Task 6

Manually Verifying an X.509 Certificate

6.1 ชุดคำสั่งภาษา C

```
#include <stdio.h>

#include <stdlib.h>

#include <string.h>

#include <openssl/pem.h>

#include <openssl/x509.h>



int main() {

        FILE *ca_cert_file = fopen("c1.pem", "r");

        if (!ca_cert_file) {

        fprintf(stderr, "Error: Unable to open CA certificate file.\n");

        return EXIT_FAILURE;

}

 X509 *ca_cert = PEM_read_X509(ca_cert_file, NULL, NULL, NULL);

fclose(ca_cert_file);
```

```
if (!ca_cert) {
        fprintf(stderr, "Error: Failed to read CA certificate.\n");
        return EXIT_FAILURE;
}
EVP_PKEY *ca_public_key = X509_get_pubkey(ca_cert);
X509_free(ca_cert);
if (!ca_public_key) {
        fprintf(stderr, "Error: Failed to extract public key from CA certificate.\n");
        return EXIT_FAILURE;
}

FILE *server_cert_file = fopen("c0.pem", "r");
if (!server_cert_file) {
        fprintf(stderr, "Error: Unable to open server certificate file.\n");
        EVP_PKEY_free(ca_public_key);
        return EXIT_FAILURE;
}
X509 *server_cert = PEM_read_X509(server_cert_file, NULL, NULL, NULL);
fclose(server_cert_file);
```

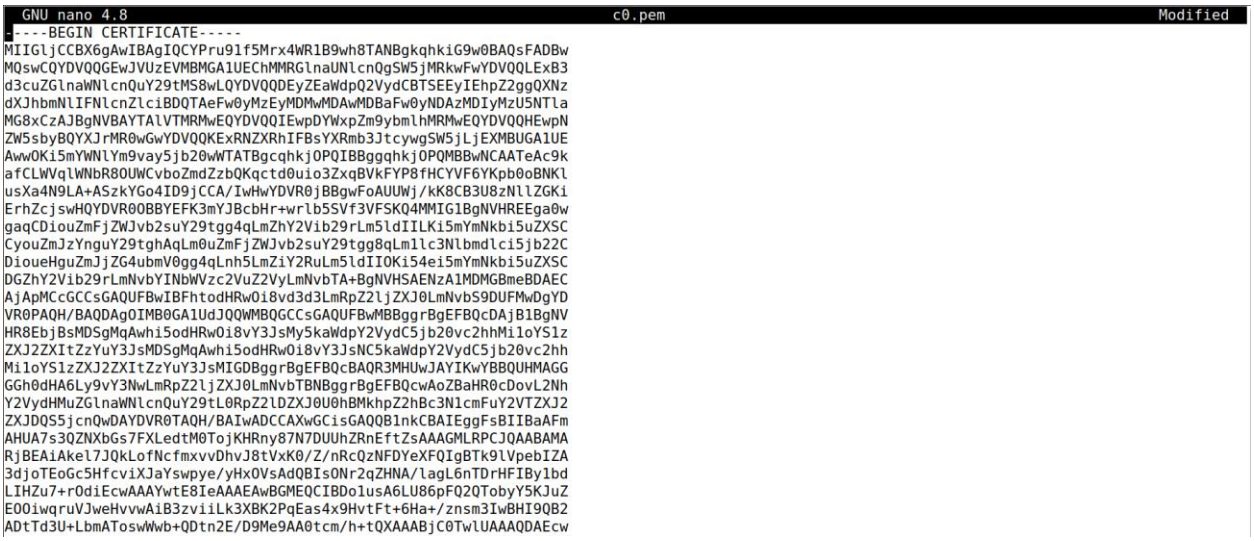
```
if (!server_cert) {
        fprintf(stderr, "Error: Failed to read server certificate.\n");
        EVP_PKEY_free(ca_public_key);
        return EXIT_FAILURE;
}


EVP_MD_CTX *md_ctx = EVP_MD_CTX_new();
if (!md_ctx) {
        fprintf(stderr, "Error: Failed to create message digest context.\n");
        X509_free(server_cert);
        EVP_PKEY_free(ca_public_key);
        return EXIT_FAILURE;
}
```

```
    if (X509_verify(server_cert, ca_public_key) != 1) {
        fprintf(stderr, "Error: Signature verification failed.\n");
        EVP_PKEY_free(ca_public_key);
        X509_free(server_cert);
        EVP_MD_CTX_free(md_ctx);
        return EXIT_FAILURE;
    }

    printf("Signature verification succeeded.\n");

    X509_free(server_cert);
    EVP_PKEY_free(ca_public_key);
    EVP_MD_CTX_free(md_ctx);

    return EXIT_SUCCESS;
}
```

