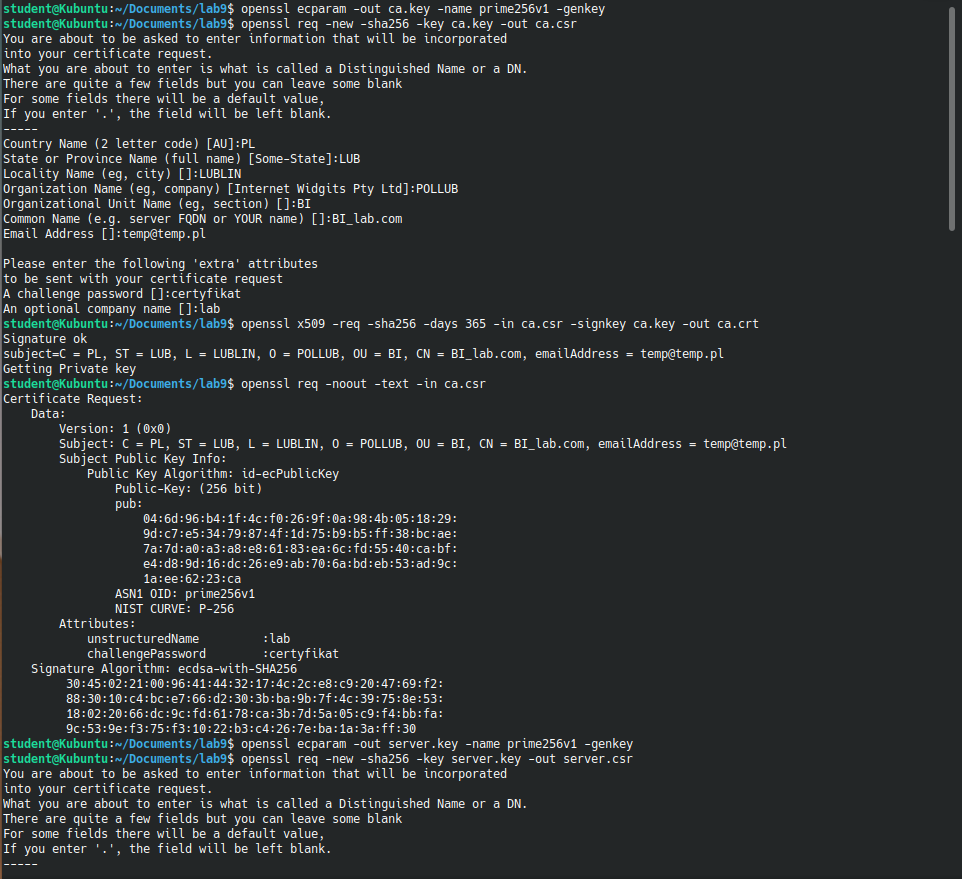
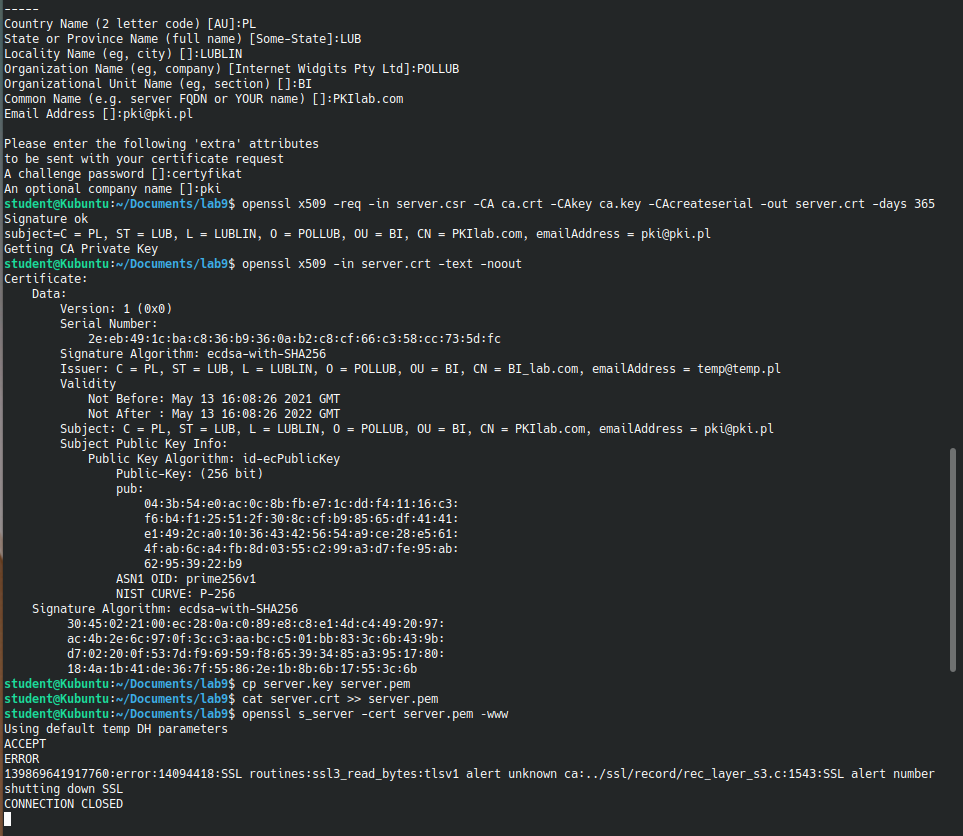
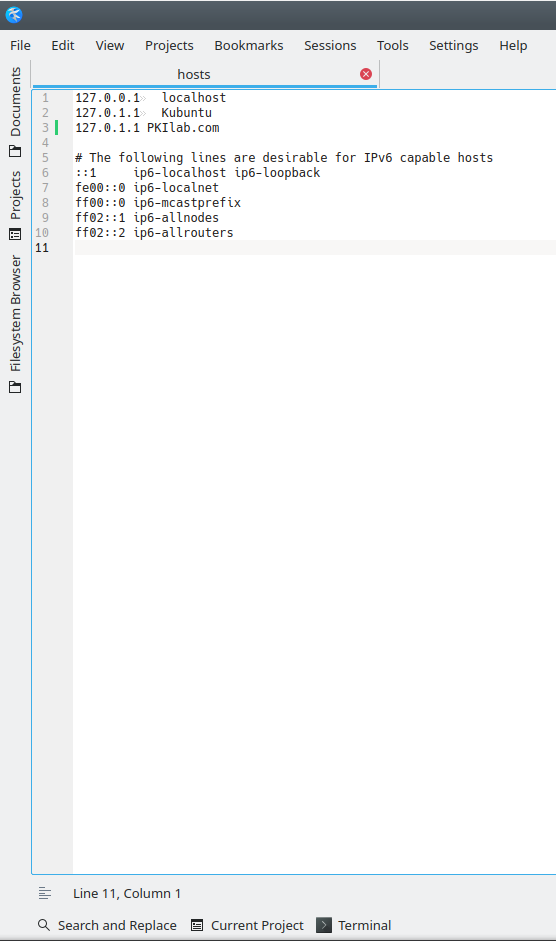
Sprawozdanie

