Ćwiczenia laboratoryjne z przedmiotu Kryptografia i Bezpieczeństwo Danych

Temat: Szyfrowanie poczty elektronicznej

Autor: Sławomir Samolej

Wprowadzenie

1. System szyfrowania z kluczem symetrycznym ma jedną podstawową wadę. Trudno jest przesłać tajny klucz w taki sposób, żeby go nikt nie przejął. Rozwiązaniem tego problemu okazało się wynalezienie kryptografii z kluczem publicznym [1]. W pewnym uogólnieniu ten nowy typ szyfrowania polega na zastosowaniu klucza składającego się z dwóch kluczy, które są ze sobą powiązane. Wiadomości zaszyfrowane z zastosowaniem jednego z nich mogą być odszyfrowywane z zastosowaniem drugiego. Można wtedy jeden z kluczy (nazywany publicznym) umieścić na swojej stronie i pozwolić osobom za jego pomocą szyfrować wiadomości. Treść wiadomości pozostanie tajna, a adresat z zastosowaniem swojego drugiego klucza (prywatnego) może odszyfrowywać przesłane wiadomości.
   Szyfrowanie z kluczem publicznym zostanie szerzej omówione na zajęciach wykładowych.

2. Na omówionej w punkcie 1 zasadzie można zorganizować przesyłanie do siebie zaszyfrowanych wiadomości poczty elektronicznej. Od wersji programu Thunderbird 78 istnieje możliwość zorganizowania systemu szyfrowanej i podpisywanie poczty w oparciu o odpowiednią konfigurację tylko tego programu [3].

3. Dla wcześniejszych wersji oprogramowania (do 68) skonfigurowanie szyfrowania poczty wymagało instalacji dodatkowych programów oraz plug-inu do klienta poczty [2].

Uwagi:

Pokazane rozwiązanie pokazuje tylko, jak ktoś z zewnątrz może do nas wysłać wiadomość w postaci zaszyfrowanej. Nie rozwiązuje problemu zapewnienia, że wiadomość przyszła od określonego odbiorcy. Do tego służą MAC lub podpisy elektroniczne.

Krótkie wyjaśnienie na podstawie [5]:
„Dla dociekliwych: PGP nie szyfruje całego dokumentu (np. listu) z użyciem algorytmu RSA - ponieważ jest on dość powolny, trwałoby to bardzo długo. Zamiast tego, PGP szyfruje z użyciem RSA pewną wygenerowaną losowo liczbę 128-bitową, która następnie jest używana jako klucz szyfrowania właściwego dokumentu (np. listu) "tradycyjnym" algorytmem IDEA. Przy deszyfracji, PGP odszyfrowuje klucz IDEA z użyciem prywatnego klucza RSA odbiorcy, a następnie kluczem IDEA odszyfrowuje list. W zasadzie zatem PGP jest połączeniem "tradycyjnego" kryptosystemu bazującego na kluczu przekazanym kanałem bezpiecznym (innym dla każdej wiadomości), i kryptosystemu opartego o metodę klucza publicznego, który zapewnia ten bezpieczny kanał).”

Przebieg ćwiczenia

1. Proszę pobrać i skonfigurować system szyfrowania poczty elektronicznej na podstawie opracowań [3] i [4].

2. Proszę korzystając z udostępnionego na stronie
   http://ssamolej.kia.prz.edu.pl/dydaktyka/KiBD/index.htm
   klucza publicznego zaszyfrować i wysłać wiadomość na adres ssamolej@kia.prz.edu.pl

3. Proszę uzupełnić samodzielnie wiadomości na temat możliwości konfigurowania innych klientów pocztowych w celu umożliwienia szyfrowania wiadomości.

Literatura

[1] (Podstawowe informacje na temat szyfrowania z kluczem publicznym)
https://pl.qwe.wiki/wiki/Public-key_cryptography

[2] (Instrukcja konfiguracji klienta poczty Thunderbird do tworzenia zaszyfrowanych wiadomości dla wersji do 68)
https://sekurak.pl/szyfrowanie-poczty-w-thunderbird/

[3] (Uwagi wskazujące zasadę konfiguracji programu Thunderbird w wersji 78 do szyfrowania poczty i podpisywania wiadomości)
https://support.mozilla.org/pl/kb/openpgp-w-thunderbirdzie-howto-i-faq

[4] (Krótki instruktarz konfiguracji szyfrowania wiadomości z zastosowaniem GPG w programie Thunderbird od wersji 78)
https://sekurak.pl/thunderbird-zaczal-domyslnie-wspierac-obsluge-szyfrowania-end2end-ochrona-przed-inwigilacja-rzadowa/

[5] (Opis systemu PGP dla laika)
https://home.agh.edu.pl/~szymon/artykuly/pgp_opis.html