

## ĆWICZENIE NR 12

### OCHRONA DANYCH

*Eugeniusz Kuriata, Radosław Barańczak*

#### 1. CEL ĆWICZENIA

Celem ćwiczenia jest zapoznanie się ze strukturą i działaniem PGP - komputerowego systemu kryptograficznego do ochrony poczty elektronicznej oraz plików danych. Ponadto ćwiczenie obejmuje rozwiązania kilku przykładowych zadań dotyczących generowania kluczy szyfrowania oraz podpisywania, szyfrowania i deszyfracji pliku tekstowego.

#### 2. WPROWADZENIE

Postępujący w drugiej połowie XX wieku rozwój różnych gałęzi gospodarki i technologii, a w szczególności spektakularny postęp w dziedzinach telekomunikacji i komputeryzacji stał się fundamentem rozwoju nowych dziedzin określanych ogólnie jako elektroniczny biznes. Są to m.in.: elektroniczny handel towarami i usługami, elektroniczny transfer płatności, home-banking, dokonywanie i realizacja zamówień elektronicznych.

Potencjalne obszary zagrożeń w systemach elektronicznej wymiany danych związane są z bezpieczeństwem transmisji oraz autoryzacją stron biorących udział w wymianie. Ponieważ do transmisji danych wykorzystywane są sieci teleinformatyczne, komunikaty narażone są na uszkodzenie oraz na różnego typu zniekształcenia. Zniekształcenia te mogą one mieć charakter przypadkowy, wynikający z błędów jakie mogą powstać w urządzeniach przekaźnikowych, ale także mogą być związane

z ingerencją osób trzecich. Przesyłane przez sieć dane, przechodzą przez wiele pośredniczących węzłów, w których mogą być przechwytywane przez „intruzów”, a także zniekształcone lub skopiowane przez nich.

Stosowane w Internecie narzędzia odpowiedzialne za bezpieczeństwo, nie spełniają w pełni wymagań stawianych przez użytkowników sieci. Brak jest jednolitych technologii i standardów bezpieczeństwa, ma to znaczny wpływ na zmniejszenie bezpieczeństwa podczas wymiany danych. W sieci Internet problemem jest brak mechanizmów kompleksowego śledzenia i potwierdzenia dokonywanych transakcji. Mechanizmy takie, mogą być stworzone jedynie na potrzeby zamkniętych społeczności (korporacji).

Brak jednolitych standardów nie oznacza braku systemów zapewniających bezpieczeństwo przesyłanych danych. Istnieje bowiem wiele systemów wykorzystujących istniejące rozwiązania i technologie systemów kryptograficznych m.in.: PGP (*Pretty Good Privacy*), SSL (*Secure Sockets Layer*), SET (*Secure Electronic Transaction*), SEPP (*Secure Electronic Payment Protocol*), S/HTTP (*Secure Hypertext Transfer Protocol*), S/MIME (*Secure Multipurpose Internet Mail Extension*), EDI (*Electronic Data Interchange*). Jednak istniejące systemy oprócz tego, że zapewniają bezpieczeństwo nie są pozbawione również wad. Mianowicie stwarzają możliwości ominięcia istniejących w nich zabezpieczeń i np. niezauważone przekierowanie wiadomości do innego adresata.[2]

Szybko rozwijające się gałęzie gospodarki elektronicznej jak i organizacje biznesowe wymagają wypracowania standardów umożliwiających dokonywanie bezpiecznych płatności realizowanych poprzez Internet. Obecnie w większości rozwiązań używany jest do tego celu protokół SSL. Zapewnia on poprzez szyfrowanie, bezpieczną transmisję danych oraz autoryzację stron uczestniczących w procesie wymiany informacji. Jednak autoryzacja opiera się na wzajemnym zaufaniu uczestników wymiany. Szereg organizacji zbudowało na tej bazie swoje systemy wymiany danych, które powszechnie uważane są jako bezpieczne. To zaufanie do tych systemów polega przede wszystkim na tym, że uczestnicy traktowani są tutaj jako członkowie korporacji.[3]

