Lab 3: Hashing Message Digest and Certificates

ITCS461: Computer and Communication Security

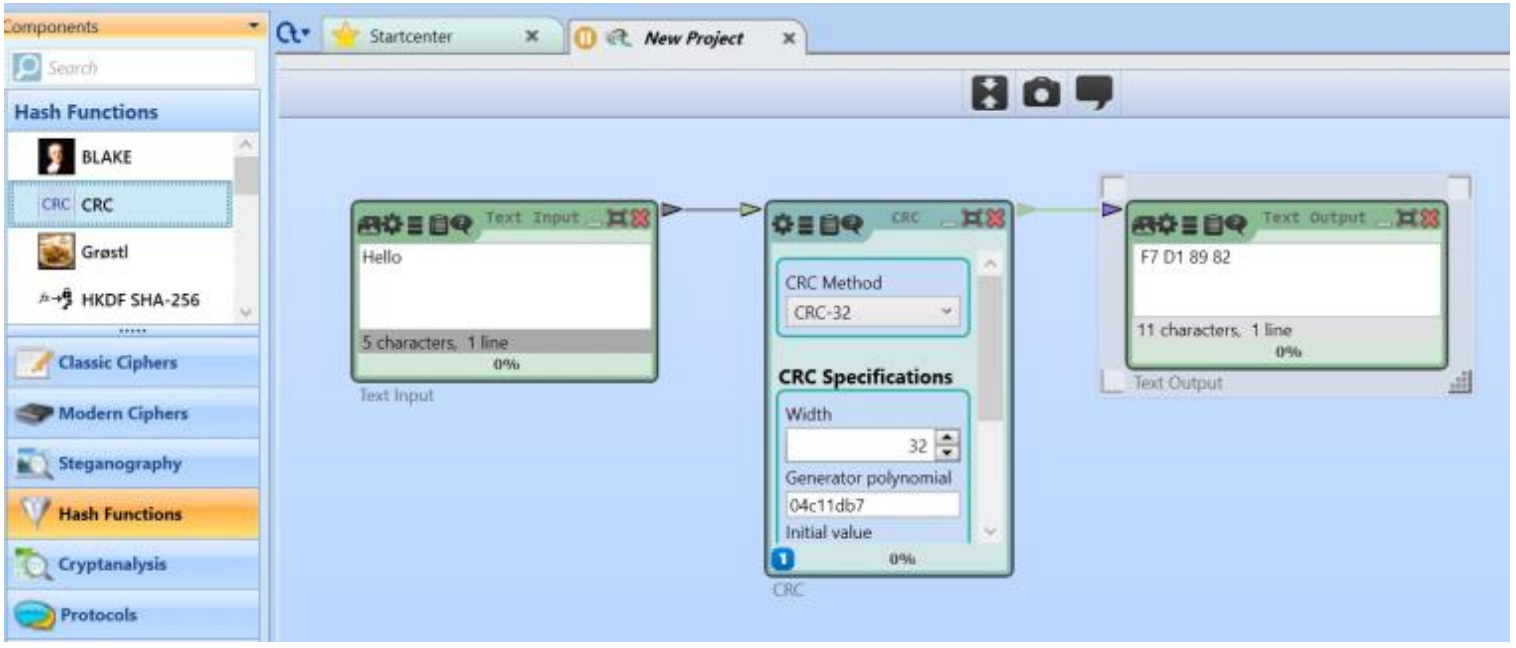
Mahidol University

Agenda

1. Part I: Hashing
2. Part II: HMAC
3. Part III: Attack to MD5 (Find collision)
4. Part IV: Viewing Website Certificate
5. Part V: Viewing a local certificate on Windows

Part I: Hashing

1. Open **Cryptool2** program
2. Create a new project
3. Click **Hash Functions** category on the left side
4. Drag **SHA** tool into the workspace
5. Adding **Text Input** and **Text Output** on the left and right side of the box as shown below



Part I: Hashing

Question 1: Find the message digests for your full name, using the following algorithms:

SHA-1, SHA-256, SHA-384, SHA-512, MD5, SHA-3 (Keccak)

Note:.

- For **SHA-1**, **SHA-256**, **SHA-384**, **SHA-512**: Use **SHA** tool and set **SHA Function** accordingly.
- For **MD5** and **Keccak**, the tool is a presentation. You need to resize the box so you can read what inside. After click ”Play”, you can then click **”Next”** or **”Skip”** button inside the box. The final hash value is at the end of the presentation.