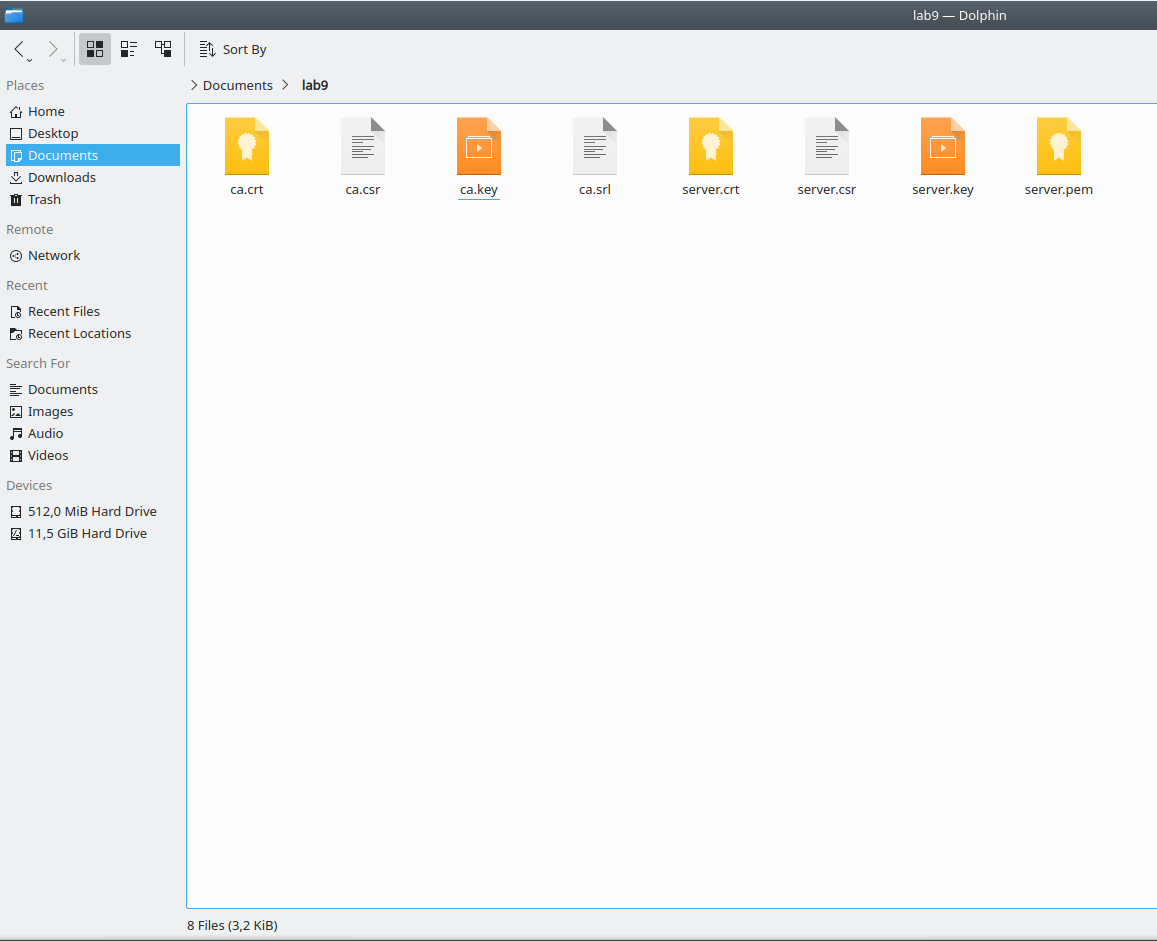
LABORATORIUM 6. INFRASTRUKTURA KLUCZA PUBLICZNEGO, PODPIS CYFROWY, SSL/TLS

