Ćwiczenie 8 Techniki kryptograficzne w programie GPG

W czasie realizacji ćwiczenia należy opracowywać sprawozdanie według załączonego wzoru, zawierające obrazy odpowiednich okien, oraz wnioski i komentarze dotyczące realizowanych zadań.
Sprawozdanie w postaci elektronicznej należy oddać prowadzącemu zajęcia przed opuszczeniem laboratorium.

Przygotowanie do ćwiczenia:

1. Zainstalować program *GPG* poprzez uruchomienie programu *gnupg-w32cli-1.4.3.exe*. Należy wybrać wersję językową zgodną z wersją językową systemu operacyjnego. Zapamiętać ścieżkę do folderu, w którym został zainstalowany program.
2. Zainstalować nakładkę graficzną programu *GPG* poprzez uruchomienie programu *GPGshell.exe*. Program ten należy zainstalować w tym samym folderze, w którym zainstalowano program *GPG*. Należy wybrać wersję językową zgodną z wersją językową systemu operacyjnego.
3. Zainstalować wtyczkę *GPGOE* do programu *GPG*, która umożliwia użytkownikowi integrację programu z klientem poczty elektronicznej. W tym celu należy uruchomić programu *GPGOEInit.exe*.

Zadanie 1 – Zarządzanie kluczami kryptograficznymi

1. Uruchomić program *GPGkeys*. W trakcie uruchamiania należy odpowiedzieć negatywnie na pytanie dotyczące generowania lub importowania kluczy.
2. W menu ***Klucz(e)*** wybrać funkcję ***Nowy***.
3. W otwartym oknie tekstowym programu *GPG* wybrać opcję 1 rodzaju klucza (*DSA and Elgamal*) a następnie zaakceptować proponowaną długość klucza oraz okres ważności klucza. Pozostałe informacje powinny być podane rzetelnie.
4. Po zakończeniu generowania kluczy w oknie programu *GPGkeys* zaprezentowana zostanie informacja o wygenerowanej parze kluczy kryptograficznych.
5. Po wybraniu w menu podręcznym prezentowanej pary kluczy, funkcji ***Eksportuj***, wyeksportować wygenerowany klucz publiczny do pliku. Nie eksportować klucza prywatnego (tajnego). Korzystając z programu ***Notatnik*** (*Notepad*) zapoznać się z zawartością utworzonego pliku.
6. Wysłać plik ze swoim kluczem publicznym do partnera.
7. Odebrać wiadomość pocztową od partnera. Powinna ona zawierać plik z kluczem publicznym partnera.
8. W oknie programu *GPGkeys*, w menu ***Klucz(e)*** wybrać funkcję ***Importuj***.
9. Wskazać miejsce przechowywania pliku pobranego z wiadomości od partnera.
10. Dokończyć proces importu.

Zadanie 2– Zabezpieczanie wiadomości pocztowych

1. Wysłać zaszyfrowaną i podpisaną wiadomość pocztową. Szyfrowanie włączamy poprzez wciśnięcie przycisku ***Szyfruj*** (*Encrypt*) a podpisywanie poprzez wciśnięcie przycisku ***Podpisz*** (*Sign*) w oknie tworzonej wiadomości. Obejrzeć treść wysłanej wiadomości w folderze ***Elementy wysłane*** (*Sent items*) programu ***Outlook Express***.
2. Odebrać zaszyfrowaną wiadomość pocztową od partnera. Obejrzeć wiadomość w postaci zaszyfrowanej i po odszyfrowaniu. Po otworzeniu wiadomości powinno pojawić się okno z żądaniem wpisanie hasła deszyfrującego klucz publiczny nadawcy. Jeżeli takie okno nie pojawi się, to należy zapisać treść wiadomości do pliku tekstowego. Następnie należy uruchomić

program ***GPGtools***. Po wybraniu funkcji deszyfrowania, wskazać plik tekstowy z zapisaną wiadomością.

Zadanie 3– Zabezpieczanie plików

1. Utworzyć plik tekstowy o nazwie P1_xx.TXT (gdzie xx jest numerem komputera, na którym realizowane jest zadanie). Wpisać do niego swoje imię i nazwisko. Zaszyfrować plik wybierając z jego menu podręcznego funkcję ***GPGshell*** a następnie ***Zaszyfruj***.
2. Odszyfrować i odczytać zaszyfrowany plik P1_xx.TXT.GPG (gdzie xx jest numerem komputera, na którym realizowane jest zadanie). W tym celu w jego menu podręcznym wybrać funkcję ***GPGshell*** a następnie ***Odszyfruj/Zweryfikuj***. W czasie deszyfracji nie „nadpisywać" pliku P1_xx.TXT, lecz umieścić odszyfrowaną zawartość w pliku P2_xx.TXT (gdzie xx jest numerem komputera, na którym realizowane jest zadanie).

Zadanie 4– Naruszenia zabezpieczeń

1. Utworzyć plik DANEXX.TXT i wpisać do niego swoje imię i nazwisko. Symbol xx jest numerem komputera, na którym realizowane jest zadanie.
2. Podpisać plik (podpis zwykły) przy pomocy polecenia:

   gpg --output DANEXX.SIG --sign DANEXX.TXT
3. Zmienić trzy dowolne znaki w pliku DANEXX.SIG. Następnie zweryfikować podpis wprowadzając polecenie:

   gpg --verify DANEXX.SIG
4. Podpisać plik (podpis *clearsign*) przy pomocy polecenia:

   gpg --clearsign DANEXX.TXT
5. W utworzonym w ten sposób pliku DANEXX.TXT.ASC zmienić swoje nazwisko. Następnie zweryfikować podpis wprowadzając polecenie:

   gpg --verify DANEXX.TXT.ASC
6. Skasować wszystkie utworzone w tym zadaniu pliki.

Samodzielnie przeprowadzić eksperyment sprawdzenia szyfrowania i deszyfrowania schowka. Tego punktu nie należy dokumentować w sprawozdaniu.

Korzystając z programu *GPGkeys* usunąć wszystkie klucze wygenerowane i importowane w tym ćwiczeniu. Odinstalować programy *GPGshell* i *GPG.*