Zadanie_1

Publiczny system kryptograficzny

1. Omów działanie systemu kryptografii wykorzystującego klucze prywatne i publiczne. Wyjaśnij zasadę i sposób szyfrowania „asymetrycznego”, w tym elementy matematyczne algorytmu.

2. Zapoznaj się z działaniem programu gnuPG (http://www.gnupg.org).

3. Wykonaj ćwiczenie z wykorzystaniem gnuPG:

   3.1. Wygeneruj parę kluczy, wraz z pomiarem czasu generowania (sposób pomiaru dowolny). Klucz 1024 bitowy zabezpieczony hasłem.

   3.2. Prześlij klucz publiczny pocztą elektroniczna drugiemu użytkownikowi.

   3.3. Otrzymany pocztą elektroniczną od drugiego użytkownika jego klucz publiczny dodaj do swojego zbioru kluczy publicznych.

   3.4. Dodaj identyfikator do swojego klucza, aby posługiwać się identyfikatorem tak samo jak pełna nazwa klucza.

   3.5. Podpisz swoim kluczem prywatnym otrzymany klucz.

   3.6. Przejrzyj zawartość swojego zbioru kluczy publicznych, aby upewnić się, że poprzednie polecenia zostały wykonane poprawnie.

   3.7. Zaszyfruj dowolny (np. graficzny) plik binarny **plik1** otrzymanym kluczem publicznym i wyślij oba pocztą elektroniczną. Usuń zaszyfrowany i oryginalny plik.

   3.8. Rozszyfruj swoim kluczem prywatnym otrzymane poczta pliki, porównaj plik z oryginałem, powinny być identyczne.

   3.9. Podpisz plik tekstowy **plik2** swoim kluczem prywatnym, tak aby jego zawartość nie została zaszyfrowana i pozostała czytelna, sprawdź poprawność podpisu, a następnie wyślij plik drugiemu użytkownikowi. Podpis umieść w sprawozdaniu.

   3.10. Sprawdź poprawność podpisu pod otrzymanym od drugiego użytkownika plikiem.

   3.11. Unieważnij swój klucz.

   3.12. Wyślij certyfikat unieważnienia drugiemu użytkownikowi, aby poinformować go, że twój klucz jest nieaktualny.

   3.13. Dołącz do swojego zbioru otrzymany pocztą certyfikat unieważnienia od drugiego użytkownika.

   3.14. Sprawdź jakie zmiany zaszły w zbiorze twoich kluczy.

   3.15. Usuń unieważnione klucze.

   3.16. Poszczególne etapy realizacji ćwiczenia przedstaw w sprawozdaniu.

4. Wyślij list e-mail do prowadzącego według wytycznych:

4.1. Temat listu powinien zawierać informacje: dzień i godzina zajęć oraz nazwisko studenta.

4.2. W treści wysłanego listu muszą znajdować się następujące informacje:

- nazwisko i imię
- numer grupy laboratoryjnej
- numer indeksu
- nazwa przedmiotu
- dzień i godzina zajęć

4.3. List musi być podpisany cyfrowo za pomocą dowolnego certyfikatu np.: POLCERT, CACERT, COMODO lub podobnego. W tym celu należy zarejestrować się w wybranym serwisie, pobrać i zainstalować certyfikat.

List należy wysłać na adres g.bialic@po.opole.pl w dniu poprzedzającym zajęcia. Listy wysłane w innym terminie nie będą brane pod uwagę.