**ITCS 461 Computer & Communication Security Date : ­­\_\_\_\_\_\_\_\_\_**

**ID : Name : Section :** \_\_\_\_\_\_\_

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Save your answer sheet as “**Student\_ID\_Firstname\_Lab02.pdf**”.

Submit to the lab folder in MyCourses website according to your section.

**Lab 2 : Public-Key Cryptography**

Follow Lab 2 explanation (Lab2\_Explain.pdf) and answer these questions:

**Part I : RSA Key Generation**

**Question 1:** What are the values of “N” and “d” ?

value of “N” =

value of “d” =

calculate ϕ(N) = (P - 1) × (Q - 1) =

Verify that N = P × Q ? (Y/N)

Verify that e × d ≡ 1 mod ϕ(N) ? (Y/N)

If No, why ?

**Question 2**: (e = **13**)

What is the value of private key “d” ?

Verify e × d ≡ 1 mod ϕ(N) ? (Y/N)

If No, why ?

**Question 3**: (e = **5**)

What is the value of private key “d” ?

Verify e × d ≡ 1 mod ϕ(N) ? (Y/N)

If No, why ?

**Part II: RSA Encryption/Decryption**

**Question 4:**

What is the ciphertext (C) ?

What is the encryption key (e) ?

Is it correct ? (Y/N) *(check manually by using a calculator)*

**Question 5:** (input = **2**)

What is the ciphertext (C) ?

Is it correct ? (Y/N) *(check manually by using a calculator)*

**Question 6:** (input = **79**)

What is the ciphertext (C) ?

Is it the same as output in question 5 ? (Y/N)

**Question 7:**

What is the message output (M) ?

Verify that the decrypted value is identical to the input message of **Question 4**. (Y/N)

*(check for* P, C, e *and* d*. If you cannot get “yes”, try again.)*

**Question 8:**

What is the message output (M) ?

Verify that the decrypted value is identical to the input message of **Question 5**. (Y/N)

*(check for* P, C, e *and* d*. If you cannot get “yes”, try again.)*

**Question 9:**

What is the message output (M) ?

Verify that the decrypted value is identical to the input message of **Question 6**. (Y/N)

If no, what do you think the reason is ?

**Question 10:** What is the maximum value of plaintext that will get a successful decryption ?

**Part III: Attack to Break RSA**

**Question 11:** Is “**334780716989568987860441698482126908177047949837137685689124313889828 83793878002287614711652531743087737814467999489**”

a prime number ? (Y/N)

**Question 12:** Use this workspace to find two prime numbers (i.e. P and Q) in the range

of **900 - 1000** and calculate N and ϕ(N)

P =

Q =

Calculate N = P × Q =

Calculate ϕ(N) = (P - 1) × (Q - 1) =

**Question 13:** Factorize N = **3992003**

P =

Q =

*(check your answer by using a calculator)*

**Question 14:** Factorize N = **98448473560141**

P =

Q =

*(check your answer by using a calculator)*

**Question 15:** Attack to RSA by trying to derive private key (d). Suppose, public-key (e)

of Alice is 6007 and global modulus number (N) is **43562419**. Find the corresponding

private-key(d) of Alice.

N = P × Q

P =

Q =

ϕ(N) = (P- 1) x (Q -1) =

e =

d = e -1 mod ϕ(N) =

*(check your answer by using a calculator, verify that e × d = 1 mod ϕ(N) ? If not,*

*try again.)*