 \bmod 299 \cdot 9 \bmod 299$

$c = (289)(289)(118)(9) \bmod 299$

$c = 88699302 \bmod 299$

$\boxed{c = 55}$

P + T P O

* M = 17

Part (a)

$c = 17^{35} \bmod 221$ (from previous eq)

$c = 17^8 \bmod 221 \cdot 17^8 \bmod 221 \cdot 17^8 \bmod 221 \cdot 17^8 \bmod 221 \cdot 17^2 \bmod 221 \cdot 17 \bmod 221$

$c = (68)(68)(68)(68)(68)(17) \bmod 221$

$c = 24716870656 \bmod 221$

$\boxed{c = 153}$

Part (b)

$c = 17^{23} \bmod 299$

$c = 17^8 \bmod 299 \cdot 17^8 \bmod 299 \cdot 17^6 \bmod 299 \cdot 17 \bmod 299$

$c = (133)(133)(196)(17) \bmod 299$

$c = 58939748 \bmod 299$

$\boxed{c = 270}$

(d) Decrypt the following messages using the keys in Part a & b.

189, 73, 127, 77

Sol

For decryption we need Private key of reciever.

So Private key for part a.

$KR = \{d, N\}$

$KR = \{11, 221\}$

And Private key for part b.

$KR = \{d, N\}$

$KR = \{23, 299\}$

* ~~C = 18~~

$C = 189$

For part a

As $M = e^d \bmod N$

$M = 189^{11} \bmod 221$

$M = 189^5 \bmod 221 \cdot 189^5 \bmod 221 \cdot 189 \bmod 221$

$M = (219)(219)(189) \bmod 221$

$M = 9064629 \bmod 221$

$M = 93$

For Part (b)

$$M = 189^{23} \bmod 299$$

As we have factorized Power 23 in previous eq So we get

$$M = 189^{8} \bmod 299 \cdot 189^{8} \bmod 299 \cdot 189^{6} \bmod 299 \cdot 189 \bmod 299$$

$$M = (16)(16)(77)(189) \bmod 299$$

$$M = 3725568 \bmod 299$$

$$\boxed{M = 28}$$ Ans

* $C = 73$

Sol Part (a)

$$M = 73^{11} \bmod 221$$

$$M = 73^{5} \bmod 221 \cdot 73^{5} \bmod 221 \cdot 73 \bmod 221$$

$$M = (99)(99)(73) \bmod 221$$

$$M = 715473 \bmod 221$$

$$\boxed{M = 96}$$

Part (b)

$$M = 73^{23} \bmod 299$$

$$M = 73^{8} \bmod 299 \cdot 73^{8} \bmod 299 \cdot 73^{6} \bmod 299 \cdot 73 \bmod 299$$

$$M = (170)(170)(25)(73) \bmod 299$$

$$M = 52742500 \bmod 299$$

$$\boxed{M = 96}$$ Ans

* C = 127

for part (a)

$M = 127^{11} \bmod 221$

$M = 127^{5} \bmod 221 \cdot 127^{5} \bmod 221 \cdot 127 \bmod 221$

$M = (43)(43)(127) \bmod 221$

$M = 234823 \bmod 221$

$\boxed{M = 121}$

for part (b)

$M = 127^{23} \bmod 299$

$M = 127^{8} \bmod 299 \cdot 127^{8} \bmod 299 \cdot 127^{6} \bmod 299.$

$127 \bmod 299$

~~$M = (225)(225)(127) \bmod 299$~~

~~$M = 6429375 \bmod 299$~~

~~$\boxed{M = 277}$~~

$M = (100)(100)(70)(127) \bmod 299$

$M = 215900000 \bmod 299$

$\boxed{M = 173}$

P + T + O

* $C = 77$

for part (a)

$M = 77^{11} \bmod 221$

$M = 77^5 \bmod 221 \cdot 77^5 \bmod 221 \cdot 77 \bmod 221$

$M = (25)(25)(77) \bmod 221$

$M = 48125 \bmod 221$

$\boxed{M = 168}$

for part (b)

$M = 77^{23} \bmod 299$

$M = 77^8 \bmod 299 \cdot 77^8 \bmod 299 \cdot 77^6 \bmod 299 \cdot 77 \bmod 299$

$M = (27)(27)(105)(77) \bmod 299$

$M = 5893965 \bmod 299$

$\boxed{M = 77}$

END OF Assignment NO: 02