6.1.1 คำอธิบายชุดคำสั่ง

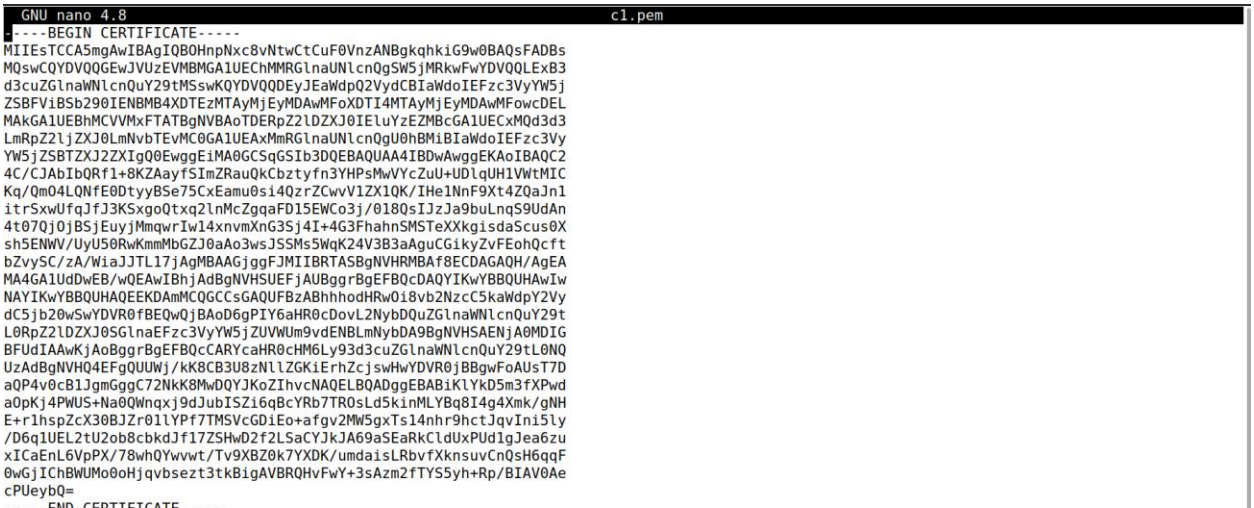
เป็นชุดคำสั่งสำหรับใช้ตรวจสอบลายเซ็นเซิร์ฟเวอร์ในไฟล์ c0.pem ว่าถูกลงชื่อด้วยคีย์สาธารณะของ Certificate Authority (CA) ที่ระบุในไฟล์ c1.pem