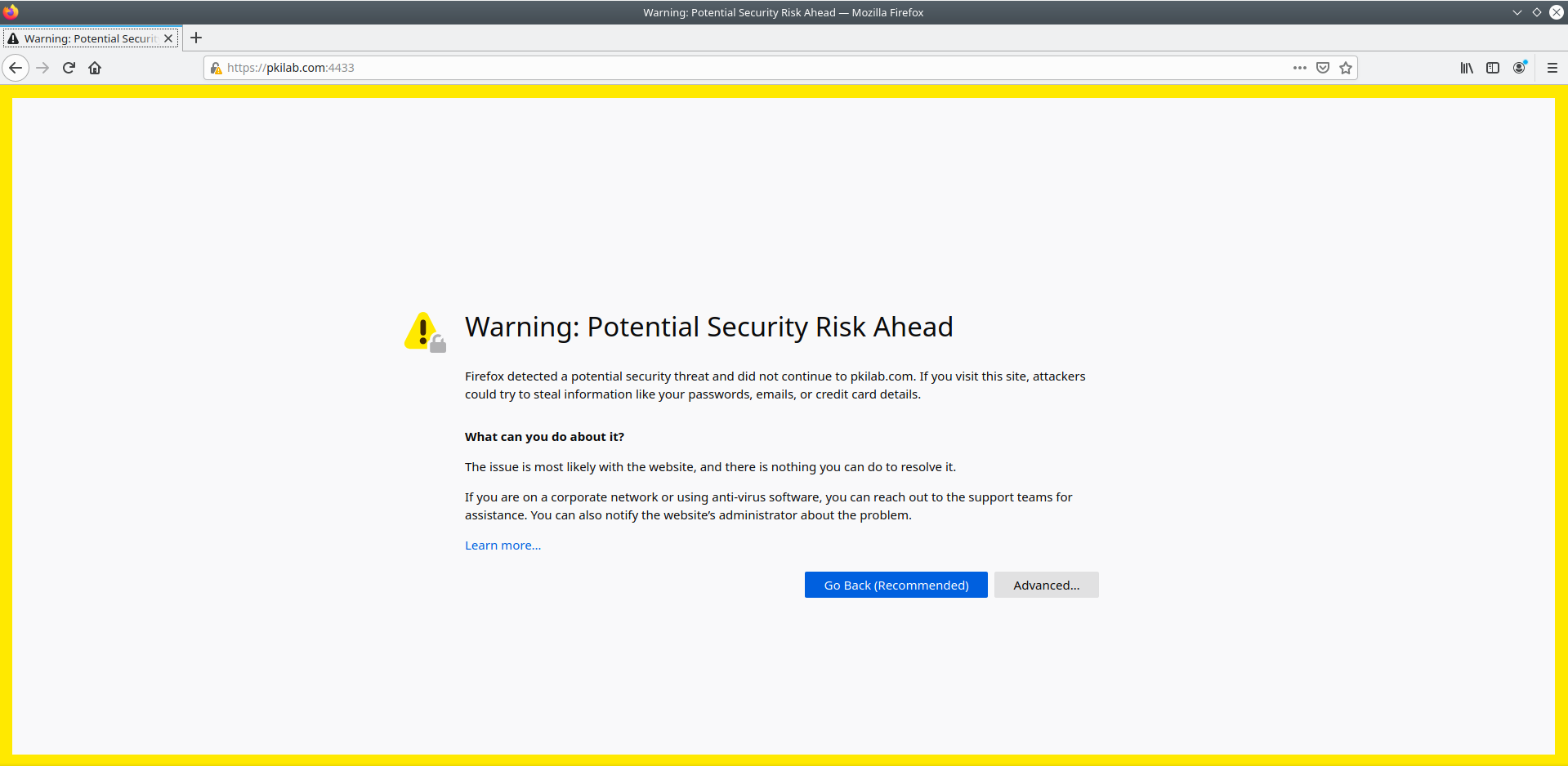
# Zadanie 6.3. Zastosowanie infrastruktury klucza publicznego do stron WWW







