**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. Może do tego posłużyć zestaw 3 darmowych narzędzi, które w łatwy sposób integrują się ze sobą: Klient poczty **Thunderbird**, plug-in do klienta poczty **Enigmail** oraz oprogramowanie szyfrujące GPG (GNU Privacey Guard). Szczegółowa instrukcja instalacji i konfiguracji oprogramowania znajduje się w [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.

Szyfrowanie z kluczem publicznym jest złożone obliczeniowo, stąd służy do wykonywania zwykle do szyfrowania „off-line”, (tak jak u nas: szyfrowanie poczty) lub szyfrowania małych porcji danych lub w końcu do zaszyfrowanego przesyłania kluczy symetrycznych. Szczegóły zostaną omówione na wykładzie.

**Przebieg ćwiczenia**

1. Proszę pobrać i skonfigurować system szyfrowania poczty elektronicznej na podstawie opracowania [2].
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)
<https://sekurak.pl/szyfrowanie-poczty-w-thunderbird/>