Bezpieczeństwo Sieci Komputerowych - laboratorium

Ćwiczenie 2: Kryptografia.

Cel ćwiczenia: Opanowanie umiejętności posługiwania się narzędziami do szyfrowania, deszyfrowania, cyfrowego podpisywania dokumentów oraz weryfikacji podpisów cyfrowych.

Wprowadzenie

Wykorzystywany jest pakiet kryptograficzny gpg4win oraz program pocztowy (np. Thunderbird lub Outlook) w wtyczką gpg. Dalsze informacje na stronie projektu www.gnupg.org oraz w pliku GnuPG.pdf.

Wymagane informacje

- Znajomość zasad działania algorytmów kryptograficznych symetrycznych i asymetrycznych oraz funkcji hashujących
- Znajomość zasad składania i weryfikacji podpisów cyfrowych
- Umiejętność posługiwania się aplikacją gpg (patrz: GnuPG.pdf)

Ćwiczenia do wykonania

- Ćwiczenia wykonywane są w systemie operacyjnym Windows dostępnym w laboratorium (może istnieć konieczność doinstalowania w/w aplikacji).
- Wykonując zadania proszę wszędzie gdzie to możliwe umieszczać **dane członków grupy** (nazwiska i numery indeksów) – w nazwach właścicieli kluczy, tworzonych plików, katalogów, kont użytkowników, treści plików, komunikatach, itp. Ich obecność na zrzutach ekranu w sprawozdaniu jest potwierdzeniem wykonania ćwiczeń.

[ZE] oznacza konieczność umieszczenia odpowiedniego zrzutu ekranu w sprawozdaniu.

UWAGA: Ćwiczenia 1-5 musi wykonać każdy z członków grupy!

1. Pobrać i zainstalować gpg4win (ze wszystkimi pakietami, w szczególności GPA), program pocztowy *Mozilla Thunderbird* oraz wtyczkę enigmail (lub analogiczne, jeśli wybrano inny program pocztowy). Skonfigurować w programie konto pocztowe (np. założyć nowe konto na ogólnodostępnym serwisie lub użyć istniejącego).
2. Wygenerować klucze: prywatny i publiczny przy wykorzystaniu programu *Thunderbird*, GPA oraz z linii poleceń za pomocą programu gpg [ZE] (tj. każdy z członków grupy generuje po 3 klucze o różnych parametrach – algorytm, długość klucza, termin ważności). **W kolejnych ćwiczeniach użyć należy jednego z 3 wygenerowanych kluczy – klucza dla algorytmu RSA.**
3. Wyeksportować klucz prywatny i publiczny do pliku w formacie ASCII. Wygenerować i zanotować odcisk klucza publicznego [ZE].

4. Wyeksportować jeden klucz publiczny na serwer kluczy [ZE]. Przeszukać serwer kluczy i sprawdzić czy jest na nim wyeksportowany klucz (indeksacja klucza zwykle trwa kilka minut). Sprawdzić, czy istnieje możliwość usunięcia klucza (i jak to zrobić).
5. Zaimportować klucz publiczny drugiej osoby z grupy oraz podpisać go swoim kluczem. Sprawdzić czy podpis jest dołączony do klucza [ZE]. Odesłać klucz publiczny drugiej osobie.
6. Utworzyć krótki plik tekstowy zawierający nazwiska członków grupy, bieżącą datę i godzinę. Podpisać cyfrowo plik korzystając z konsoli a następnie zweryfikować podpis korzystając z nakładki graficznej (Kleopatra) [ZE].
7. Podpisać plik binarny (np. PDF z tą instrukcją) zamieszczając podpis w osobnym pliku (w postaci 'czytelnej') [ZE].
8. Zaszyfrować plik spod nakładki graficznej (Kleopatra) i odszyfrować korzystając z konsoli [ZE].
9. Zaszyfrować plik poleceniem konsoli, odszyfrować korzystając z nakładki graficznej [ZE].
10. Pobrać klucz prowadzącego z serwera kluczy. Na serwerze znajduje się kilka kluczy dla podanego adresu, ale tylko jeden jest poprawny - należy zidentyfikować poprawny klucz.
    Klucz dla adresu e-mail: *bsk2030@w4.pwr.pl*
    Odcisk właściwego klucza: *89DBEEDD6092A4F1576D83DDE02FABA5A9C05432*
    Klucz będzie niezbędny do wykonania kolejnego zadania.
11. Treść tego zadania została przez prowadzącego zapisana w osobnym pliku ZAD11.txt i umieszczona na stronie. Niestety, na stronie umieszczono kilka podobnych plików z fałszywą treścią. Na szczęście prowadzący podpisał oryginalny plik (kluczem z zad. 10), więc te podrobione nie przejdą weryfikacji podpisu. Zidentyfikować oryginalny plik [ZE] za pomocą klucza prowadzącego i wykonać właściwe zadanie.

    (Do zmiany używanego algorytmu symetrycznego służy opcja `--cipher-algo`, np.:
    `gpg --cipher-algo 3des ... )`
12. Z klienta poczty wysłać, do drugiej osoby z grupy, podpisany cyfrowo i zaszyfrowany e-mail. Odczytać e-mail otrzymany od drugiej osoby z grupy, zweryfikować poprawność podpisu [ZE].
13. Sprawdzić, jakim algorytmem symetrycznym są szyfrowane dane. Zaszyfrować plik tekstowy z wykorzystaniem tylko kryptografii symetrycznej za pomocą 3 różnych algorytmów [ZE]. Porównać rozmiary i zawartość zaszyfrowanych plików.

Przed opuszczeniem sali wyłączyć komputer.

Sprawozdanie - składa się z trzech części:

1. Klucze publiczne – każdy student zamieszcza swój klucz publiczny, podpisany przez drugiego członka grupy. Zamieszczony ma zostać czytelny plik (ASCII). Plik z kluczem ma mieć nazwę *Klucz_Nazwisko.asc*. Klucz prywatny należy przechowywać do ostatnich zajęć, będzie potrzebny do kolejnych ćwiczeń i sprawozdań.

2. Sprawozdanie z ćwiczenia - wyłącznie w formacie .pdf. Proszę udokumentować wykonane zadania za pomocą zrzutów ekranu opatrzonych własnymi komentarzami. W przypadku zadań wymagających samodzielnego rozwiązania zamieścić dokładny opis ich realizacji (np. wybrane opcje i wartości). Odpowiedzieć na pytania z instrukcji, omówić różnice pomiędzy różnymi algorytmami symetrycznymi, zamieścić wymagane analizy.

3. Podpisy pod sprawozdaniem. Plik ze sprawozdaniem ma zostać podpisany (oczywiście cyfrowo) przez wszystkich członków grupy. Podpisy mają być osobnymi plikami i muszą być weryfikowalne za pomocą kluczy publicznych z pierwszej części sprawozdania. Plik z podpisem ma mieć nazwę złożoną z czterech pierwszych liter nazwiska (tylko małe litery, bez polskich znaków), np.: *kowa.sig* (student Kowalski), *zak.asc* (student Żak), nazwa pliku jest bardzo ważna – poprawność podpisów weryfikuje skrypt. Brak lub niepoprawny podpis oznacza obniżenie oceny z ćwiczenia o 20%.

Klucze proszę zachować - podpisywane mają być również kolejne sprawozdania.