Innym szeroko wykorzystywanym rozwiązaniem jest Elektroniczna Wymiana Danych - EDI.[4] Oznacza ona wymianę standardowo

sformatowanych danych w postaci uzgodnionych komunikatów w formie elektronicznej między systemami informatycznymi partnerów handlowych przy minimalnej ingerencji ze strony człowieka. Zastosowanie EDI z jednej strony niesie za sobą wiele korzyści m.in.: poprawia sprawność funkcjonowania firmy oraz jakość i efektywność świadczonych usług, automatyzuje obieg dokumentów, zapewnia szybki dostęp do informacji biznesowych, pozwala na efektywniejsze wykorzystanie zatrudnionego personelu oraz usprawnia obieg płatności. Z drugiej strony, stanowi źródło problemów związanych z bezpieczeństwem i autoryzacją danych przesyłanych drogą elektroniczną.

W prezentowanym ćwiczeniu zostanie przedstawiony system PGP, który służy do ochrony poczty elektronicznej, może być on również wykorzystywany do szyfrowania plików. Poczta elektroniczna (e-mail) jest usługą internetową, która obecnie jest najczęściej wykorzystywana do komunikowania się za pośrednictwem sieci. Zanim list wysyłany przy pomocy poczty elektronicznej trafi do adresata, przechodzi przez wiele węzłów pośrednich w sieci komputerowej. W każdym z tych punktów może on zostać łatwo odczytany. Powstaje tylko pytanie, kto chciałby to zrobić? Mogą to być organizacje szpiegowskie obcych państw, lokalne rządy zainteresowane szpiegowaniem własnych obywateli, przedsiębiorstwa konkurujące z nami w interesach, dziennikarze po to by zdobyć ciekawy sprzedający się temat, przestępcy chcący uzyskać pewne wartościowe dla nich dane (numery kont lub kart kredytowych), czy nawet nasz pracodawca. Dlatego też, zawsze gdy zależy nam na poufności informacji którą przesyłamy, powinno się stosować programy do ochrony poczty elektronicznej np. PGP. Dodatkowo adresat dodając do przesyłanej wiadomości podpis cyfrowy, może zapewnić, że odbiorca będzie wiedział kto wysłał wiadomość. Odbiorca nie będzie mógł również podstawić innej wiadomości w miejsce oryginalnej i udawać, że otrzymał ją od deklarowanego nadawcy.

Obecnie użytkownicy prowadzący wymianę informacji wykorzystując do tego sieć zmuszeni są do „wzajemnego zaufania do siebie”, muszą także polegać na dostawcach usług sieciowych przesyłających wymieniane informacje.[2] W celu zapewnienia odpowiedniego poziomu bezpieczeństwa stosowane są wybrane techniki szyfrowania a autoryzację stron realizuje się poprzez wykorzystanie certyfikatów oraz agencji uwierzytelniających tzw. zaufanych trzecich stron.

Głównym czynnikiem ograniczającym stosowanie internetu do zastosowań biznesowych jest obecnie brak ogólnie (prawnie) obowiązujących reguł, definiujących obowiązki, zakres odpowiedzialności, tryb i sposoby rozstrzygania sporów w zakresie przesyłania komunikatów między partnerami wykorzystującymi Internet.[5]

### **Kilka słów na temat szyfrowania**

Szyfrowanie jest podstawowym mechanizmem zapewniającym ochronę plików i wiadomości w postaci binarnej. W konwencjonalnych systemach kryptograficznych stosuje się pojedynczy klucz zarówno do zaszyfrowania jak i do deszyfracji. Oznacza to, że nadawca, który chce wysłać do adresata zaszyfrowaną w takim systemie wiadomość, musi w pierwszej kolejności dostarczyć mu wcześniej klucz kryptograficzny szyfrowania. Przy pomocy tego klucza adresat będzie mógł odszyfrować otrzymaną wiadomość oraz zaszyfrować odpowiedź do nadawcy. Klucz musi być przesłany przez tzw. kanał bezpieczny zanim obie strony będą wymieniać zaszyfrowane wiadomości przez tzw. kanał niezabezpieczony. Jeżeli nadawca i adresat widzieli się zanim zaczęli wymieniać wiadomości mogli uzgodnić klucz szyfrowania. Jeżeli zaś nigdy wcześniej się nie widzieli, nie mają zaufania do telefonu i poczty, znalezienie bezpiecznego kanału może okazać się niemożliwe.