รูปภาพของภายในไฟล์ c0.pem ที่เก็บลายเซ็นเซิร์ฟเวอร์ของ Facebook.com



```
 GNU nano 4.8                                    c0.pem                                    Modified
-----BEGIN CERTIFICATE-----
MIIGljCCBX6gAwIBAgIQCYPru91f5Mrx4WR1B9wh8TANBgkqhkiG9w0BAQsFADBw
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMS8wLQYDVQQDEyZEaWdpQ2VydCBTSEEyIEhpZ2ggQXNz
dXJhbmNlIFNlcnZlciBDQTAeFw0yMzEyMDMwMDAwMDBaFw0yNDAzMDIyMzU5NTla
MG8xCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRMwEQYDVQQHEwpN
ZW5sbyBQYXJrMR0wGwYDVQQKExRNZXRhIFBsYXRmb3JtcywgSW5jLjEXMBUGA1UE
AwwOKi5mYWNlYm9vay5jb20wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATeAc9k
afCLWVqlWNbR8OUWCvboZmdZzbQKqctd0uio3ZxqBVkFYP8fHCYVF6YKpb0oBNKl
usXa4N9LA+ASzkYGo4ID9jCCA/IwHwYDVR0jBBgwFoAUUWj/kK8CB3U8zNllZGKi
ErhZcjswHQYDVR0OBBYEFK3mYJBcbHr+wrlb5SVf3VFSKQ4MMIG1BgNVHREEga0w
gaqCDiouZmFjZWJvb2suY29tgg4qLmZhY2Vib29rLm5ldIILKi5mYmNkbi5uZXSC
CyouZmJzYnguY29tghAqLm0uZmFjZWJvb2suY29tgg8qLm1lc3Nlbmdlci5jb22C
DioueHguZmJjZG4ubmV0gg4qLnh5LmZiY2RuLm5ldIIOKi54ei5mYmNkbi5uZXSC
DGZhY2Vib29rLmNvbYINbWVzc2VuZ2VyLmNvbTA+BgNVHSAENzA1MDMGBmeBDAEC
AjApMCcGCCsGAQUFBwIBFhtodHRwOi8vd3d3LmRpZ2ljZXJ0LmNvbS9DUFMwDgYD
VR0PAQH/BAQDAgOIMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjB1BgNV
HR8EbjBsMDSgMqAwhi5odHRwOi8vY3JsMy5kaWdpY2VydC5jb20vc2hhMi1oYS1z
ZXJ2ZXItZzYuY3JsMDSgMqAwhi5odHRwOi8vY3JsNC5kaWdpY2VydC5jb20vc2hh
Mi1oYS1zZXJ2ZXItZzYuY3JsMIGDBggrBgEFBQcBAQR3MHUwJAYIKwYBBQUHMAGG
GGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBNBggrBgEFBQcwAoZBaHR0cDovL2Nh
Y2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0U0hBMkhpZ2hBc3N1cmFuY2VTZXJ2
ZXJDQS5jcnQwDAYDVR0TAQH/BAIwADCCAXwGCisGAQQB1nkCBAIEggFsBIIBaAFm
AHUA7s3QZNXbGs7FXLedtM0TojKHRny87N7DUUhZRnEftZsAAAGMLRPCJQAABAMA
RjBEAiAkel7JQkLofNcfmxvvDhvJ8tVxK0/Z/nRcQzNFDYeXFQIgBTk9lVpebIZA
3djoTEoGc5HfcviXJaYswpye/yHxOVsAdQBIsONr2qZHNA/lagL6nTDrHFIBy1bd
LIHZu7+rOdiEcwAAAYwtE8IeAAAEAwBGMEQCIBDo1usA6LU86pFQ2QTobyY5KJuZ
EOOiwqruVJweHvvwAiB3zviiLk3XBK2PqEas4x9HvtFt+6Ha+/znsm3IwBHI9QB2
ADtTd3U+LbmAToswWwb+QDtn2E/D9Me9AA0tcm/h+tQXAAABjC0TwlUAAAQDAEcw

RQIgOLtxl32FVu+u1643t/hqTTdfd7jD255t7rtwCsZB+PwCIQD7rrcQlVD2XzAC
eFgML/rhVrRYpglzmexej9VmTzAs8TANBgkqhkiG9w0BAQsFAAOCAQEAJ7OVn6KO
6l3INwI/wdOZLe2s/SJhKuL3LhRJlCC1BsA83ord8/KLfau2oACf4pFCRrL/fomd
a15uzv+Fp2fLRRBUOnAgF7FJy1SkRrT0YrscPiGiiUMltE6Q712hmm6joBgjCmEj
A0CK62mbI9f4+uzKgGgA0MYI6A+/flurPsdbQYHhLSiqXIMaeKjBMTzTRdD3nWbE
u+zUkUAxx6JgFs5kawnG65L8aGnHVSKbFkGiFfWuyfnqAo1VmnJF9d51tBFPV6rL
ni/+LReVSeTQBcSChSZAXlE0Slas3NJ9Rkm+vfc1XX73ciVnsnhOU24i0vg8mzBC
NKtmHVXIx8SMQA==
-----END CERTIFICATE-----
```