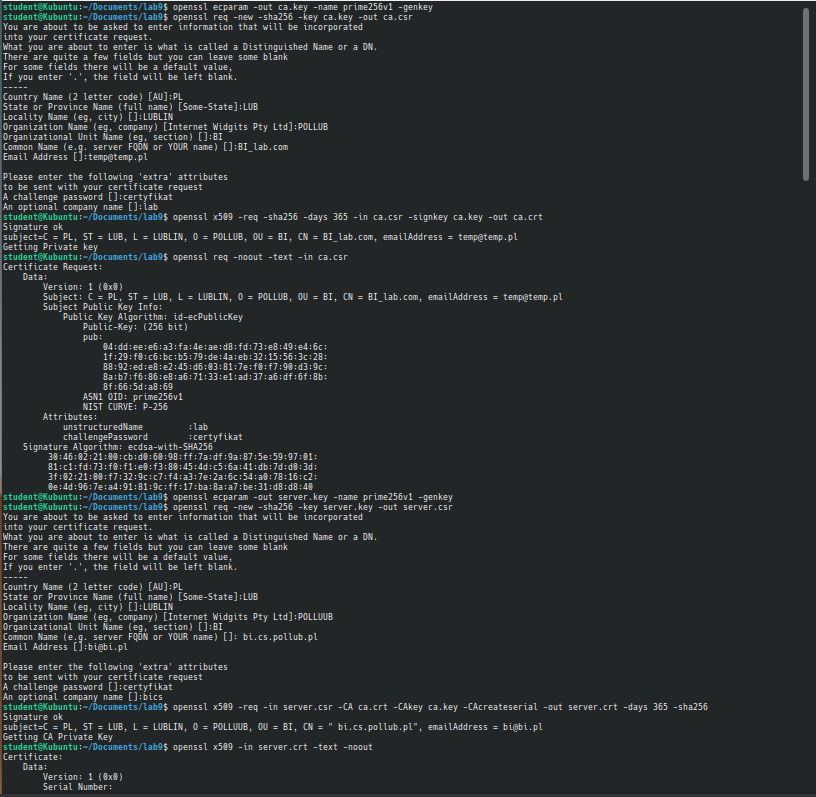


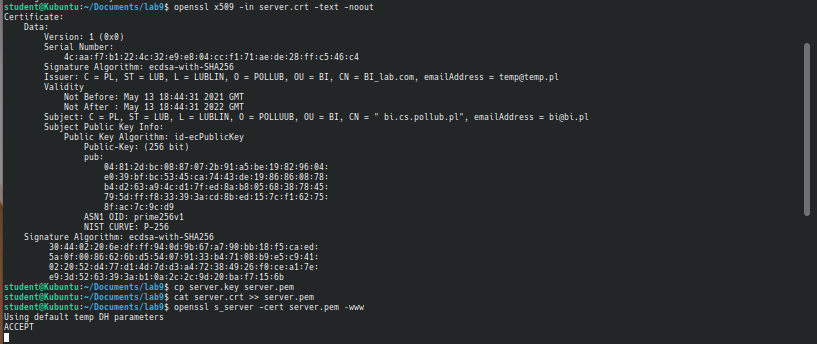


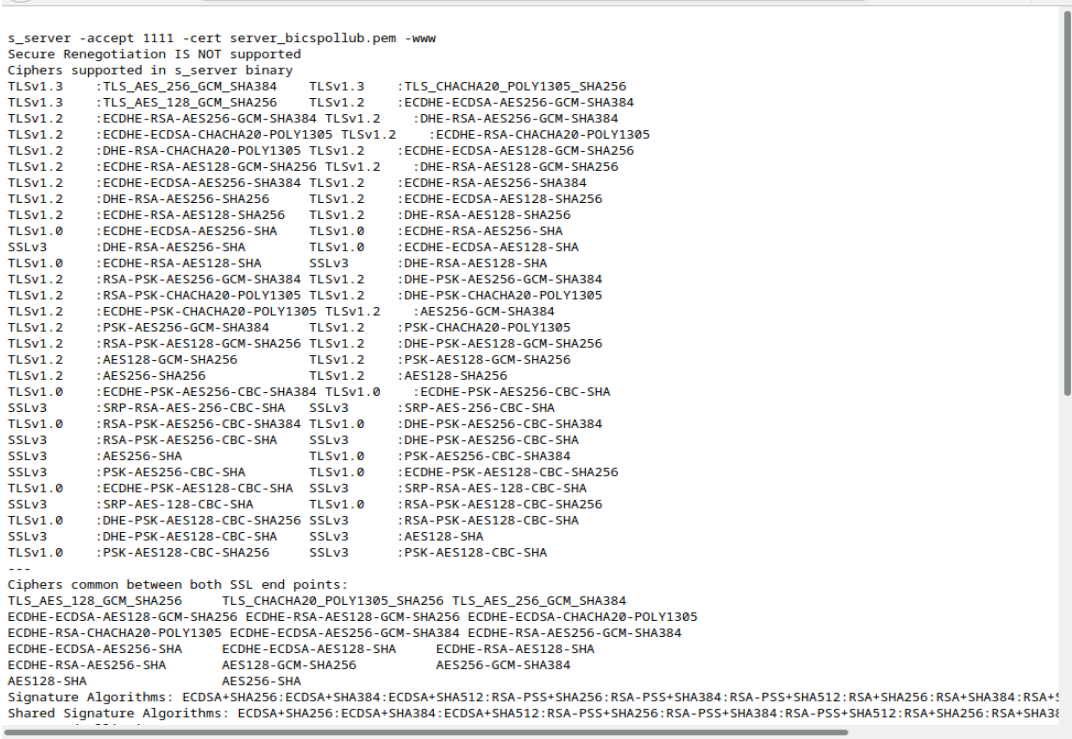
## P.6.1. Opisz i wyjaśnij swoje obserwacje. Co się stało i dlaczego?