W systemach kryptograficznych z kluczem jawnym każdy posiada dwa związane ze sobą komplementarne klucze: klucz jawny (ujawniony publicznie) i klucz tajny (znany tylko właścicielowi klucza). Wiadomość zaszyfrowaną za pomocą każdego klucza z pary można odszyfrować przy pomocy drugiego. Znajomość jawnego klucza nie pomaga w odgadnięciu odpowiadającego mu klucza tajnego, dlatego klucz jawny można opublikować i rozpowszechnić w sieci komunikacyjnej np. internecie. W systemach tych nie ma potrzeby korzystania z kanału zabezpieczonego, który był potrzebny w konwencjonalnych systemach kryptograficznych.[1]

Każdy może zastosować klucz jawny odbiorcy aby zaszyfrować wiadomość do niego, odbiorca posiada bowiem własny, odpowiadający jawnemu, klucz tajny do odszyfrowania tej wiadomości. Wiadomość może odszyfrować tylko odbiorca, ponieważ nikt inny nie ma dostępu do jego klucza tajnego. W systemach z kluczem jawnym nawet osoba która

zaszyfrowała wiadomość nie może jej odszyfrować, może to zrobić tylko adresat.

Własny klucz tajny nadawcy można również zastosować do zaszyfrowania wiadomości. Tworzy się w ten sposób podpis cyfrowy wiadomości, który może sprawdzić odbiorca, lub dowolna inna osoba, korzystając z klucza jawnego nadawcy do jej odszyfrowania. Dzięki temu wiemy, że nadawca jest prawdziwym autorem wiadomości oraz, że nikt oprócz nadawcy nie mógł jej zmienić, ponieważ tylko nadawca posiada klucz tajny użyty do podpisywania. Nadawca nie może się wyprzeć swojego podpisu. [1]

Dzięki połączeniu tych dwóch procesów uzyskuje się zapewnienie zarówno prywatności oraz uwierzytelnienie. W tym celu najpierw podpisuje się wiadomość za pomocą klucza tajnego nadawcy, a następnie szyfruje za pomocą klucza jawnego odbiorcy. Odbiorca wykonuje te kroki w odwrotnej kolejności: najpierw odszyfrowuje wiadomość za pomocą swojego klucza tajnego, a następnie sprawdza podpis za pomocą klucza jawnego nadawcy. Kroki te są realizowane automatycznie przez oprogramowanie odbiorcy.[1]

### **Jak działa PGP?**

Ponieważ algorytmy szyfrowania z kluczem jawnym są o wiele wolniejsze od konwencjonalnego szyfrowania z kluczem pojedynczym. W PGP wykorzystuje się oba rodzaje szyfrowania jednocześnie. Oryginalna wiadomość niezaszyfrowana nazywana jest tekstem jawnym. W pierwszej kolejności w procesie niezauważalnym dla użytkownika zostaje wygenerowany tymczasowy losowy klucz szyfrowania, tylko dla potrzeb jednej sesji, który następnie jest używany do zaszyfrowania w systemie konwencjonalnym pliku tekstu jawnego. W następnej kolejności tymczasowy losowy klucz szyfrowania szyfruje się przy pomocy klucza jawnego odbiorcy. Zaszyfrowany w ten sposób losowy klucz sesji przesyła się razem z zaszyfrowanym tekstem (nazywanym szyfrogramem) do odbiorcy. Odbiorca przy pomocy własnego klucza tajnego odtwarza tymczasowy losowy klucz sesji, po czym używa go do odszyfrowania szyfrogramu przy pomocy algorytmu konwencjonalnego. [1]

Klucze jawne są przechowywane w indywidualnych „certyfikatach kluczy”. Zawierają one: identyfikator właściciela klucza (nazwa osoby), znacznik czasowy wydany w chwili utworzenia pary kluczy oraz aktualny ciąg klucza. Certyfikaty kluczy jawnych zawierają ciąg klucza jawnego, a certyfikaty klucza tajnego ciąg klucza tajnego. Każdy klucz tajny szyfruje się także za pomocą jego własnego hasła na wypadek kradzieży. W pliku kluczy, albo inaczej „pęku kluczy”, znajduje się jeden lub więcej takich certyfikatów kluczy. Pęki kluczy jawnych zawierają certyfikaty kluczy jawnych, a pęki kluczy tajnych zawierają certyfikaty kluczy tajnych (zwanym też prywatnymi).[1]