Also, count the bytes of each hash. (remember: 2 hexadecimal digits are counted as 1 byte.)

Algorithm	Hash Value (Message Digest)	Length (bytes)
SHA-1	D0 07 FB 1F 4B E6 D6 EE 6D F0 F9 97 CB 78 0A F8 D0 29 D9 29	20
…	…	…
…	…	…

Part II: HMAC

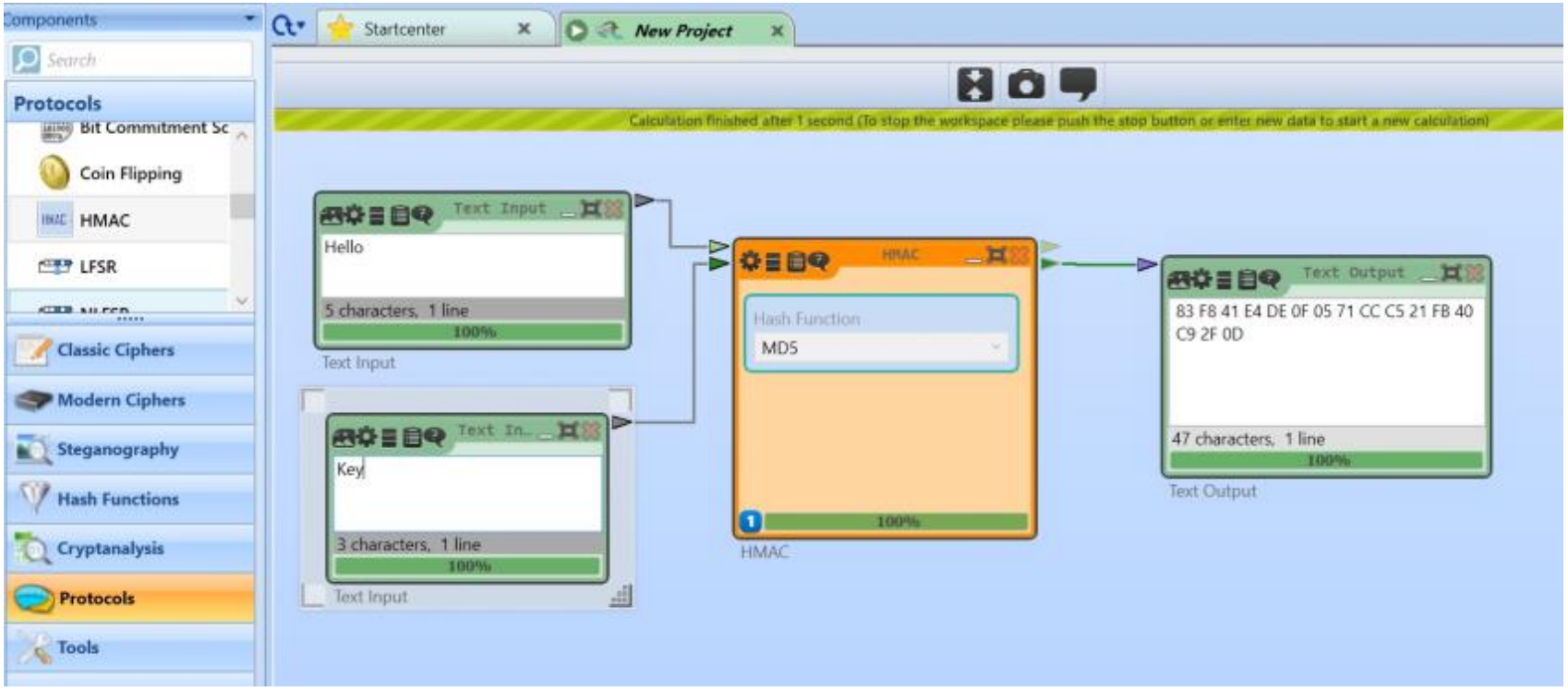
HMAC is a keyed-hash message authentication code.

It requires a Key (or Password) that knows between both parties (sender/receiver). It is to ensure, whether or not only the message has been tampered with, but also the message has only been seen by either of the parties, not someone else.