Utworzyliśmy certyfikat i uruchomiliśmy serwer korzystający z tego certyfikatu. Strona w przeglądarce pokazuje się nadal jako niebezpieczna, ponieważ urząd certyfikacji na podstawie jakiego utworzyliśmy certyfikat nie jest rozpoznawany przez przeglądarkę. Po dodaniu urzędu w liście w przeglądarce strona zaczyna być wyświetlana jako bezpieczna

## P.6.2. Wygeneruj i certyfikuj certyfikat dla serwera bi.cs.pollub.pl. W sprawozdaniu zamieść użyte polecenia oraz zrzut ekranu prezentujący odpowiedź uruchomionego serwera w przeglądarce.







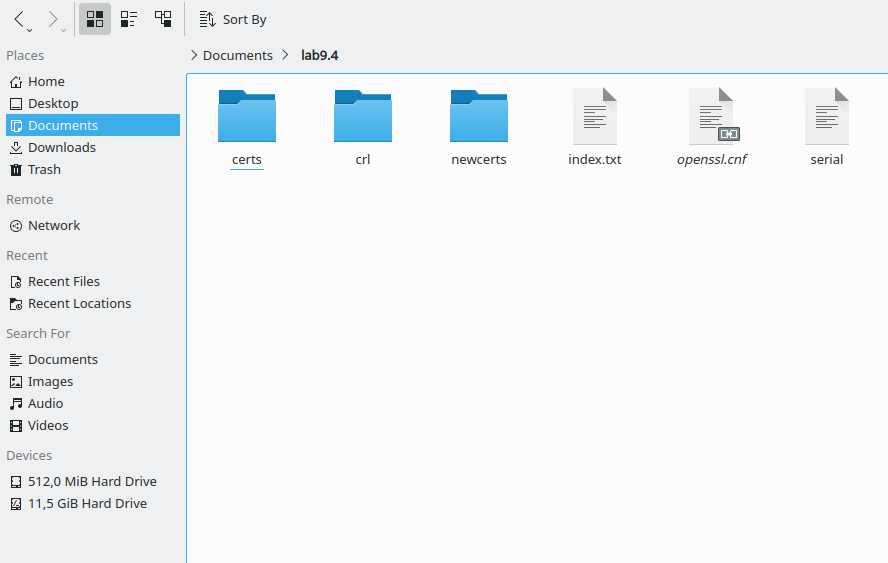
## P.6.3. Określ, z jakich elementów składa sie plik certyfikatu (\*.pem) i jak wpływa modyfikacja bitów w poszczególnych elementach tegoż pliku na działanie serwera. Zmodyfikuj pojedyńczy bit w pliku server.pem przy użyciu edytora Hex. Uruchom ponownie serwer i przeładuj zawartość udostępnianej przez niego strony. Wyniki zamieść w tabeli zawierającej trzy kolumny: element pliku pem, opis elementu, opis wpływu modyfikacji bitu w tym elemencie na działanie serwera.

|  |  |  |
| --- | --- | --- |
| **Parametry** | **Klucz Prywatny** | **Certyfikat** |
| -----BEGIN EC PARAMETERS-----  BggqhkjOPQMBBw==  -----END EC PARAMETERS----- | -----BEGIN EC PRIVATE KEY-----  MHcCAQEEINUY4fF1VZBtVuaaB8iZOd9Xp4jbEGJwmGfifn5q9H7ioAoGCCqGSM49  AwEHoUQDQgAEO1TgrAyL++cc3fQRFsP2tPElUS8wjM+5hWXfQUHhSSygEDZDQlZU  qc4o5WFPq2yk+40DVcKZo9f+latilTkiuQ==  -----END EC PRIVATE KEY----- | -----BEGIN CERTIFICATE-----  MIIB8TCCAZcCFC7rSRy6yDa5NgqyyM9mw1jMc138MAoGCCqGSM49BAMCMHwxCzAJ  BgNVBAYTAlBMMQwwCgYDVQQIDANMVUIxDzANBgNVBAcMBkxVQkxJTjEPMA0GA1UE  CgwGUE9MTFVCMQswCQYDVQQLDAJCSTETMBEGA1UEAwwKQklfbGFiLmNvbTEbMBkG  CSqGSIb3DQEJARYMdGVtcEB0ZW1wLnBsMB4XDTIxMDUxMzE2MDgyNloXDTIyMDUx  MzE2MDgyNlowejELMAkGA1UEBhMCUEwxDDAKBgNVBAgMA0xVQjEPMA0GA1UEBwwG  TFVCTElOMQ8wDQYDVQQKDAZQT0xMVUIxCzAJBgNVBAsMAkJJMRMwEQYDVQQDDApQ  S0lsYWIuY29tMRkwFwYJKoZIhvcNAQkBFgpwa2lAcGtpLnBsMFkwEwYHKoZIzj0C  AQYIKoZIzj0DAQcDQgAEO1TgrAyL++cc3fQRFsP2tPElUS8wjM+5hWXfQUHhSSyg  EDZDQlZUqc4o5WFPq2yk+40DVcKZo9f+latilTkiuTAKBggqhkjOPQQDAgNIADBF  AiEA7CgKwInoyOFNxEkgl6xLLmyXDzzDqrzFAbuDPGtDm9cCIA9TfflpWfhlOTSF  o5UXgBhKG0HeNn9Vhi4bi2sXVTxr  -----END CERTIFICATE----- |
| Po zmianie bitu i uruchomieniu serwera pokazuje się nam komunikat że nie mamy dodanego certyfikatu | Nie możemy włączyć serwera | Nie możemy włączyć serwera |

