Podstawy obsługi kryptografii PGP za pomocą pakietu GPG4WIN

Instalacja GPG pod Windows: gpg4win
http://www.gpg4win.org/download.html

Generacja własnej pary kluczy (pub, sub):

gpg --gen-key

Wyświetlanie listy kluczy publicznych w „keyringu" lokalnego komputera:

gpg --list-keys

Wyświetlanie listy kluczy prywatnych w „keyringu" lokalnego komputera:

gpg --list-secret-keys

Sprawdzanie „fingerprint" – odcisku kluczy lokalnego komputera (odcisk jest potrzebny do autoryzacji klucza publicznego)

gpg --fingerprint

Eksport własnego klucza publicznego na internetowy serwer kluczy:

gpg --keyserver subkeys.pgp.net --send-key *ośmioznakowy_id*

Eksport własnego klucza publicznego do pliku tekstowego:

gpg --armour --output *dowolna_nazwa_pliku* --export *email_klucza (jeśli nie zostanie podany, wyeksportowane zostaną wszystkie klucze)*

Wyszukiwanie klucza publicznego na internetowym serwerze kluczy:

gpg --keyserver subkeys.pgp.net --search-key *email_klucza*

Pobieranie klucza publicznego z internetowego serwera kluczy:

gpg --keyserver subkeys.pgp.net --recv-key *email_klucza*

Podpisywanie i weryfikacja zaimportowanego klucza publicznego za pomocą własnego klucza prywatnego:

gpg –edit-key *email_klucza*
sign
trust
check

Szyfrowanie pliku do formatu tekstowego za pomocą klucza publicznego (parametr –r określa, kto może taki plik odszyfrować, jeśli nie podamy więc własnego klucza, to nie odszyfrujemy takich danych)

gpg --armour --output *nazwa.gpg* -r *email_klucza* --encrypt *nazwa_pliku_do_zaszyfrowania*

Deszyfrowanie pliku za pomocą klucza prywatnego

gpg --output *nazwa_pliku* --decrypt *nazwa_pliku_zaszyfrowanego*

Szyfrowanie symetryczne (uwaga – nie używamy hasła do klucza prywatnego!)

gpg –o *nazwa_pliku_zaszyfrowanego* -c *nazwa_pliku_jawnego*
gpg -o *nazwa_pliku_jawnego* -d *nazwa_pliku_zaszyfrowanego*

Podpisywanie danych (bez szyfrowania)

gpg --output *nazwa_pliku* --clearsign *nazwa_pliku_do_podpisania*

Weryfikacja podpisu

gpg --verify /tmp/wiadomosc.sig /tmp/wiadomosc.txt

Nakładka graficzna dla Windows: GpgEx, opcje w menu kontekstowym.

Zadanie do wykonania w parach, w konsoli cmd:

1. Uruchom wiersz poleceń (cmd) i sprawdź czy działa polecenie gpg, jeśli nie, to zainstaluj aplikację GPG4WIN http://www.gpg4win.org/download.html
2. Wygeneruj własną parę kluczy.
3. Wyeksportuj klucz publiczny na serwer subkeys.pgp.net oraz do pliku.
4. Zaimportuj klucz partnera.
5. Wyświetl listę kluczy umieszczonych na komputerze.
6. Podpisz i zweryfikuj zaufanie do klucza partnera.
7. Utwórz plik tekstowy o nazwie *twojeimię1.txt* z dowolną zawartością
8. Zaszyfruj plik tekstowy kluczem publicznym partnera i prześlij plik *twojeimię1.txt* do niego dowolnym sposobem (np. przez e-mail).
9. Odszyfruj plik *imiępartnera1.txt* otrzymany od partnera.
10. Utwórz plik o nazwie *twojeimię2.txt* z dowolną zawartością.
11. Zaszyfruj symetrycznie plik *twojeimię2.txt* i wyślij ten plik do partnera dowolnym sposobem.
12. Odszyfruj plik *imiępartnera2.txt* otrzymany od partnera.
13. Utwórz plik tekstowy z dowolną zawartością o nazwie *twojeimię3.txt*
14. Podpisz plik *twojeimię3.txt* i prześlij go do partnera dowolnym sposobem.
15. Zweryfikuj podpis pliku *imiępartnera2.txt*, który otrzymasz od partnera.

Dla chętnych: przećwicz szyfrowanie asymetryczne oraz podpisywanie i weryfikację za pomocą graficznej nakładki GpgEx.