Part II: HMAC

To use HMAC

select **Protocol** category, then drag **HMAC** tool into the workspace, and configure it as shown below:



Part II: HMAC

Question 2: Find a message digest of your full name using HMAC with these variations:

1. set Password to blank, and Hash function = MD5
2. set Password to blank, and Hash function = SHA1
3. set Password to the word "secret", and Hash function = MD5
4. set Password to the word "secret", and Hash function = SHA1

- When using the blank password and using the same hashing function (MD5, SHA1) as in Question 1, does the HMAC produces the same value as hashing in Question 1 ? ____(Y/N)
- Comparing between using blank password and password="secret", are these output values equal or differ? _____

Part III: Attack to MD5 (Find collision)

To find 2 different data blocks having the same MD5 hash value, perform the following steps:

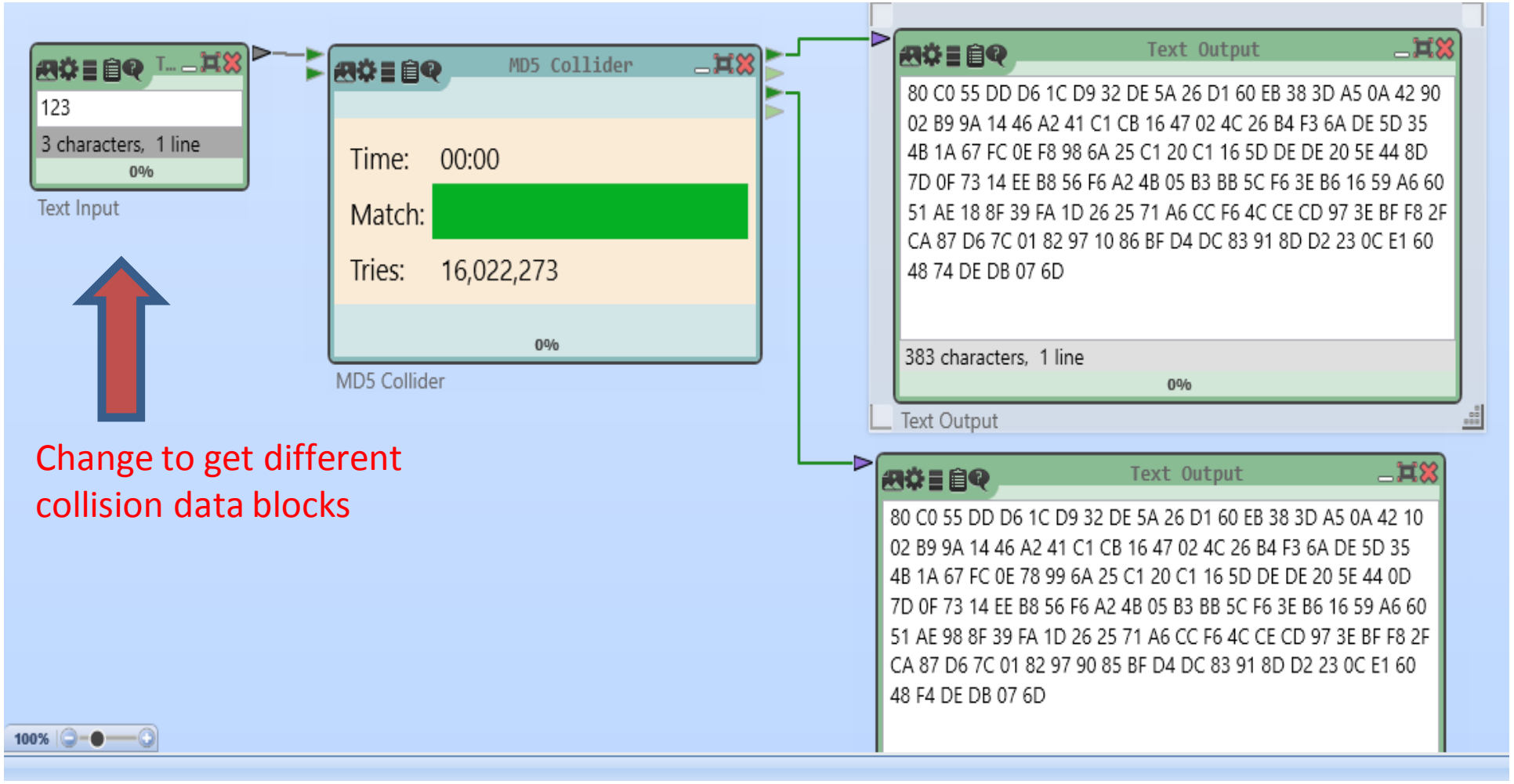
1. Click at **New** to create a new project.
2. Click **Hash Functions** category on the left side.
3. Drag **MD5 Collider** into the workspace.
4. Drag and create input random seed box as text input on the left of **MD5 Collider** and 2 text output for 2 data blocks on the right side as shown in the next slide.
5. Enter *last 3 digits of your student ID* in random seed box, then click play, wait until output data blocks are obtained, then stop.