รูปภาพของภายในไฟล์ c1.pem ที่เก็บคีย์สาธารณะ Certificate Authority (CA)ของ Facebook.com



```
 GNU nano 4.8                                    c1.pem
-----BEGIN CERTIFICATE-----
MIIEsTCCA5mgAwIBAgIQBOHnpNxc8vNtwCtCuF0VnzANBgkqhkiG9w0BAQsFADBs
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSswKQYDVQQDEyJEaWdpQ2VydCBIaWdoIEFzc3VyYW5j
ZSBFViBSb290IENBMB4XDTEzMTAyMjEyMDAwMFoXDTI4MTAyMjEyMDAwMFowcDEL
MAkGA1UEBhMCVVMxFTATBgNVBAoTDERpZ2lDZXJ0IEluYzEZMBcGA1UECxMQd3d3
LmRpZ2ljZXJ0LmNvbTEvMC0GA1UEAxMmRGlnaUNlcnQgU0hBMiBIaWdoIEFzc3Vy
YW5jZSBTZXJ2ZXIgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC2
4C/CJAbIbQRf1+8KZAayfSImZRauQkCbztyfn3YHPsMwVYcZuU+UDlqUH1VWtMIC
Kq/QmO4LQNfE0DtyyBSe75CxEamu0si4QzrZCwvV1ZX1QK/IHe1NnF9Xt4ZQaJn1
itrSxwUfqJfJ3KSxgoQtxq2lnMcZgqaFD15EWCo3j/018QsIJzJa9buLnqS9UdAn
4t07QjOjBSjEuyjMmqwrIw14xnvmXnG3Sj4I+4G3FhahnSMSTeXXkgisdaScus0X
sh5ENWV/UyU50RwKmmMbGZJ0aAo3wsJSSMs5WqK24V3B3aAguCGikyZvFEohQcft
bZvySC/zA/WiaJJTL17jAgMBAAGjggFJMIIBRTASBgNVHRMBAf8ECDAGAQH/AgEA
MA4GA1UdDwEB/wQEAwIBhjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw
NAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhhodHRwOi8vb2NzcC5kaWdpY2Vy
dC5jb20wSwYDVR0fBEQwQjBAoD6gPIY6aHR0cDovL2NybDQuZGlnaWNlcnQuY29t
L0RpZ2lDZXJ0SGlnaEFzc3VyYW5jZUVWUm9vdENBLmNybDA9BgNVHSAENjA0MDIG
BFUdIAAwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cuZGlnaWNlcnQuY29tL0NQ
UzAdBgNVHQ4EFgQUUWj/kK8CB3U8zNllZGKiErhZcjswHwYDVR0jBBgwFoAUsT7D
aQP4v0cB1JgmGggC72NkK8MwDQYJKoZIhvcNAQELBQADggEBABiKlYkD5m3fXPwd
aOpKj4PWUS+Na0QWnqxj9dJubISZi6qBcYRb7TROsLd5kinMLYBq8I4g4Xmk/gNH
E+r1hspZcX30BJZr01lYPf7TMSVcGDiEo+afgv2MW5gxTs14nhr9hctJqvIni5ly
/D6q1UEL2tU2ob8cbkdJf17ZSHwD2f2LSaCYJkJA69aSEaRkCldUxPUd1gJea6zu
xICaEnL6VpPX/78whQYwvwt/Tv9XBZ0k7YXDK/umdaisLRbvfXknsuvCnQsH6qqF
0wGjIChBWUMo0oHjqvbsezt3tkBigAVBRQHvFwY+3sAzm2fTYS5yh+Rp/BIAV0Ae
cPUeybQ=
-----END CERTIFICATE-----
```

