|  |  |  |  |
| --- | --- | --- | --- |
| POLITECHNIKA LUBELSKA  Wydział Elektrotechniki i Informatyki  Informatyka | **Bezpieczeństwo Informacji**  **Prowadzący: dr Waldemar Suszyński** | | |
| Nazwisko i Imię | Semestr  IV | Rok akademicki  2023/2024 | Grupa:  IIST 4.5 |
| 1. |
| Data wykonania ćwiczenia: | GL 9 |
| Temat ćwiczenia:  INFRASTRUKTURA KLUCZA PUBLICZNEGO, PODPIS CYFROWY, SSL/TLS | | Data oddania sprawozdania: | OCENA: |

1. **Utworzenie głównego urzędu certyfikacji CA.**



Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Czcionka

Opis wygenerowany automatycznie

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

1. **Utworzenie certyfikatu dla organizacji.**

**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, komputer

Opis wygenerowany automatycznie**

Przeglądarka zignorowała certyfikat. Konsola pokazała takie komunikatyObraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

Próba utworzenia kolejnego certyfikatu w ten sam sposób skutkowała tak samo.

Zmiana bitu i przywrócenie go do stanu początkowego nic nie zmieniło. FireFox flagował stronę jako niebezpieczną i po wyświetleniu strony pokazywał pustą przestrzeń.

1. **Zastosowanie infrastruktury klucza publicznego do stron WWW.**

Nie, nie jest. Jednak przyjęło się by korzystać z konkretnych długości kluczy przy konkretnych funkcjach.

1. **Tworzenie infrastruktury PKI z wykorzystaniem algorytmu RSA (bounus).**

**-**

1. **Porównanie wydajności algorytmu niesymetrycznego do symetrycznego.**

**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznie**

**openssl genrsa -out private.key 1024 .**

**openssl rsa -in private.key -pubout -out public1024.key .**

**openssl rsautl -in 10.txt -out 10\_1024.txt -pubin -inkey public1024.key -encrypt .**

**openssl rsautl -in 10\_1024.txt -out 10\_1024d.txt -inkey private.key -decrypt .**

**openssl enc -aes-128-ofb -e -in 10.txt -out 10aes.txt -K 012345678abcdef012345678abcdefff -iv 012345678abcdef012345678abcdefff .**

**openssl enc -aes-128-ofb -d -in 10aes.txt -out 10aes\_d.txt -K 012345678abcdef012345678abcdefff -iv 012345678abcdef012345678abcdefff .**

1. **Utworzenie podpisu cyfrowego.**

**openssl genrsa -aes256 -out private.key 1024 //klucz - haslo**

**openssl rsa -in private.key -out public.pem -outform PEM -pubout .**

**openssl dgst -sha256 -sign private.key -out podpis.sha256 podpis.txt .**

**openssl dgst -sha256 -verify public.pem -signature podpis.sha256 podpis.txt**

**Verified OK**

**//Modyfikacja tekstu**

**openssl dgst -sha256 -verify public.pem -signature podpis.sha256 podpis.txt**

**Verification Failure**

**//Reedycja tekstu na pierwotny**

**openssl dgst -sha256 -verify public.pem -signature podpis.sha256 podpis.txt**

**Verified OK**