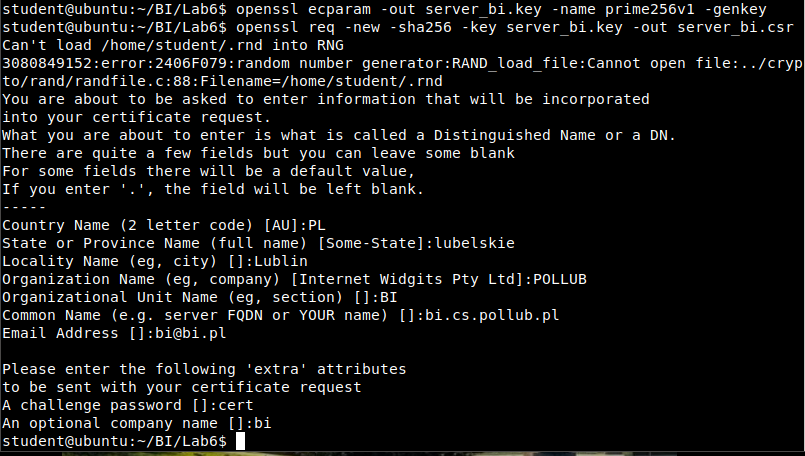
**Jakub Dudek**

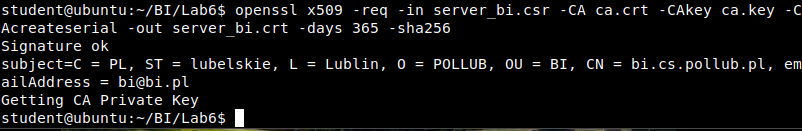
**Sprawozdanie Laboratorium 6**

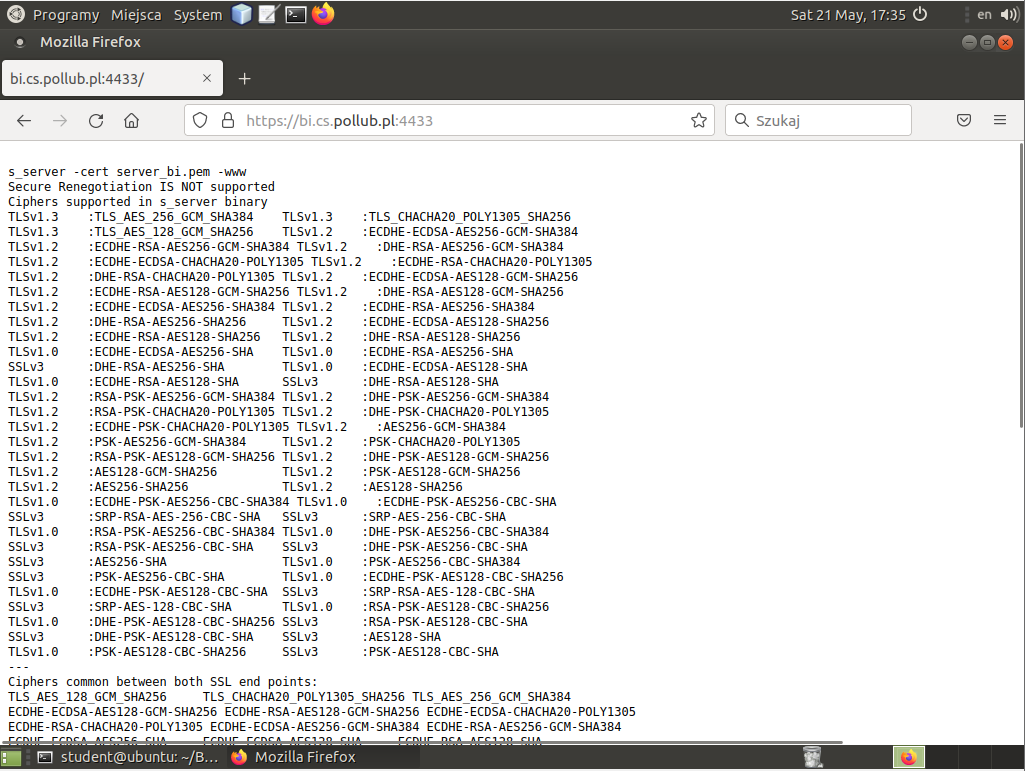
**P.6.1. Opisz i wyjaśnij swoje obserwacje. Co się stało i dlaczego?**

Certyfikat został wystawiony w taki sposób jaki jest przedstawiony w instrukcji. Jednak on nie zadziała dopóki nasza przeglądarka lub system operacyjny nie będzie znał certyfikatu urzędu certyfikacji. Zaczyna działać dopiero, gdy dodamy certyfikat do repozytorium certyfikatów znanych przez przeglądarkę.

