Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

Лабораторная работа №6

По дисциплине «КМЗИ»

Тема: “Сертификаты X.509 и инфраструктура открытых ключей”

Выполнил:

Студент 3 курса

Группы ИИ-21

Пучинский А. А.

Проверила:

Хацкевич А.С.

Брест 2023

Цель:Создать программу, которая создание сертификатов X.509

Код программы:

chcp 65001

# Генерируем корневую ключевую пару алгоритмом ED25519

openssl genpkey -algorithm ED25519 -out root\_keypair.pem -quiet

# Выводим текстовую информацию о корневом ключевом сертификате

openssl pkey -in root\_keypair.pem -noout -text

# Создаем запрос на подпись (CSR) для корневого сертификата

openssl req -new -subj "/CN=Root CA" -addext "basicConstraints=critical,CA:TRUE" -key root\_keypair.pem -out root\_csr.pem

# Выводим текстовую информацию о CSR для корневого сертификата

openssl req -in root\_csr.pem -noout -text

# Подписываем корневой сертификат с использованием его собственного ключа

openssl x509 -req -in root\_csr.pem -copy\_extensions copyall -signkey root\_keypair.pem -days 7 -out root\_cert.pem

# Выводим текстовую информацию о корневом сертификате

openssl x509 -in root\_cert.pem -noout -text -quiet

# Генерируем промежуточную ключевую пару алгоритмом ED25519 и сохраняем в файл

openssl genpkey -algorithm ED25519 -out intermediate\_keypair.pem -quiet

# Создаем CSR для промежуточного сертификата

openssl req -new -subj "/CN=Intermediate CA" -addext "basicConstraints=critical,CA:TRUE" -key intermediate\_keypair.pem -out intermediate\_csr.pem

# Подписываем промежуточный сертификат с использованием корневого сертификата и ключа

openssl x509 -req -in intermediate\_csr.pem -copy\_extensions copyall -CA root\_cert.pem -CAkey root\_keypair.pem -days 7 -out intermediate\_cert.pem

# Выводим текстовую информацию о промежуточном сертификате

openssl x509 -in intermediate\_cert.pem -noout -text -quiet

# Генерируем ключевуй пару для конечного (листового) узла алгоритмом ED25519 и сохраняем в файл

openssl genpkey -algorithm ED25519 -out leaf\_keypair.pem -quiet

# Создаем CSR для конечного сертификата

openssl req -new -subj "/CN=Leaf" -addext "basicConstraints=critical,CA:FALSE" -key leaf\_keypair.pem -out leaf\_csr.pem

# Подписываем конечный сертификат с использованием промежуточного сертификата и ключа

openssl x509 -req -in leaf\_csr.pem -copy\_extensions copyall -CA intermediate\_cert.pem -CAkey intermediate\_keypair.pem -days 7 -out leaf\_cert.pem

# Выводим текстовую информацию о конечном сертификате

openssl x509 -in leaf\_cert.pem -noout -text -quiet

# Проверка цепочки сертификации конечного сертификата с выводом подробной информации

openssl verify -verbose -show\_chain -trusted root\_cert.pem -untrusted intermediate\_cert.pem leaf\_cert.pem

Вывод: изучил создание сертификатов X.509 и инфраструктуру открытых ключей.