ITCS 461 Computer & Communication Security Date : 29/1/2021

ID : _6288102_ Name : ____Krissanapong Palakham____________________ Section : __1___

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 ϕ(N) = (P - 1) × (Q - 1) = ____60___________

Verify that N = P × Q ? ____________Y___________ (Y/N)

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

If No, why ? ____

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

What is the value of private key "d" ? _____37_____

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

If No, why ? ____

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

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

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

If No, why ? _______No, because e = 5 can't generate a key.____________________________________

____

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 ? _____Because of it's max length if 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 “**3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799948 9**”
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.)