**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.**





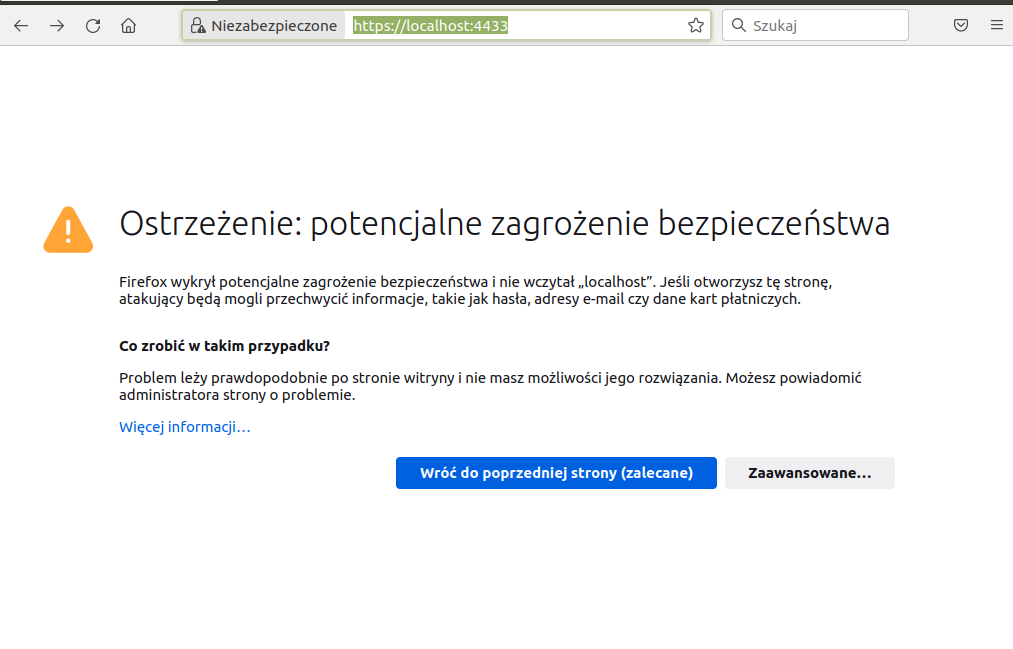


**P.6.3. Określ, z jakich elementów składa sie plik certyfikatu (\*.pem) i jak wpływa  
modyfikacja bitów w poszczególnych elementach tegoż pliku na działanie serwera. Zmodyfikuj pojedyńczy bit w pliku server.pem przy użyciu edytora Hex. Uruchom ponownie serwer i przeładuj zawartość udostępnianej przez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

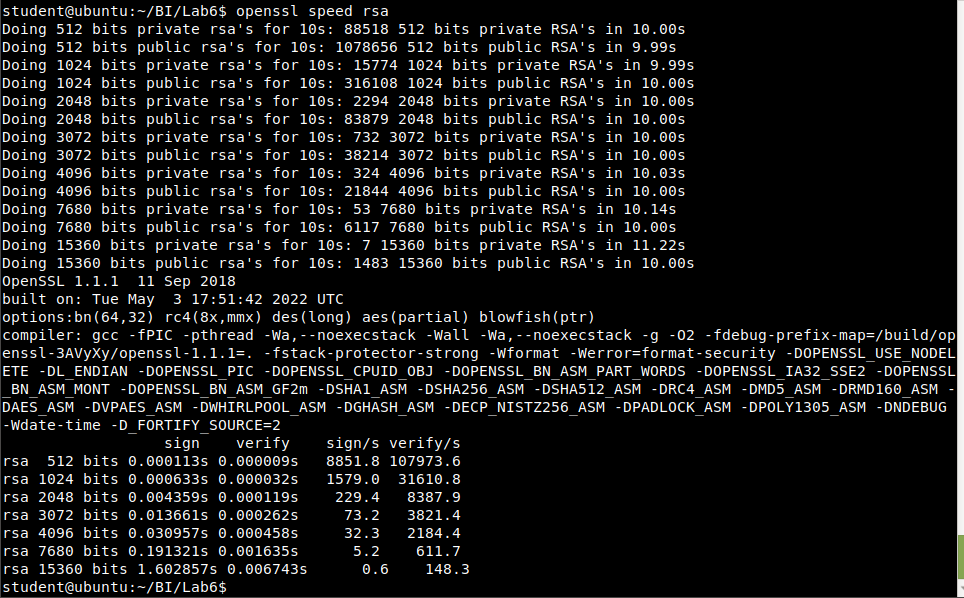
|  |  |  |
| --- | --- | --- |
| Element pliku pem | Opis elementu | Opis wpływu modyfikacji bitu |
| Parametry algorytmu EC | Określa z jakimi parametrami został wygenerowany |  |
| Klucz prywatny | Klucz prywatny serwera | Uszkodzenie klucza prywatnego |
| Certyfikat | Certyfikat serwera | Uszkodzenie certyfikatu |

