ID: 640315 **Name:** สิทธิกร เฉลิมกิตติชัย **Section :** 01

- Save this answer sheet as " **Lab2-YourID.pdf**" (Removing all figures will help reduce the file size).
- Submit this file to the lab folder in e-learning website according to your session.

Lab 8 : Public-Key Cryptography and Message Digest

Part I: RSA Key Generation

Question 1: What are the values of "N" and "d"?

value of "N" = 77

value of "d" = 53

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

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

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

If No, why? _____

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

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

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

If No, why? _____

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

What is the value of private key "d"? none (จำนวนเต็ม)

Verify $e \times d \equiv 1 \bmod \phi(N)$? none (Y/N)

If No, why? _____

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) *(by using calculator)*

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

What is the ciphertext (C)?____18____

Is it correct ?____Y____(Y/N) *(by using 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: congruent modulo n

Question 10: What is the maximum value of plaintext that will get a successful decryption? 77

Part III: Breaking RSA

Question 11: Is "**334780716989568987860441698482126908177047949837137685689124313889828837938780022876147116525317430877378144679994 89**"

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

$\phi(N) = (P - 1) \times (Q - 1) =$ 43562419

e = 6007

$d = e^{-1} \bmod \phi(N) =$ 6007 - 1 = 6006

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

Part IV: Hashing

Question 16:

Algorithm	Hash Value (Message Digest)	Length (bytes)
CRC16	53 C0	2
CRC32	C5 DA B1 BB	4
MD5	B2 E3 76 C7 1E 1C 1F B8 D9 0F 05 AD 0E 8A 6A 78	16
SHA-1	A5 99 E3 02 24 11 5C 69 A5 E6 97 CD 03 D4 54 B7 82 7A BA BD	20
SHA-256	E6 D3 0F 5F 60 7A 3D 00 79 B7 62 39 BB 44 08 38 D2 5E C3 3E 4C B6 9A 9E 27 5C D9 25 D7 9C E8 64	32
SHA-384	5A 95 8F 05 72 F3 81 82 33 54 7B 35 3D 19 85 6F B0 C3 45 C6 DF 1A 69 05 4B 17 21 35 10 A0 20 9D E5 85 E9 C7 ED F6 C8 E0 E8 25 64 09 18 F3 EC F0	48

SHA-512	02 B1 2D 15 B3 33 95 B8 70 AF E5 5D DF 26 BE EC BB E9 77 F3 A6 3A 7B 43 81 22 52 40 BC 9C 99 20 32 79 08 3A 36 4B 44 EF CD C5 55 AA 22 F5 AC E5 77 83 FD 33 F7 15 C3 5A CF F1 22 80 F1 9A 4D AF	64
Keccak	7B 82 FB BB 7C F4 46 9B EB A6 E5 63 55 FC 73 D7 69 48 F3 E7 CA D3 12 D4 A5 6E 02 8B 11 87 8D 5C	32

Part V: HMAC

Question 17:

Password	Hash Function	HMAC value
blank	MD5	CC 1E 54 20 58 A9 BB 5A 2D 09 67 D3 A1 12 D8 F6
blank	SHA1	B9 A9 80 C7 FF D9 03 AA C9 26 8E 0E 01 A4 8A A8 D3 59 D3 32
“secret”	MD5	DD CC 19 C6 CD 51 A3 8B 06 6B F0 14 53 88 39 88
“secret”	SHA1	9F 9D 98 67 1B E2 3A 0A BE 3C CC B4 12 12 21 A4 1C A8 A6 CA

- When using the blank password and using the same hashing function (MD5, SHA1) as in Question 1, does the HMAC produce the same value as hashing in **Question 16**? N (Y/N)
- Comparing between using blank password and password= “secret”, are these output values equal or differ? difference

Part VI: Viewing Website Certificate

Question 18:

- What is the URL of the website you chose? https://www.google.co.th/?hl=th
- What is the name of protocol? https://
- What is the name of key exchange algorithm? SHA-256 , SHA-1
- What is the name of encryption cipher algorithm? RSA

Question 19: What are the values of “IssuedTo” and “IssuedBy” on your website? (answer all CN, O, OU)

- CN = *.google.co.th
- O = <ไม่ใช่ส่วนหนึ่งของใบรับรอง>
- OU = <ไม่ใช่ส่วนหนึ่งของใบรับรอง>

Question 20: For each certificate in the "Certificate Hierarchy" box, from the bottom-up, fill in this table.

Certificate Name	Subject (only CN)	Issuer (only CN)
*.google.co.th	*.google.co.th	Google Internet Authority G3
*.google.co.th	*.google.co.th	Google Trust Services LLC

Part VII: Viewing a local certificate on Windows

Question 21:

- How many matched certificates that you have found? 2 (there must be at least 1)
- List the name of the found certificates and the name of the tab you found them in.

Found certificates

Certificate Name (Subject/CN)	Found in tab
2d2844a8-2552-4cbc-a097-8e761640599a	Details

Question 22: Examine one of the found certificates from Question 21.

Attribute	Value
Subject (only CN)	2d2844a8-2552-4cbc-a097-8e761640599a
Issuer (only CN)	MS-Organizaion-Acess
Signature Algorithm	sha256RSA
Signature Hash Algorithm	sha256
Public Key (only algorithm name and bits)	RSA 2048 bit