ITCS 461 Computer & Communication Security Date : 30/01/2023

ID : **6388014** **Name** : **Waris Damkham** **Section** : 2

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" = 77

value of "d" = 53

calculate $\phi(N) = (P - 1) \times (Q - 1)$ = 60

Verify that $N = P \times Q$? Y (Y/N)

Verify that $e \times d \equiv 1 \bmod \phi(N)$? N (Y/N)

If No, why ? 901 is no equal 1

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

What is the value of private key "d" ? 37

Verify $e \times d \equiv 1 \bmod \phi(N)$? N (Y/N)

If No, why ? 481 is not equal 1

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

What is the value of private key "d" ? Error

Verify $e \times d \equiv 1 \bmod \phi(N)$? N (Y/N)

If No, why ? Error to generator

Part II: RSA Encryption/Decryption

Question 4:
What is the ciphertext (C) ? 52
What is the encryption key (e) ? 17
Is it correct ? Y (Y/N) *(check manually by using a calculator)*

Question 5: (input = **2**)
What is the ciphertext (C) ? 18
Is it correct ? Y (Y/N) *(check manually by using a calculator)*

Question 6: (input = **79**)
What is the ciphertext (C) ? 18
Is it the same as output in question 5 ? Y (Y/N)

Question 7:
What is the message output (M) ? 61
Verify that the decrypted value is identical to the input message of **Question 4**. Y (Y/N)
(check for P, C, e *and* d. *If you cannot get "yes", try again.)*

Question 8:
What is the message output (M) ? 2
Verify that the decrypted value is identical to the input message of **Question 5**. Y (Y/N)
(check for P, C, e *and* d. *If you cannot get "yes", try again.)*

Question 9:
What is the message output (M) ? 2
Verify that the decrypted value is identical to the input message of **Question 6**. N (Y/N)
If no, what do you think the reason is ? The max of length N

Question 10: What is the maximum value of plaintext that will get a successful decryption ? 76

Part III: Attack to Break RSA

Question 11: Is "**33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489**"
a prime number ? Y (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 = 907

Q = 911

Calculate N = P × Q = 826277

Calculate ϕ(N) = (P - 1) × (Q - 1) = 824460

Question 13: Factorize N = **3992003**

P = 1997

Q = 1999

(check your answer by using a calculator)

Question 14: Factorize N = **98448473560141**

P = 8827823

Q = 11152067

(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 = 5501

Q = 7919

ϕ(N) = (P- 1) x (Q -1) = 43549000

e = 6007

d = e^{-1} mod ϕ(N) = 33769143

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