Name_____ student ID_____No_____

Activity: Digital Certificate

1) Use Mozilla Firefox or Google Chrome to visit a web site with https protocol

1.1) URL: _____

1.2) view the certificate of the site and answer the following questions

　　　Issuer of the certificate: _____

　　　Validity of the certificate: _____

　　　Certificate Hierarchy: _____

　　　_____

　　　_____

　　　_____

　　　Certificate signature algorithm: _____

　　　Subject: _____

　　　Subject Public key algorithm: _____

　　　CRL Distribution point: _____

2) Check the certificates installed on your machine

2.1) Did you find any certificate from DigiNotar CA? ☐ No ☐ Yes How many? _____

　　　List the subject of the certificates _____

　　　_____

　　　_____

　　　_____

　　　_____

2.2) Did you find any certificate that is expired? ☐ No ☐ Yes How many? _____

　　　List the subject of the certificates _____

　　　_____

　　　_____

　　　_____

　　　_____

2.3) Did you find any certificate that uses RSA 1024 bits? ☐ No ☐ Yes How many? _____

　　　List the subject of the certificates _____

　　　_____

　　　_____

　　　_____

　　　_____

2.4) Did you find any certificate that uses ECC? ☐ No ☐ Yes How many? _____

　　　List the subject of the certificates _____

　　　_____

　　　_____

　　　_____

Name_____ student ID_____No_____

3) Visit https://passport.psu.ac.th/index.php?content=ca, please note that you will be asked to provide your PSU passport in order to visit the site. Download CA certificate. Then open it. Check the following

Issuer of the certificate: _____

Validity of the certificate: _____

Certificate Hierarchy: _____

_____

_____

_____

_____

_____

Certificate signature algorithm: _____

Subject: _____

Subject Public key algorithm: _____

CRL Distribution point: _____

In your opinion, will you trust this certificate? ☐ No ☐ Yes Why? Or Why not? _____

_____

_____

_____

_____

_____

4) Visit https://punchsalad.com/ssl-certificate/install-lets-encrypt-godaddy/ Read about how to generate a free SSL certificate provided on the page, and answer the following questions

4.1) what are being checked by the site in order to generate the certificate?

_____

_____

_____

_____

_____

_____

_____

4.2) Will you trust the certificate generated from this site? ☐ No ☐ Yes Why? Or Why not? _____

_____

_____

_____

_____

_____

_____

_____

_____