## P.6.4. Przywróć poprawną postać certyfikatu serwera, uruchom ponownie serwer, a następnie wyświetl stronę WWW korzystając z adresu https://localhost:4433. Jaki jest efekt? Wyjaśnij, co sie stało.

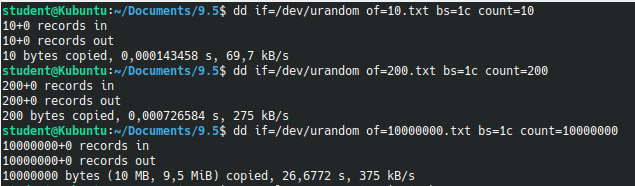
Pokazuje, że brakuje nam certyfikatu, w certyfikacie mamy zapisany dokładny adres strony wiec jeśli wchodzimy na nią przez localhost przez dany port wychodzi nam brak komunikatu.

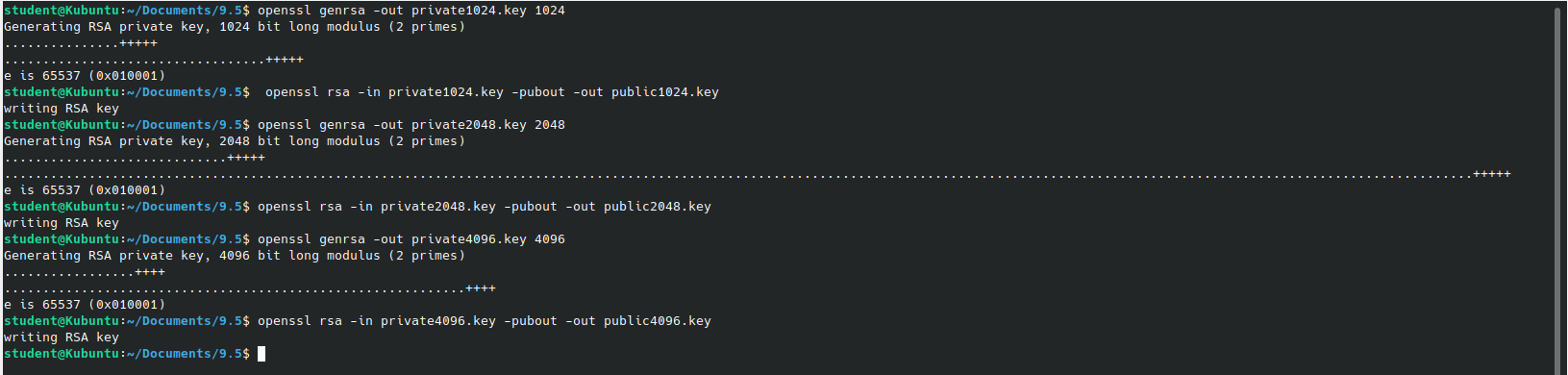
# Zadanie 6.4. Tworzenie infrastruktury PKI z wykorzystaniem algorytmu RSA



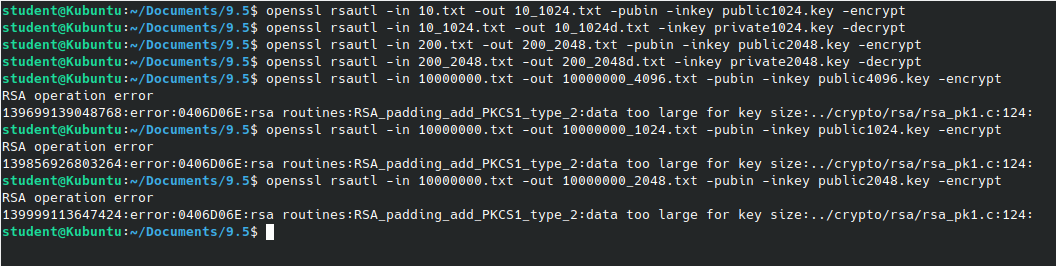
ECC używa znacznie mniejszych wielkości kluczu względem RSA. Szyfrowanie ECC jest szybsze i zużywa mniej mocy obliczeniowej.

