

**RSA Class Activity**

**APT3090 CRYPTOGRAPHY AND NETWORK SECURITY**

1. Provide the notation for generating RSA key pair, Encryption and Decryption

**Prime numbers(distinct): p, q**

**Modulus n= p \*q**

**Euler's Totient Function ϕ(n)=(p−1)×(q−1)**

**Integer e: 1<e<ϕ(n) and gcd(e, ϕ(n))=1**

**Integer d: (d\*e-1)/ ϕ(n)= integer**

**Public key: (e,n)**

**Private key:(d, n)**

**Encryption: Message M, Ciphertext C= Me mod n**

**Decryption: M= Cd mod n**

1. **Decoding in RSA**

Decode the three ciphertext symbols 5, 9 and 3 using the private RSA key (7, 11). What are the corresponding plaintext symbols?

**Private key :(d, n) =(7, 11)**

**Decryption: M= Cd mod n**

**57 mod 11 = 3**

**97 mod 11 =4**

**37 mod 11 =9**

1. **Matching RSA Keys**

Which of the following private RSA keys matches the public RSA key (5, 91)?

- (19, 91) x

- (24, 91) x

- (29, 91)

- (19, 81) x

- (24, 81) x

- (29, 81) x

**Public key: (e,n)= (5,91)**

**Private key: (d, n)**

**91= 7 \*13**

**Φ(n) =6\*12=72**

**e=5**

**Integer d: (d\*e-1)/ϕ(n)= integer**

**- (29, 91)**

1. **Generate Your Own RSA Key Pair**

Use the procedure as described in the lecture to generate a RSA key pair, using primes in the range from 20 to 100. Test the correctness of your key pair by encoding and decoding a number. If your key pair is correct, after decoding an encoded number, you should arrive at the number you started from.

**P=29, q= 53**

**n= 29\*53=1537**

**ϕ(n) = 28\*52= 1456**

**e= 3**

**d\*e -1/ ϕ(n) =integer**

**d= 971**

**public key (3,1537) , private key (971,1537)**

**message, M = 5**

**Encryption : 53 mod 1537 =125**

**Decryption : 125971 mod 1537 = 5**