Program PGP odwołuje się wewnętrznie do kluczy za pomocą „identyfikatora klucza”. Powstaje on przez „obcięcie” pewnej części klucza jawnego. Chociaż wiele kluczy może mieć ten sam identyfikator użytkownika, to ze względów praktycznych żadne dwa klucze nie posiadają tego samego identyfikatora klucza.

Do tworzenia podpisów cyfrowych program PGP stosuje „skrót wiadomości”. Skrót wiadomości szyfruje się za pomocą klucza tajnego (nadawcy) w celu uformowania podpisu cyfrowego. Szyfruje się tylko skrót a nie całą wiadomość, ponieważ potrzeba do tego celu o wiele mniej czasu. Długość skrótu każdej wiadomości wynosi 128 bitów i powstaje w wyniku zastosowania kryptograficznie silnej, jednokierunkowej funkcji skrótu. Atakującemu trudno jest obliczyć wiadomość zastępcza, która dałaby w wyniku identyczny skrót wiadomości, a dodanie do wiadomości nawet jednego znaku (np. spacji) daje w wyniku różny skrót.[1]

Dokumenty podpisuje się, poprzedzając je certyfikatami podpisów, które zawierają identyfikator klucza zastosowanego do podpisu, skrót wiadomości dokumentu podpisany za pomocą klucza tajnego i znacznik czasowy określający czas złożenia podpisu. Identyfikatorowi klucza umożliwia odbiorcy odszukanie klucza jawnego nadawcy, w celu sprawdzenia podpisu. Oprogramowanie odbiorcy automatycznie wyszukuje klucz jawny nadawcy i identyfikator użytkownika w pęku kluczy jawnych odbiorcy.[1]

Zaszyfrowane pliki są poprzedzane identyfikatorem klucza jawnego, który został użyty do ich zaszyfrowania. Dzięki temu odbiorca stosuje może wyszukać klucz tajny, niezbędny do odszyfrowania wiadomości.

Czynności te są wykonywane automatycznie przez oprogramowanie odbiorcy, które wyszukuje potrzebny tajny klucz deszyfrujący w pęku kluczy tajnych odbiorcy. Te dwa typy pęków kluczy są podstawą metod przechowywania i zarządzania kluczami jawnymi i tajnymi. Zamiast przechowywać każdy klucz w odrębnym pliku, klucze są gromadzone w pękach kluczy. Taki sposób przechowywania kluczy ułatwia ich automatyczne wyszukiwanie za pomocą identyfikatora klucza lub identyfikatora użytkownika. Każdy użytkownik przechowuje swoją parę pęków kluczy. [1]

### 3. INSTALACJA PROGRAMU PGP

W prezentowanych poniżej przykładach użyto programu PGP freeware 6.5.3, którego program instalacyjny został dołączony na płycie CD-ROM w katalogu \PGP\install\. Instalację rozpoczynamy uruchamiając plik *setup.exe*. Po uruchomieniu program instalacyjny poprosi o zamknięcie wszystkich otwartych wcześniej programów. Jeżeli pracowaliśmy wcześniej w jakimś programie i nie zakończyliśmy pracy, zamykamy go i powracamy do programu instalacyjnego. Przechodzimy do kolejnego okna wybierając klawisz [Next]. Po zapoznaniu się z warunkami licencji musimy nacisnąć klawisz [Yes] aby przejść do kolejnego kroku, w którym możemy przeczytać o nowościach w programie, jego możliwościach i wymaganiach. Następnie wybieramy klawisz [Next] i przechodzimy do okna w którym podajemy w polu [Name] – imię i nazwisko, oraz w polu [Company] nazwę firmy w której pracujemy (nieobowiązkowo). Po wypełnieniu tych pól wciskamy klawisz [Next]. W następnym oknie wybieramy katalog w którym ma być zainstalowany program. Domyślny katalog to c:\Program files\Network Associates\PGP. Jeżeli chcemy wybrać inny katalog wciskamy klawisz [Browse...], jeżeli odpowiada nam zaproponowany - wciskamy klawisz [Next]. W następnym kroku wybieramy składniki programu, które mają być zainstalowane. Do wykonania ćwiczenia wystarczą składniki standardowo zaproponowane przez program instalacyjny. Po wybraniu składników przechodzimy do okna, w którym przedstawione jest to co zostało przez nas podane i wybrane. Jeżeli wszystko się zgadza wybieramy przycisk [Next] i rozpoczyna się proces instalacji. Po zakończeniu instalacji należy ponownie uruchomić komputer.