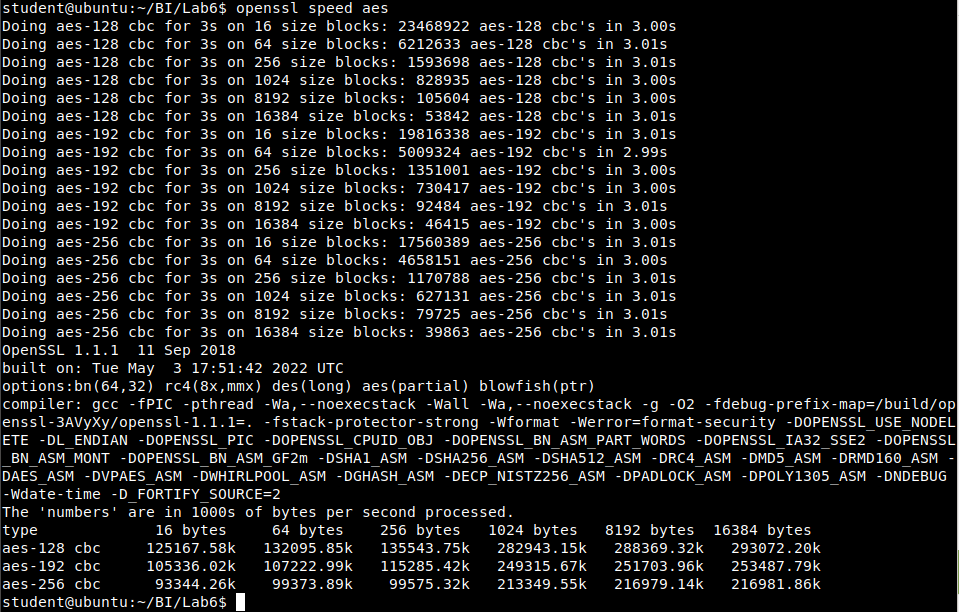
**P.6.4. Przywróć poprawną postać certyfikatu serwera, uruchom ponownie serwer, a następnie wyświetl stronę WWW korzystając z adresu https://localhost:4433. Jaki jest efekt? Wyjaśnij, co sie stało.**

Pojawia się ostrzeżenie o zagrożeniu bezpieczeństwa. Domena, która jest w certyfikacie nie zgadza się, więc pokazuje się ostrzeżenie.



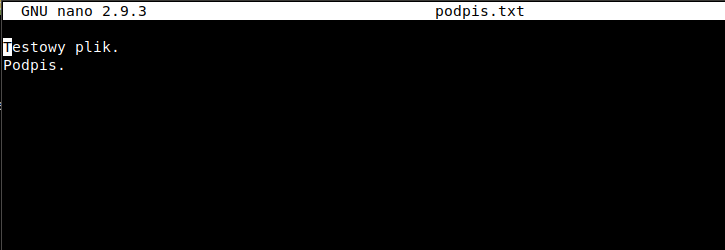
**P.6.6. Przedstaw wyniki analogicznie do tych z P. 6.5. Porównaj je ze sobą i skomentuj.**

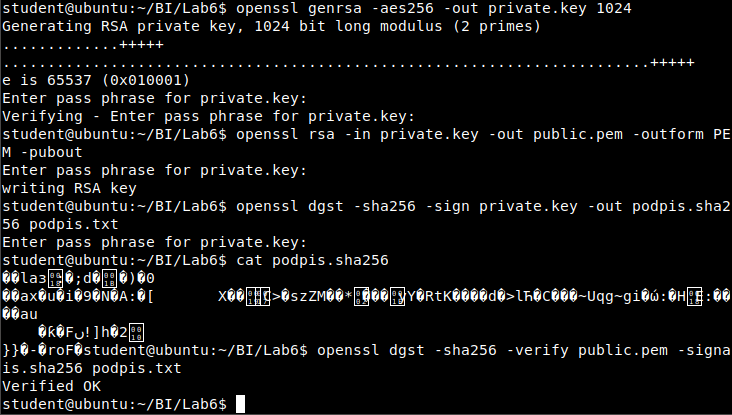
****

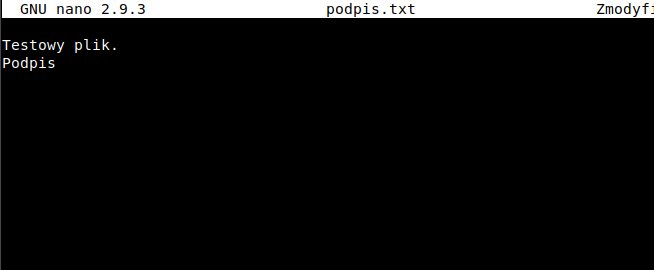
****

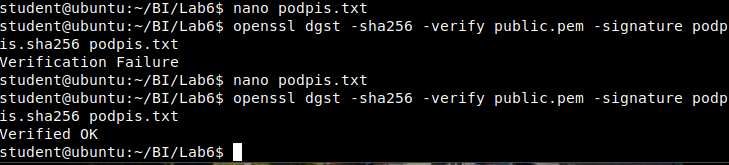
AES jest szybszy od RSA

**P.6.7. Udokumentuj poprawność przeprowadzonego ćwiczenia i opisz uzyskane wyniki. Omów jak wpływa modyfikacja wiadomości na weryfikację podpisu cyfrowego.**

****

****

****

****

Jak zmienimy zawartość pliku weryfikacja nie powiedzie się. Jednak gdy przywrócimy zawartość znowu będzie możliwa.