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

Data block 1 : _____

Data block 2 : _____

Using MD5 Collider



Change to get different collision data blocks

Part III: Attack to MD5 (Find collision)

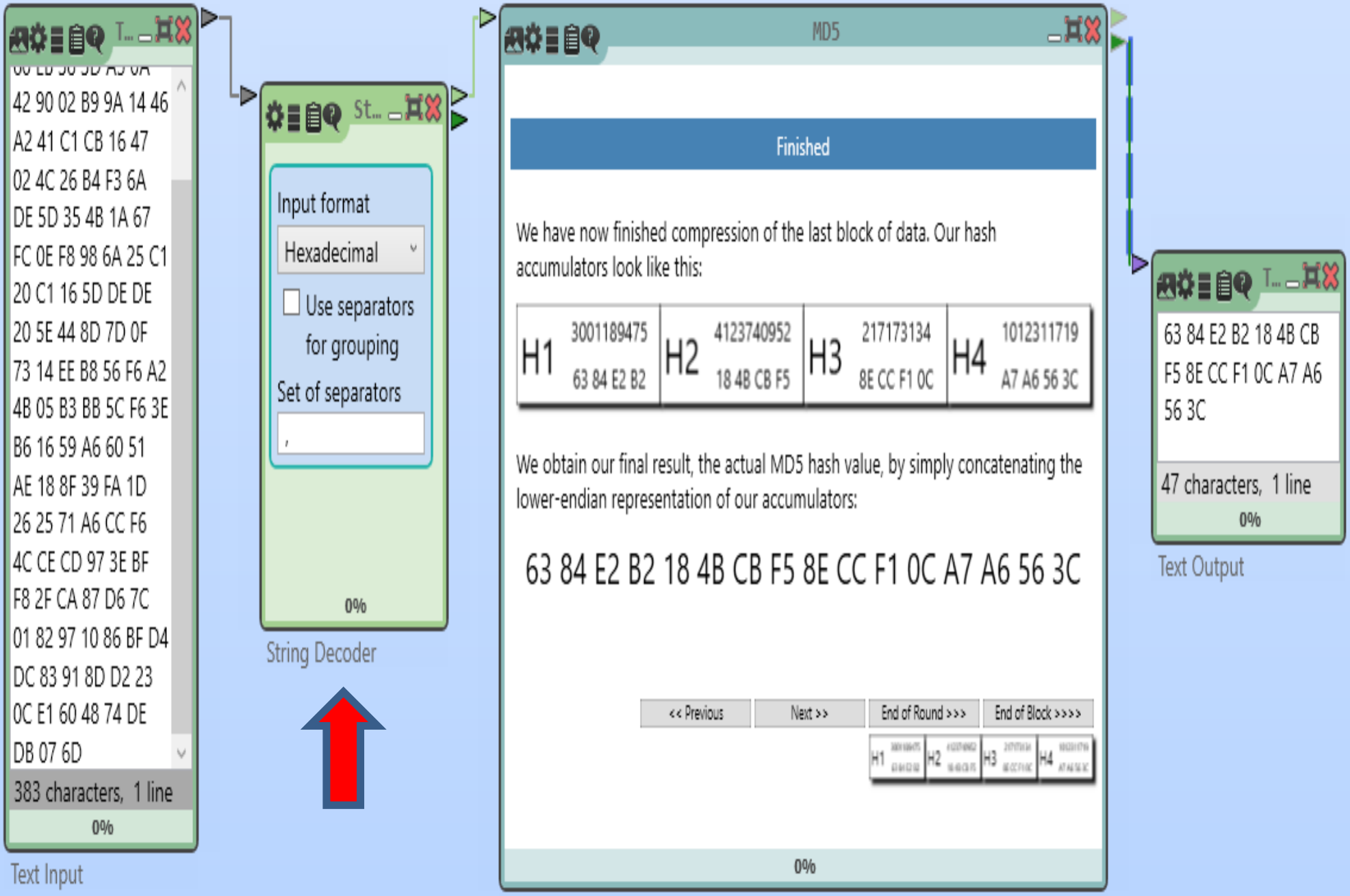
Verify for the collision : Copy output data from both blocks, one by one, to **MD5** input (**Question 1**), and play to find hash values.