Teraz aby można było korzystać z programu należy wygenerować parę kluczy. Należy do tego użyć program PGPkeys, który można uruchomić z: Menu Start >Programs >PGP >PGPkeys

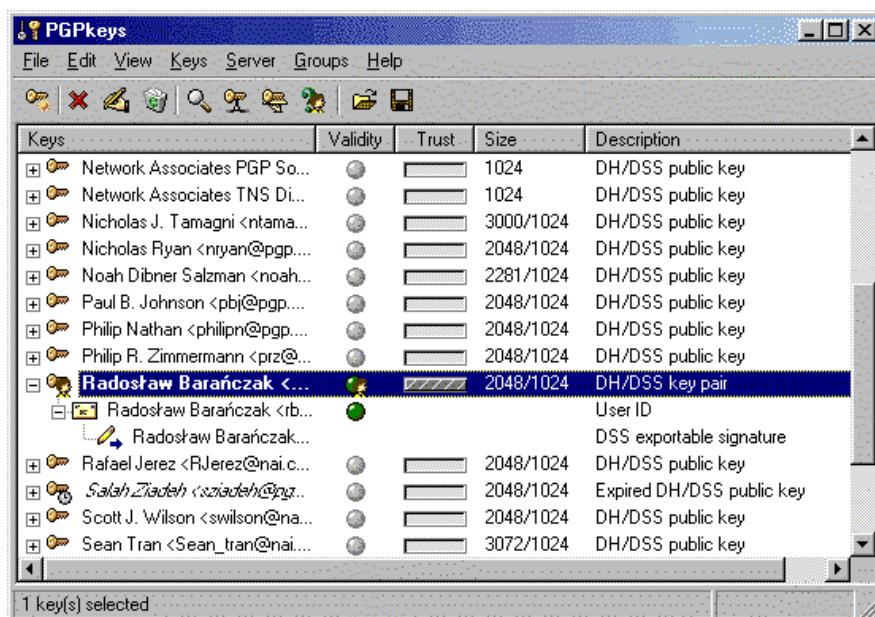
Przy pierwszym uruchomieniu programu PGPkeys proces generowania kluczy jest inicjowany automatycznie. Opis procesu generacji znajduje się poniżej w ćwiczeniu Generowanie pary kluczy

#### 4. PRZYKŁADY ZASTOSOWAŃ

Do zaprezentowania omawianych wcześniej problemów poniżej przedstawiono trzy ćwiczenia. Pokazują one jak w praktyce generować klucze, podpisywać tekst oraz zaszyfrować wiadomość do osoby, z którą chcemy się komunikować.


##### Generowanie pary kluczy

Zadanie polega na wygenerowaniu pary kluczy o długości 2048 bitów.



Rys.1. Widok okna programu PGPkeys

Po kliknięciu na ikonkę PGP  w prawej dolnej części ekranu wybieramy program PGPkeys.

Używając ikony  generatora kluczy uruchamiamy go, i przystępujemy do generowania pary kluczy.

W pierwszym kroku generator informuje, że aby można było podpisywać cyfrowo wiadomości oraz wysyłać do innych osób poufne wiadomości, musimy wygenerować parę kluczy jawny i tajny.

W drugim kroku podajemy dane osoby, dla której będą generowane klucze. Nie musimy koniecznie podawać imienia i nazwiska. Można wpisać np. pseudonim. Jednak podanie prawdziwych danych ułatwi innym użytkownikom PGP identyfikację naszej osoby.



