**ITCS 461 Computer & Communication Security Date : ­­­\_\_\_\_7/02/23\_\_\_\_\_**

**ID: 6388016 Name: Thanawath Huayhongthong** **Section:** 1

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

Save this answer sheet as “ **Lab3-6188xxx.docx**” or “ **Lab3-6188xxx.pdf**”.. Submit this file to the lab folder in MyCourses website according to your section.

**Lab 3 : Message Digest, Hash & Certificates**

Follow Lab 3 direction (Lab3\_Explain.pdf) and answer these questions:

**Part I: Hashing**

**Question 1:** Find hash values for given algorithms and their lengths (bytes).

|  |  |  |
| --- | --- | --- |
| **Algorithm** | **Hash Value (Message Digest)** | **Length (bytes)** |
| SHA-1 | 21 71 52 D9 E2 49 32 3C 43 C6 F3 20 F9 28 1B 72 1F 2E D3 C1 | 20 |
| SHA-256 | EE 84 66 7D C7 F7 5D B7 60 B1 2C B2 4B BD 46 1E 7F 45 69 E6 42 E7 79 C0 11 F5 35 EF F4 94 2F A8 | 32 |
| SHA-384 | E4 10 43 61 C7 01 02 DF 18 F7 A2 0F F4 39 BA 78 CE 7D 76 CF 36 B2 D3 EA F4 D0 69 88 06 FF EB 74 05 AF 87 4A 8C 45 CE 95 54 96 CF 43 82 E7 E3 3C | 48 |
| SHA-512 | F6 50 3E 14 C3 23 A5 CB AA 69 90 BD 84 E0 95 21 17 8D CF 0A 2D 66 55 4C 0F 63 68 93 BE 84 9B D9 FC 6D 48 2B 4A 36 6B 87 B5 75 17 81 11 10 CE 91 D2 87 05 90 5F 61 66 1C FE F2 E3 85 2A 5D 7C 24 | 64 |
| MD5 | 75 21 2F 3E C0 F8 6E 61 98 84 ED 13 66 09 C2 BA | 16 |
| SHA-3 (Keccak) | AC CD 44 FE B1 0D 83 50 23 ED 2D 0D 82 20 9C FC C0 14 41 73 E8 87 3C 18 D7 6A 09 A9 55 C2 5D 9E | 32 |

**Part II: HMAC**

**Question 2:** Find HMAC values for given hash messages and functions.

|  |  |  |
| --- | --- | --- |
| **Password** | **Hash Function** | **HMAC value** |
| Blank | MD5 | A5 B9 22 FF 7C FE 9E B9 77 5E 4F 15 C1 1D 14 CE |
| Blank | SHA-1 | BE 05 92 D7 95 41 B3 39 87 D2 44 57 38 31 D3 2D AE 90 93 E5 |
| “secret” | MD5 | BE 84 0B C1 72 25 F4 0C 06 F8 B5 27 73 3B 23 79 |
| “secret” | SHA-1 | 27 1A B9 2A 1D 50 7C 3E 1F 98 81 89 5B D2 24 B3 8F B7 6A 83 |

* When using the blank password and using the same hashing function (MD5, SHA-1) as in Question 1, does the HMAC produces the same value as hashing in Question 1? N\_ (y/n)
* Comparing between using blank password and password= “secret”, are these output values equal ? N (y/n)

**Part III: Attack to MD5 (find collision in MD5)**

**Question 3:** What are 2 different data blocks having the same MD5 hash value obtained ? Please compare and highlight/underline the different parts.

Data block 1: F1 34 14 E2 19 A5 44 2E DB 46 1A 7D DE 3B 76 46 95 9A 11 40 4A 6D D8 15 2C 2A 3C B1 D7 41 13 D0 A6 16 F5 C1 E8 B3 2D 24 87 46 77 79 CB B1 53 49 B1 5A E3 E7 6E F6 9C F4 C8 FB 9B 7C 3F 14 56 90 7B 80 D0 A2 6E D8 D2 F0 8D 56 23 77 B9 FD 6E 56 52 07 F2 5B FE 77 E1 5D C1 57 15 C1 CD 60 7D 22 0B 37 17 D7 69 D8 B2 90 57 B7 CC AF 8D 61 83 E8 B4 B4 C5 6D B0 05 D2 8F 2C 59 54 77 76 11 6D 16

Data block 2: F1 34 14 E2 19 A5 44 2E DB 46 1A 7D DE 3B 76 46 95 9A 11 C0 4A 6D D8 15 2C 2A 3C B1 D7 41 13 D0 A6 16 F5 C1 E8 B3 2D 24 87 46 77 79 CB 31 54 49 B1 5A E3 E7 6E F6 9C F4 C8 FB 9B FC 3F 14 56 90 7B 80 D0 A2 6E D8 D2 F0 8D 56 23 77 B9 FD 6E 56 52 07 F2 DB FE 77 E1 5D C1 57 15 C1 CD 60 7D 22 0B 37 17 D7 69 D8 B2 90 57 B7 CC AF 8D E1 82 E8 B4 B4 C5 6D B0 05 D2 8F 2C 59 54 F7 76 11 6D 16

What is the MD5 of data block 1 ? 78 A5 64 B2 C7 D3 71 27 A4 A8 E8 86 7D 4B B4 D7

What is the MD5 of data block 2 ? 78 A5 64 B2 C7 D3 71 27 A4 A8 E8 86 7D 4B B4 D7

Are the 2 MD5’s equal ? \_Y\_\_ (y/n) If ‘no’, try again.

**Part IV: Viewing Website Certificate**

**Question 4:**

What is the URL of the website you chose? https://www.google.com/

What is the name of protocol? QUIC

What is the name of key exchange algorithm? X25519

What is the name of encryption algorithm? AES\_128\_GCM

**Question 5:** Give the general information and details of “**Issued to**” and “**Issued by**” of the website certificate.

Purpose of Certificate Ensure the identity of a remote computer.

Valid from \_\_\_\_\_\_09/01/23\_\_\_\_\_\_\_\_ to \_\_\_\_\_\_\_03/04/23\_\_\_\_\_\_\_\_\_\_\_

Issued to : \*.google.com (Subject)

CN (Certificate Name) = GTS CA 1C3

O (Organization) = -

OU (Organizational Unit) = -

C (Country) = -

Issued by: GTS CA 1C3 (Issuer)

CN = GTS CA 1C3

O = Google Trust Services LLC

OU = -

C = US

Signature algorithm: PKCS #1 SHA-256 With RSA Encryption

Signature hash algorithm: SHA-256

Public key = ECC (256 Bits)

**Question 6:** For each certificate in “Certification Path” 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 |
| GTS CA 1C3 | GTS CA 1C3 | GTS Root R1 |
| GTS Root R1 | GTS Root R1 | GlobalSign Root CA |

**Part V: Viewing a local certificate on Windows**

**Question 7:**

* How many matched certificates (with certificates in Question 6) that you have found ? 1 (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** |
| GlobalSign Root CA | Trusted Root Certificated Authorities |
|  |  |

**Question 8:** Examine one of the found certificates from Question 7.

|  |  |
| --- | --- |
| **Attribute** | **Value** |
| Subject (only CN) | GlobalSign Root CA |
| Issuer (only CN) | GlobalSign Root CA |
| Signature Algorithm | sha1RSA |
| Signature Hash Algorithm | sha1 |
| Public Key (only algorithm name and bits) | RSA (2048 Bits =) |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_