What is the MD5 of data block 1 ? _____

What is the MD5 of data block 2 ? _____

Are they equal ? ___ (y/n) If 'not', try again.

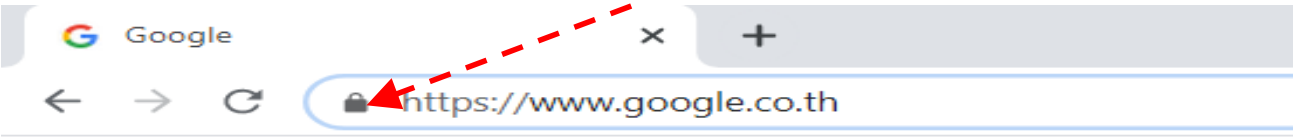
Because the input data to **MD5** is hexadecimal you need "**String Decoder**" to convert data before input to **MD5** as shown in the next slide.


42 90 02 B9 9A 14 46
A2 41 C1 CB 16 47
02 4C 26 B4 F3 6A
DE 5D 35 4B 1A 67
FC 0E F8 98 6A 25 C1
20 C1 16 5D DE DE
20 5E 44 8D 7D 0F
73 14 EE B8 56 F6 A2
4B 05 B3 BB 5C F6 3E
B6 16 59 A6 60 51
AE 18 8F 39 FA 1D
26 25 71 A6 CC F6
4C CE CD 97 3E BF
F8 2F CA 87 D6 7C
01 82 97 10 86 BF D4
DC 83 91 8D D2 23
0C E1 60 48 74 DE
DB 07 6D
383 characters, 1 line
0%
Text Input
Input format
Hexadecimal
Use separators for grouping
Set of separators
,
0%
String Decoder
MD5
Finished
We have now finished compression of the last block of data. Our hash accumulators look like this:
H1 3001189475 63 84 E2 B2
H2 4123740952 18 4B CB F5
H3 217173134 8E CC F1 0C
H4 1012311719 A7 A6 56 3C
We obtain our final result, the actual MD5 hash value, by simply concatenating the lower-endian representation of our accumulators:
63 84 E2 B2 18 4B CB F5 8E CC F1 0C A7 A6 56 3C
<< Previous
Next >>
End of Round >>>
End of Block >>>>
0%
63 84 E2 B2 18 4B CB F5 8E CC F1 0C A7 A6 56 3C
47 characters, 1 line
0%
Text Output

Part IV: Viewing Website Certificate

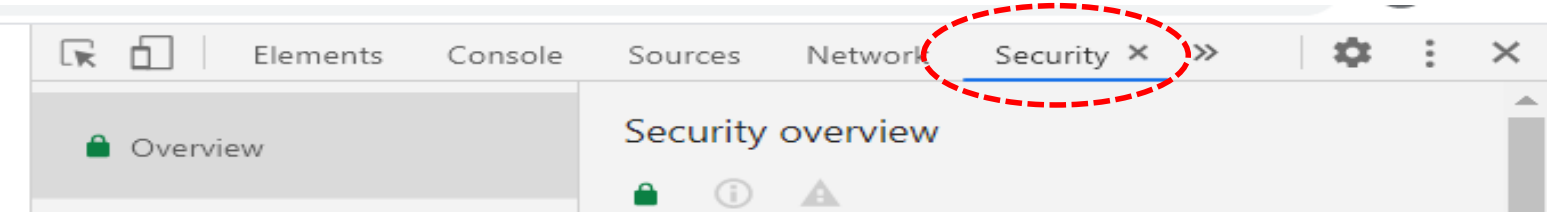
Now we switch to see encryption in real-life usage.

1. Open Google Chrome browser.
2. Go to any website that uses HTTPS (for example: google.com, facebook.com, twitter.com, etc.)
3. Notice that there must be a padlock symbol in front of the URL.



It means the website is properly setup for HTTPS, and the transmission is encrypted.