ลำดับการทำงาน

1.เปิดไฟล์ของ Certificate Authority (CA) ที่เก็บในไฟล์ c1.pem และอ่านข้อมูล Certificate Authority ด้วยฟังก์ชัน PEM_read_X509() เพื่อดึงข้อมูลสาธารณะของ CA ออกมาจากไฟล์ PEM

2.หลังจากอ่านข้อมูล CA แล้ว ใช้ฟังก์ชัน X509_get_pubkey() เพื่อดึงคีย์สาธารณะของ CA ออกมาจาก Certificate Authority (CA)

3.เปิดไฟล์ของเซิร์ฟเวอร์ที่ต้องการตรวจสอบลายเซ็นในไฟล์ c0.pem และอ่านข้อมูล Certificate ด้วยฟังก์ชัน PEM_read_X509() เพื่อดึงข้อมูล Certificate ของเซิร์ฟเวอร์ออกมาจากไฟล์ PEM

4.ใช้ฟังก์ชัน X509_verify() เพื่อทำการตรวจสอบลายเซ็นของ Certificate โดยใช้คีย์สาธารณะของ CA

5.ถ้าตรวจสอบลายเซ็นผ่าน โปรแกรมจะแสดงข้อความ "Signature verification succeeded."

6.สุดท้ายจะคืนค่าทั้งหมด

6.2 ผลลัพธ์การรันชุดคำสั่ง

6.2.1 เมื่อ ตรวจสอบลายเซ็นเซิร์ฟเวอร์ในไฟล์ c0.pem ว่าถูกลงชื่อด้วยคีย์สาธารณะของ Certificate Authority (CA) ภายในไฟล์ c1.pem ถูกต้อง

```
[02/25/24]seed@VM:~/task6_R06$ ./CS324_Security_Lab01-Cryptography-RSA_R06_task-6
Signature verification succeeded.
```

6.2.2 ตัวอย่างเมื่อเกิด Error ภายในตัวไฟล์

```
[02/25/24]seed@VM:~/task6_R06$ ./CS324_Security_Lab01-Cryptography-RSA_R06_task-6
Error: Failed to read CA certificate.
```

6.3 อภิปรายผลลัพธ์

ผลลัพธ์ที่ได้จากการรันคือ Signature verification succeeded. ซึ่งเป็นไปตามกระบวนการที่ให้ไว้ในชุดคำสั่ง ซึ่งแสดงว่า กระบวนการตรวจสอบลายเซ็นได้ผลลัพธ์ว่าถูกต้อง

เนื่องจาก

1.มีการใช้ Public Key ที่ถูกต้อง กระบวนการตรวจสอบลายเซ็นจำเป็นต้องใช้ Public Key ของ Certificate Authority (CA) เพื่อทำการตรวจสอบลายเซ็นของ Certificate ของเซิร์ฟเวอร์

2.การลงชื่อของ Certificate Authority การตรวจสอบลายเซ็นเป็นไปได้เนื่องจาก Certificate Authority (CA) ได้ลงชื่อใบรับรองดิจิทัลของเซิร์ฟเวอร์อย่างถูกต้อง และ Public Key ของ CA นั้นเชื่อถือได้

3.ข้อมูลใน Certificate ถูกต้อง