**ITCS 461 Computer & Communication Security Date : ­\_\_\_6/2/2022\_\_\_\_**

**ID: 6288102\_ Name: Krissanapong Palakham** **Section:** \_\_\_\_1\_\_\_\_\_\_

**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 7E 55 AA F5 1D BC EE 95 C5 B3 4A E7 43 E4 B8 FF CC B4 13 | 20 |
| SHA-256 | 89 40 80 89 E6 A4 76 46 B7 16 8A 82 A2 B8 79 5C 42 27 4D A6 50 E0 9F 82 AD 4A C1 61 A5 C9 A1 03 | 32 |
| SHA-384 | 2B 88 FB 81 C6 15 BA 5B 88 00 F0 9E D7 11 0D 40 93 3A 5F 33 C3 77 5C 37 CC 2C D9 FD 95 00 24 4A 59 BB 0F 2B C9 0A DA 05 7E EE E7 27 E5 B7 0A 67 | 48 |
| SHA-512 | C8 BF D7 8E DE 37 10 EC 9A DB 70 B3 85 50 7D 90 30 57 D6 46 2F 53 30 B0 59 E9 F3 3D B7 DE 6F 83 F3 4D F3 B2 86 A5 9F 10 6A 3E EA 40 37 12 34 02 D2 EA 33 93 52 CC 91 E2 E9 E9 E1 07 CE 51 F8 65 | 64 |
| MD5 | 47 AF DF 0B CA F0 96 73 6F 12 BA C0 6B 16 3E D0 | 16 |
| SHA-3 (Keccak) | 02 80 1D 22 63 EB F0 A6 12 72 62 AB 64 92 B7 CB B7 62 1F 08 5B C3 57 77 45 87 E3 81 DF 7C 8B 7B | 32 |

**Part II: HMAC**

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

|  |  |  |
| --- | --- | --- |
| **Password** | **Hash Function** | **HMAC value** |
| Blank | MD5 | CB 78 A4 89 43 9F EC 82 48 0C E9 AA 05 B5 6C 02 |
| Blank | SHA-1 | F2 DF E5 43 B2 D2 1E 27 71 CA EA 8B 90 BD 53 8E 67 3A AD BB |
| “secret” | MD5 | 8B D6 20 FA EB 07 40 14 9B A2 9B A9 1A 73 B8 25 |
| “secret” | SHA-1 | E1 DB E9 48 C3 4D D5 86 DE 01 B0 73 8B 87 86 F2 85 4A A1 B7 |

* 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: C7 CC 80 39 AD 59 13 12 6F 73 FA DC C2 75 AB 47 A5 B8 51 9F 9E 34 7B C7 53 02 37 46 1A 29 30 1F EB B3 B0 F8 D0 C5 6A 57 8F 3E 54 F9 02 7E 38 68 8A 08 4C 13 B3 5D B5 2F 44 63 F0 4C 5A 93 01 C7 62 BF 7B F1 E0 E5 6C 25 A9 3D A3 B8 25 39 41 02 BE 78 18 23 0D 3B A0 60 CD 7B F5 CC D5 29 5D 2E 85 2B 16 DE 1D 8C A3 D1 B1 43 D1 CF 8F D5 67 A6 ED F7 04 DE D4 40 EA EB 29 A7 BB 9A 66 77 34 B2

Data block 2: C7 CC 80 39 AD 59 13 12 6F 73 FA DC C2 75 AB 47 A5 B8 51 1F 9E 34 7B C7 53 02 37 46 1A 29 30 1F EB B3 B0 F8 D0 C5 6A 57 8F 3E 54 F9 02 FE 38 68 8A 08 4C 13 B3 5D B5 2F 44 63 F0 CC 5A 93 01 C7 62 BF 7B F1 E0 E5 6C 25 A9 3D A3 B8 25 39 41 02 BE 78 18 A3 0D 3B A0 60 CD 7B F5 CC D5 29 5D 2E 85 2B 16 DE 1D 8C A3 D1 B1 43 D1 CF 8F 55 67 A6 ED F7 04 DE D4 40 EA EB 29 A7 BB 1A 66 77 34 B2

What is the MD5 of data block 1 ? 36 56 91 5F 62 B7 D6 63 3F B7 42 BE 10 93 FD 51

What is the MD5 of data block 2 ? 36 56 91 5F 62 B7 D6 63 3F B7 42 BE 10 93 FD 51

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.co.th/?hl=th

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 \_\_\_\_ Ensures the identity of a remote computer\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Valid from \_\_\_\_\_\_1/10/2022\_\_\_\_\_\_\_\_\_\_\_ to \_\_\_\_\_\_4/4/2022\_\_\_\_\_\_\_\_\_\_\_\_

Issued to : \_\_\_\_\_\*.google.co.th\_\_\_\_\_\_\_\_\_\_\_\_(Subject)

CN (Certificate Name) = \*.google.co.th

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 \_\_\_\_\_\_\_sha256RSA\_\_\_\_\_\_\_\_\_\_

Signature hash algorithm \_\_\_\_\_\_\_sha256\_\_\_\_\_\_\_\_\_\_

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 |
| GlobalSign Root CA - R1 | GlobalSign Root CA - 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 |

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