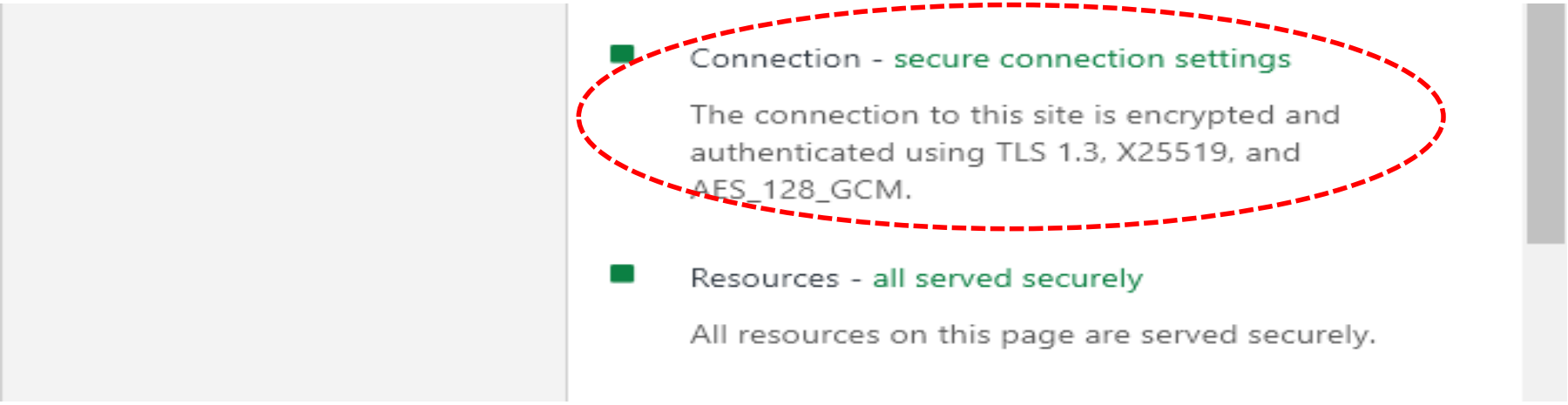
4. Press **F12** key on your keyboard, a new window will appear. This is Chrome's built-in developer tools window.
5. Click on "**Security**" tab.



Part IV: Viewing Website Certificate

Question 4: Read the "secure connection settings" section. It lists the algorithm names that currently using with this connection to the website. Fill in the followings:

- What is the URL of the website you chose? _____
- What is the name of protocol? _____
- What is the name of key exchange algorithm? _____
- What is the name of encryption algorithm? _____

