Kodowanie i bezpieczeństwo informacji

Laboratorium - lista nr 1 na 12-24 lutego 2012

Zadanie 1 Wygeneruj klucze PGP (GPG) do podpisywania i szyfrowania wiadomości. Wyeksportuj certyfikat na: keys.gnupg.net.

Zadanie 2 PGP wykorzystuje model "web of trust" umożliwiając użytkownikom podpisywanie kluczy publicznych innych użytkowników. Podpisz klucze co najmniej dwóm osobom uczęszczającym na kurs. Zdobądź podpis od co najmniej jednej osoby pod Twoim kluczem publicznym.

Zadanie 3 Jakie są zalety wzajemnego podpisywania kluczy w PGP? Na co należy zwrócić uwagę przy podpisywaniu czyichś kluczy? Czym model PGP różni się od hierarchii certyfikatów X.509?

Zadanie 4 Odnajdź klucze następujących osób: prezydent RP, USA, premier RP, minister cyfryzacji, James Bond, Hans Kloss. Wyjaśnij pokrótce jakie są zalety i wady serwerów kluczy PGP.

Zadanie 5 Prześlij podpisaną wiadomość na adres imie.nazwiskoProwadzacego@pwr.wroc.pl tak, aby tylko on mógł odczytać wiadomość od Ciebie. W tytule wiadomości umieść ciąg: [kbi2012] L1 Z3. W treści wiadomości umieść identyfikatory kluczy z zadania 2 oraz odpowiedzi na pytania z zadania 3 i 4.

Pamiętaj, aby cytować źródła na które się powołujesz.