4.16 Wygeneruj swoją parę kluczy. Wymień się kluczami publicznymi z wybraną osobą na sali (możesz to zrobić za pomocą e-maila, serwera kluczy **keyserver.ubuntu.com**, …). Zaszyfruj kluczem publicznym osoby, z którą się wymieniłeś kluczami dowolny plik. Wyślij tak zaszyfrowany plik do tej osoby (np. mailem). Odszyfruj plik i porównaj zawartość.

4.17 Wygeneruj swoją parę kluczy. Wymień się kluczami publicznymi z wybraną osobą na sali (możesz to zrobić za pomocą e-maila, serwera kluczy **keyserver.ubuntu.com**, …). Podpisz dowolny plik swoim kluczem prywatnym, a następnie wyślij podpisany plik oraz początkowy plik do osoby, z którą się wymieniłeś kluczami. Zweryfikuj podpis.

4.18 Wygeneruj swoją parę kluczy. Wymień się kluczami publicznymi z wybraną osobą na sali (możesz to zrobić za pomocą e-maila, serwera kluczy **keyserver.ubuntu.com**, …). Podpisz i zaszyfruj dowolny plik, wyślij go drugiej osobie, która powinna go zweryfikować i odszyfrować.

Linki

https://www.gnupg.org/gph/en/manual/x135.html
https://stackoverflow.com/questions/57223719/gpg-sign-clear-sign-detach-sign