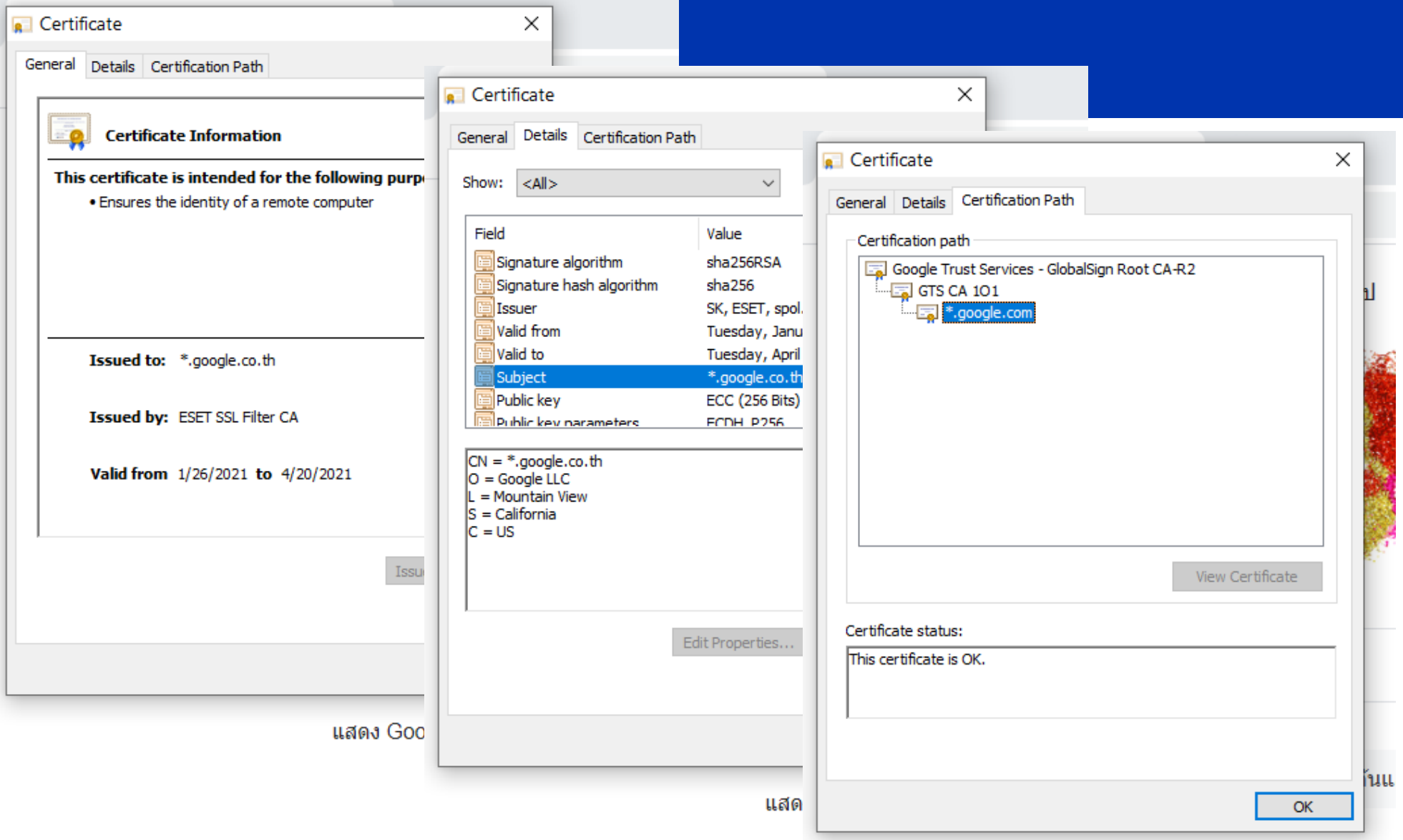


Part IV: Viewing Website Certificate

Next, Click on the button named "View certificate".
A pop-up Certificate window will appear, showing general information of current certificate of this website.

On the pop-up window, click on the "Details" tab. This tab shows full certificate details.

Question 5: What are the general information, and detailed values of "Issued to" and "Issued by" of the website certificate? (answer all CN, O, OU, C if available)



แสดง Google ใน: English

Part IV: Viewing Website Certificate

On the pop-up Certificate window, click on the "Certification Path" tab. This tab shows full certificate chain and detail of each certificate.

Question 6: Click to view details of each certificate in "Certification Path" box from the bottom-up, and fill it in the table.

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

Part V: Viewing a local certificate on Windows

To view a local certificate on Windows, proceed the following steps.