# Zadanie 6.5. Porównanie wydajności algorytmu niesymetrycznego do symetrycznego

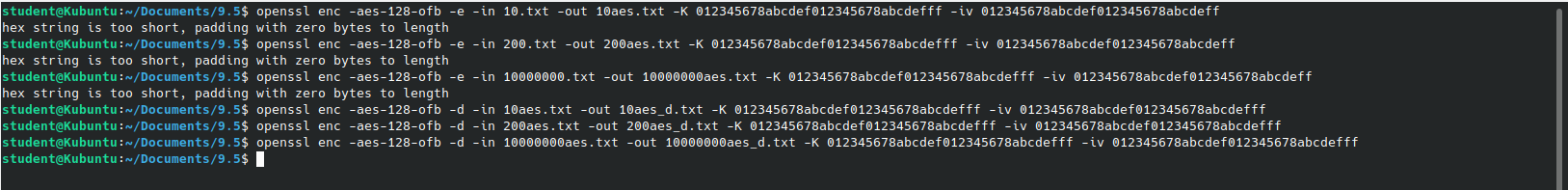


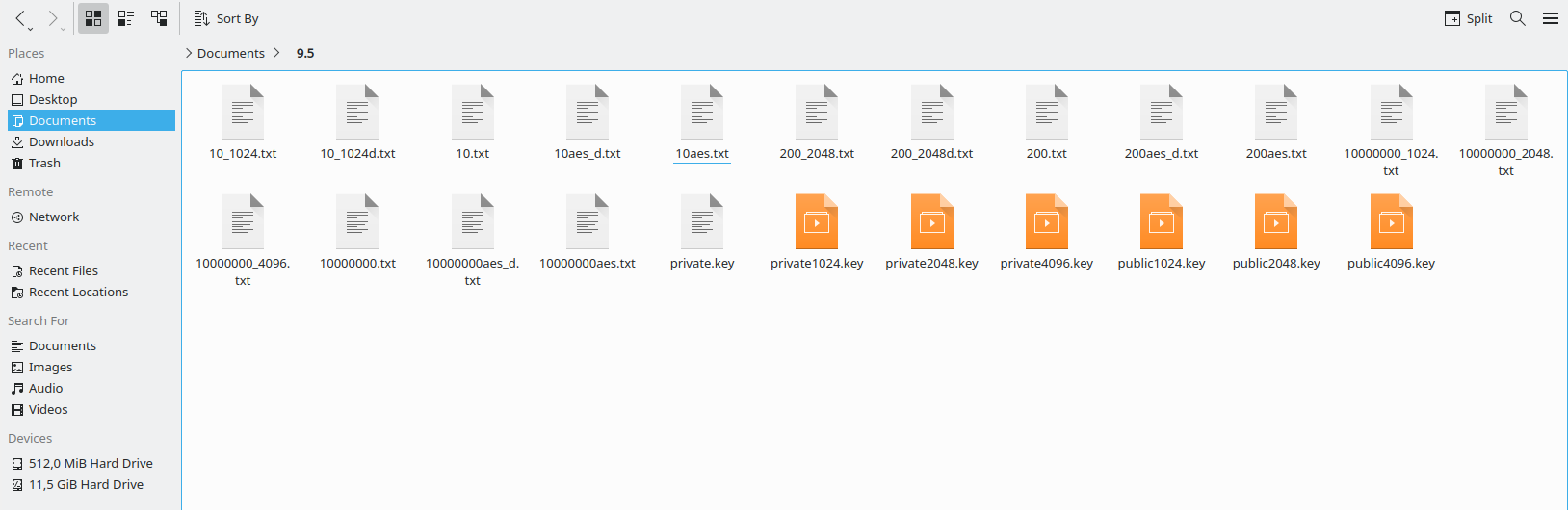


## RSA:



## AES:

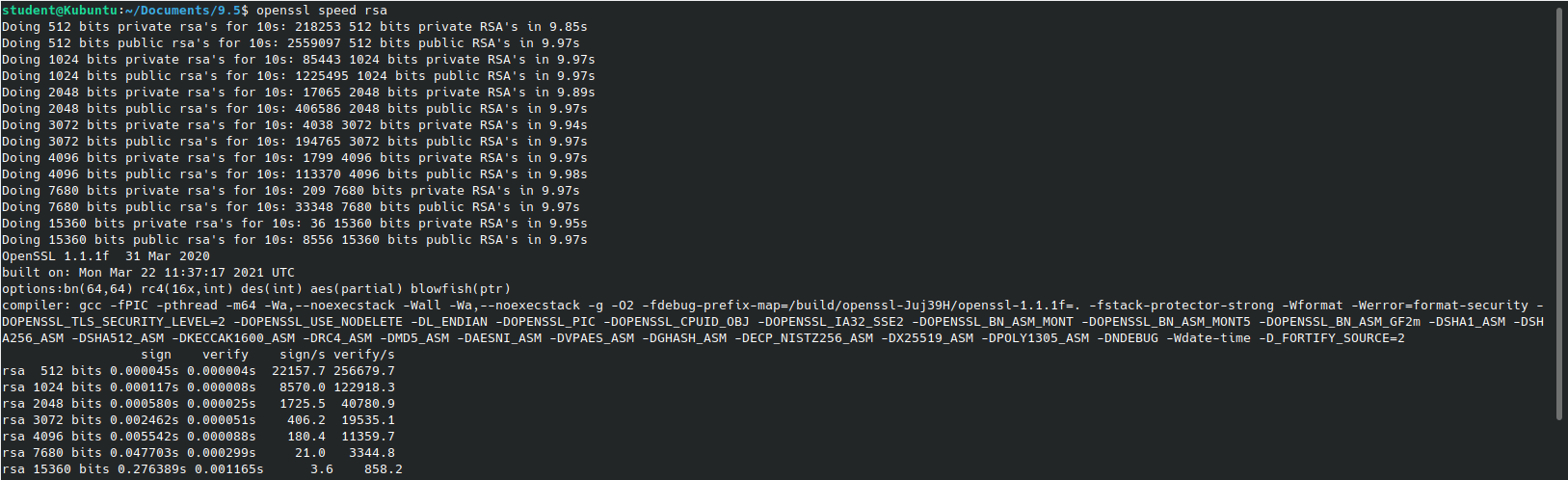




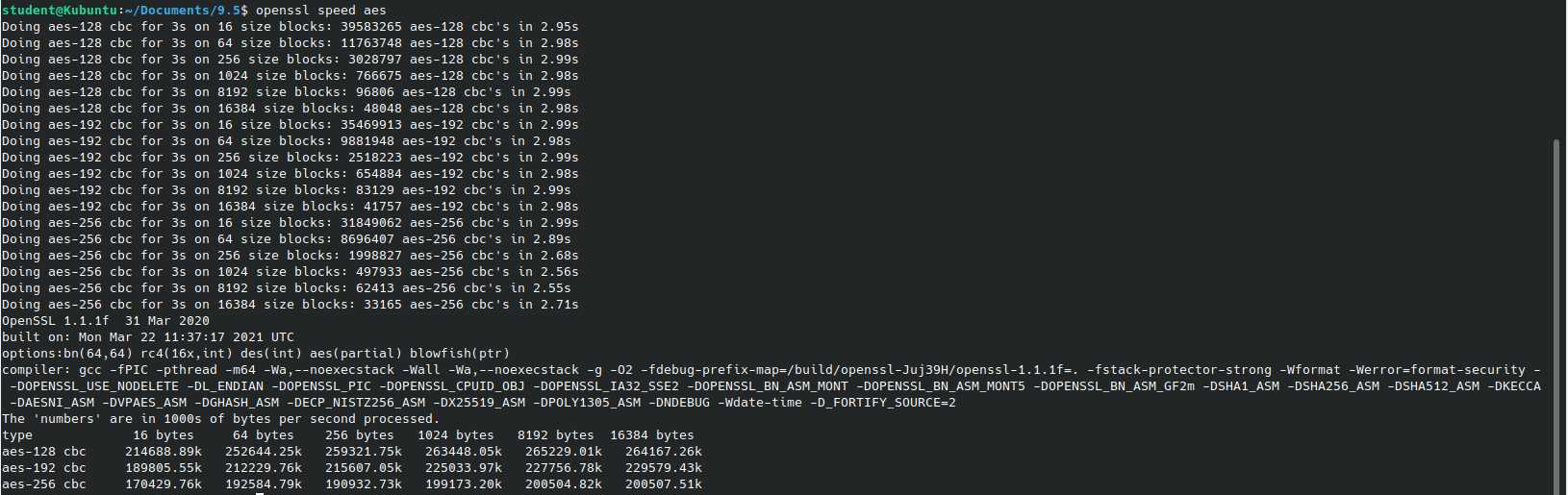
## P.6.5. W celu określenia czasu szyfrowania i deszyfrowania skorzystaj z systemowego polecenia "time". Jako wynik zapisz sumy czasów user+sys. W celu zminimalizowania błędów napisz skrypt realizujący 100 powtórzeń dla każdej operacji mierząc w ten sposób czas jej wielokrotnego wykonania, następnie podaj wyniki średnie dla każdej operacji. Przedstaw je w postaci umożliwiającej porównanie wydajności np. obliczając ilość danych przetwarzanych w ciągu jednej sekundy. Opracuj zestawienie uzyskanych wyników w formie tabeli. Sporządź wykresy dla uzyskanych wyników.

## P.6.6. Przedstaw wyniki analogicznie do tych z P. 6.5. Porównaj je ze sobą i skomentuj.

## RSA:



## AES:



Szyfrowanie AES jest o wiele szybsze od RSA.