*Rys.2. Generowanie pary kluczy – krok drugi – wprowadzanie danych identyfikacyjnych*

W trzecim kroku wybieramy algorytm, przy pomocy którego będzie wygenerowana para kluczy. Jeżeli będziemy wymieniali wiadomości z osobami używającymi PGP w wersji co najmniej 5.0 możemy wybrać algorytm Dieffie-Hellman/DSS, w przeciwnym wypadku wybieramy opcję RSA. Można też wygenerować dwie oddzielne pary kluczy jedną przy użyciu algorytmu Dieffiiego-Hellmana/DSS, a drugą przy użyciu RSA. Należy tylko powtórzyć proces generowania kluczy dwa razy.



*Rys.3. Generowanie pary kluczy – krok trzeci – wybór algorytmu generacji klucza*

Następnie wybieramy rozmiar klucza. Rozmiar klucza odpowiada ilości bitów użytych do jego budowy. Im większy jest rozmiar klucza, tym mniejsze są szanse na jego złamanie. Należy jednak pamiętać, że im dłuższy jest klucz tym dłuższy jest czas szyfrowania i deszyfracji.



*Rys.4. Generowanie pary kluczy – krok czwarty – wybór długości klucza*

Po wybraniu długości pary kluczy wybieramy okres ich ważności. Przy wybieraniu okresu ważności należy pamiętać, że nie można zmienić raz wybranego okresu ważności. Jeżeli nasz prywatny klucz straci swoją ważność, wiadomości zaszyfrowane wcześniej, kiedy klucz prywatny był jeszcze ważny będzie można ciągle odczytać. Nie będzie możliwe tylko podpisywanie wiadomości do innych osób.



Rys.5. Generowanie pary kluczy – krok piąty – ustalenie okresu ważności klucza

W kolejnym kroku podajemy hasło, przy pomocy którego będzie zaszyfrowany nasz klucz prywatny. Dla bezpieczeństwa ważnym jest aby hasło to miało co najmniej 8 znaków oraz zawierało znaki z poza alfabetu np. pBpwOI\$244. Hasło może być zdaniem, może zawierać wiele słów rozdzielonych spacjami. Ważne jest także to aby hasła tego nigdzie nie zapisywać. Należy je po prostu cały czas pamiętać.



*Rys.6. Generowanie pary kluczy – krok szósty – ustalenie hasła dostępu do kluczy*

Po wykonaniu tych czynności system zweryfikuje losowość naszego hasła. Jeżeli okaże się ono zbyt słabe system poprosi o ponowny wybór. Po pomyślnym przeprowadzeniu powyższych czynności następuje generowanie pary kluczy. Następnie system umożliwi nam wysłanie klucza jawnego do serwera, gdzie przechowywane są certyfikaty i klucze jawne innych użytkowników PGP. Dzięki umieszczenia naszego klucza jawnego na tym serwerze, będziemy dostępni dla osób chcących z nami wymieniać zaszyfrowane wiadomości.

Wykonanie powyższych kroków, kończy pracę generatora kluczy. Wygenerowane klucze tajny i jawny są szyfrowane i zapisywane odpowiednio do plików `secring.skr` i `pubring.pkr` (domyślnie pliki te są umieszczone na pulpicie).

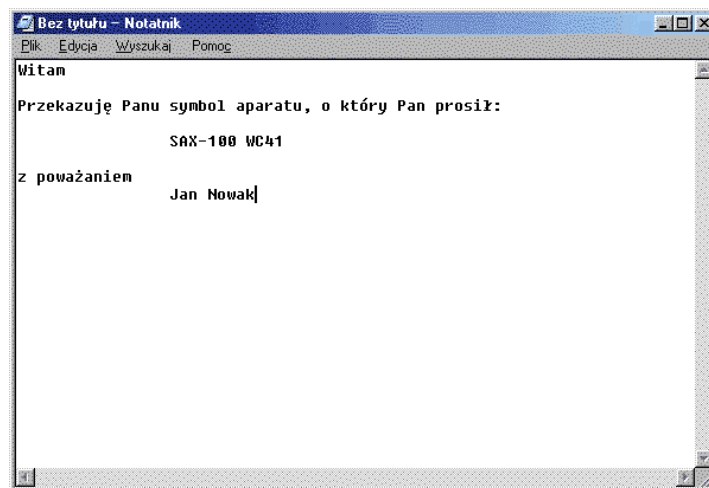


Rys.7. Generowanie pary kluczy – krok siódmy - wysyłanie klucza jawnego do serwera kluczy

## 5. PODPISYWANIE PLIKU TEKSTOWEGO

Zadanie polega na podpisaniu tekstu wpisanego w oknie notatnika.