In your browser, click at

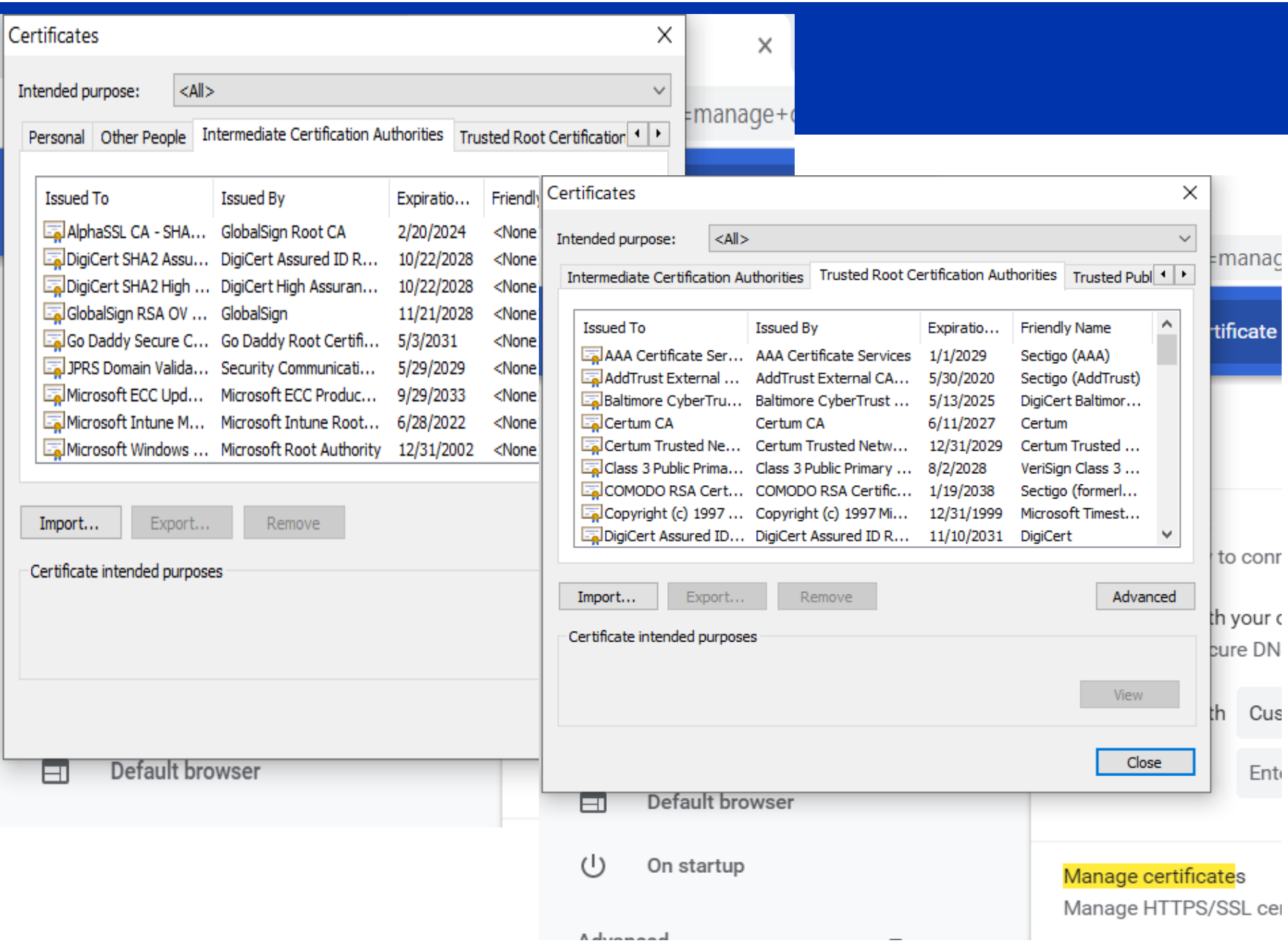
→ **triple dots icon, ⋮ or . . .**

→ **Settings**

→ Search for **"Manage Certificates"**

→ **click**

On the pop-up Certificate window, click on every tab to find certificate information then answer to the following questions.


Certificates
Intended purpose: <All>
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification
Issued To | Issued By | Expiratio... | Friendly
AlphaSSL CA - SHA... | GlobalSign Root CA | 2/20/2024 | <None
DigiCert SHA2 Assu... | DigiCert Assured ID R... | 10/22/2028 | <None
DigiCert SHA2 High ... | DigiCert High Assuran... | 10/22/2028 | <None
GlobalSign RSA OV ... | GlobalSign | 11/21/2028 | <None
Go Daddy Secure C... | Go Daddy Root Certifi... | 5/3/2031 | <None
JPRS Domain Valida... | Security Communicati... | 5/29/2029 | <None
Microsoft ECC Upd... | Microsoft ECC Produc... | 9/29/2033 | <None
Microsoft Intune M... | Microsoft Intune Root... | 6/28/2022 | <None
Microsoft Windows ... | Microsoft Root Authority | 12/31/2002 | <None
Import...
Export...
Remove
Certificate intended purposes
Default browser
Certificates
Intended purpose: <All>
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Issued To | Issued By | Expiratio... | Friendly Name
AAA Certificate Ser... | AAA Certificate Services | 1/1/2029 | Sectigo (AAA)
AddTrust External ... | AddTrust External CA... | 5/30/2020 | Sectigo (AddTrust)
Baltimore CyberTru... | Baltimore CyberTrust ... | 5/13/2025 | DigiCert Baltimor...
Certum CA | Certum CA | 6/11/2027 | Certum
Certum Trusted Ne... | Certum Trusted Netw... | 12/31/2029 | Certum Trusted ...
Class 3 Public Prima... | Class 3 Public Primary ... | 8/2/2028 | VeriSign Class 3 ...
COMODO RSA Cert... | COMODO RSA Certific... | 1/19/2038 | Sectigo (formerl...
Copyright (c) 1997 ... | Copyright (c) 1997 Mi... | 12/31/1999 | Microsoft Timest...
DigiCert Assured ID... | DigiCert Assured ID R... | 11/10/2031 | DigiCert
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Close
Default browser
On startup
Manage certificates
Manage HTTPS/SSL cer

Part V: Viewing a local certificate on Windows

Question 7: Using the answer from **Question 6**, try to find the certificates that match with the **Subject (CN)** names. You may need to look for it in all the tabs as well.

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

  _____

Part V: Viewing a local certificate on Windows

Question 8: Pick one certificate that you have found, and examine it by select on it and click on “View” button and then click on “Details” tab. Then, fill in this table:

Attribute	Value
Subject (only CN)	…
Issuer (only CN)	…
Signature Algorithm	…
Signature Hash Algorithm	…
Public Key (only algorithm name and bits)	…