ITCS 461 Computer & Communication Security Date : _2/7/2023__
ID:_6388014_ Name: Waris Damkham_________ Section: ____2______

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	47 7B 5C 65 9D 36 76 BC D2 59 80 DF 77 B8 41 76 F1 35 15 76	20
SHA-256	A9 28 0D EC C5 2D 03 94 E6 BE 58 1E 1A 0B 3E A0 5B 6C E4 BC E5 99 D0 2B 11 E2 37 5E B3 51 BB 5B	32
SHA-384	7B BE B6 28 E7 8A 95 56 EF F2 42 A3 E4 4C 74 1C F1 63 56 B5 0F AC 36 F6 32 75 A7 55 43 4F 44 5B 1D 0D C9 0E 9E 63 C9 BB 8C E1 97 2B FC 08 5B 5A	48
SHA-512	F9 5D D2 B2 20 81 CF 14 48 EE 4D A9 6F E7 E6 46 3E 16 AA BA 63 BE 98 55 F4 94 A3 4E F7 D4 C8 52 75 40 9B B8 F1 E4 7A BA 5A 73 E3 E0 6F 42 7B 2F 2F 30 CE E3 A1 18 D7 0A 11 CB F4 D4 7A 38 C2 76	64
MD5	CA 0C E6 12 BB DA 3D 0C 84 96 A7 01 C0 B6 EF A8	16
SHA-3 (Keccak)	89 6F C8 C9 95 29 4C CA 0F 4B 5D 25 B4 FF D9 6D E2 23 F4 20 30 55 6F 3E 36 A0 CC 0B BF 0D 63 16	32

Part II: HMAC

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

Password	Hash Function	HMAC value
Blank	MD5	CD 75 96 94 48 AD 5E F2 9A E2 A7 39 F0 AB DF 57
Blank	SHA-1	50 9B D1 EB 24 1D BF DB 01 6F 6D D8 4A 37 E9 33 11 54 FF DE
"secret"	MD5	62 32 6F 20 BC F8 15 71 45 4E 8D B3 8F 0D 71 B9
"secret"	SHA-1	17 08 66 71 D9 42 30 CA CE 3F D5 46 62 AE 50 E5 A3 19 CD 72

- 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: A9 38 28 FC B9 74 23 A4 F6 5E DB 0F F3 51 3C C5 7D CE 7B E1 5F C3 0B 58 54 3A 3A 52 D2 3B A1 4E 6F 12 14 E9 6A 92 CD 1E 67 22 4E 02 DC B3 74 D0 98 FF BE 2A 0E 7A D5 C2 5C EE 36 73 74 29 76 32 BE DC 11 39 C0 18 3D A7 83 54 71 D1 1F 21 6D 2A D9 D7 D9 38 8C D6 70 3C 20 FD B1 96 CD 1A 82 CE ED D7 3E C1 AF B2 ED 85 2E 40 D9 A9 8F 28 5A 9C 00 E5 A1 39 8D C5 53 05 E1 5B C7 EA 24 B0 C8 40

Data block 2: A9 38 28 FC B9 74 23 A4 F6 5E DB 0F F3 51 3C C5 7D CE 7B 61 5F C3 0B 58 54 3A 3A 52 D2 3B A1 4E 6F 12 14 E9 6A 92 CD 1E 67 22 4E 02 DC 33 75 D0 98 FF BE 2A 0E 7A D5 C2 5C EE 36 F3 74 29 76 32 BE DC 11 39 C0 18 3D A7 83 54 71 D1 1F 21 6D 2A D9 D7 D9 B8 8C D6 70 3C 20 FD B1 96 CD 1A 82 CE ED D7 3E C1 AF B2 ED 85 2E 40 D9 A9 8F A8 59 9C 00 E5 A1 39 8D C5 53 05 E1 5B C7 6A 24 B0 C8 40

What is the MD5 of data block 1 ? 0E 51 01 1A 4C 48 91 E5 C0 1C 12 D8 5C 4D CA A7

What is the MD5 of data block 2 ? 0E 51 01 1A 4C 48 91 E5 C0 1C 12 D8 5C 4D CA A7

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? _TLS 1.3, 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 _Validate website certificate__
Valid from _ Monday, January 9, 2023 at 3:19:12 PM to _Monday, April 3, 2023 at 3:19:
Issued to : __ www.google.com ________(Subject)
CN (Certificate Name) = ___www.google.com____
O (Organization) = _____<Not Part Of Certificate>_________
OU (Organizational Unit) = ________<Not Part Of Certificate>_________
C (Country) = _________-______________________
Issued by : ___ ESET SSL Filter CA _________(Issuer)
CN = __ESET SSL Filter CA__
O = ___ESET, spol. s r. o.____
OU = _<Not Part Of Certificate>____
C = ____-__________________________
Signature algorithm ___ PKCS #1 SHA-256 With RSA Encryption ______
Signature hash algorithm ______SHA-256 ___________
Public key ___ 00 04 C8 D0 7A 1F 7B 8C 49 FC 6E 98 B6 84 83 3B
DD E3 88 9F 50 BB AF 4E 0F F2 B9 CB 6F 76 56 E3
D5 D4 CE CA 97 01 22 EA B0 35 A3 AD 5F 48 F4 2C
14 84 10 B5 BF 83 83 3E F2 AE B8 9D A9 DC 91 0A
02 14 _

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
ESET SSL Filter CA	ESET SSL Filter CA	ESET SSL Filter 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
Microsoft to GoDaddy G2 Cross Certificate	*Intermediate certification authorities*
GoDaddy Class 2 Certification Authority Root Certificate - G2	*Intermediate certification authorities*

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

Attribute	Value
Subject (only CN)	Go Daddy Secure Certificate Authority - G2
Issuer (only CN)	Go Daddy Root Certificate Authority - G2
Signature Algorithm	sha256RSA
Signature Hash Algorithm	sha256
Public Key (only algorithm name and bits)	RSA (2048 Bits)