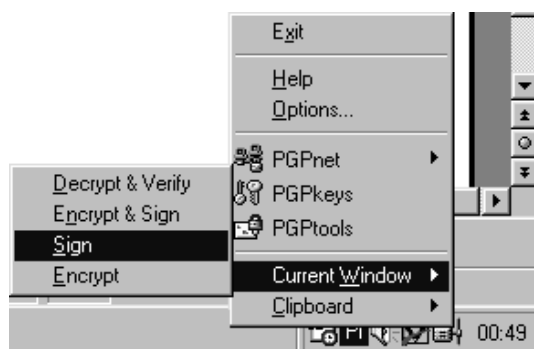
Zaczynamy od wpisania tekstu który będziemy podpisywać.



Rys.8. Przykładowy tekst w oknie notatnika.

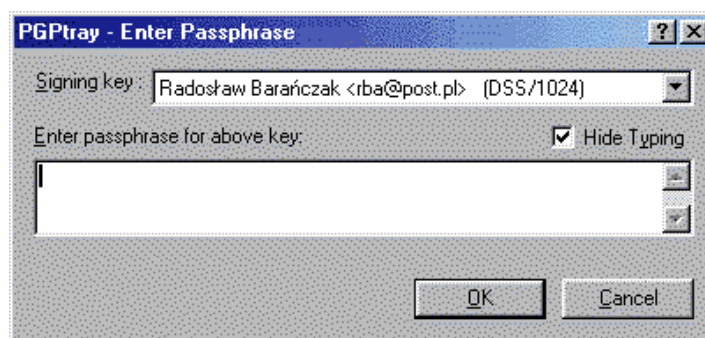
Następnie klikamy ikonę PGP  w prawej części paska zadań i wybieramy opcję:

Current Window > Sign



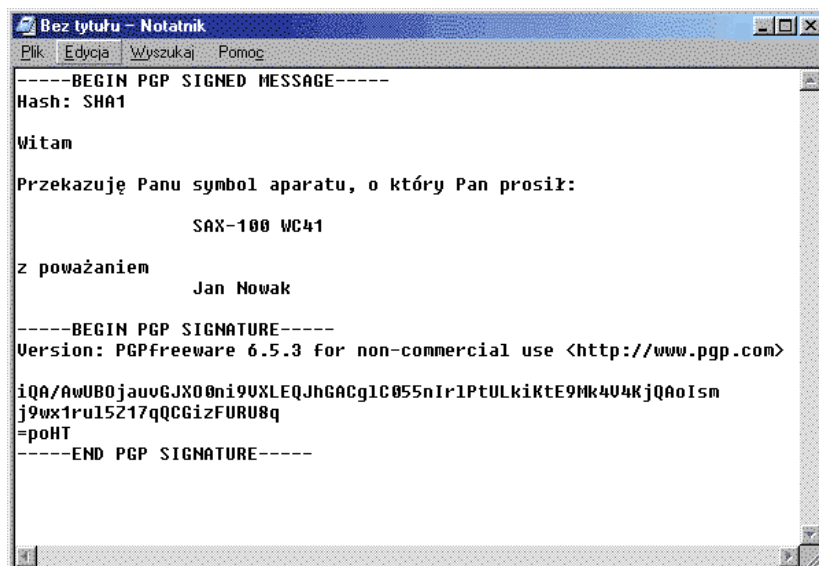
Rys.9. Widok menu programu PGP z paska zadań – wybrana opcja Sign.

Wprowadzamy hasło do tymczasowego odszyfrowania naszego klucza tajnego.




Rys.10. Okno wprowadzania hasła dostępu do klucza.

System automatycznie odszyfruje nasz klucz tajny i następnie podpisze tekst zawarty w okienku notatnika.

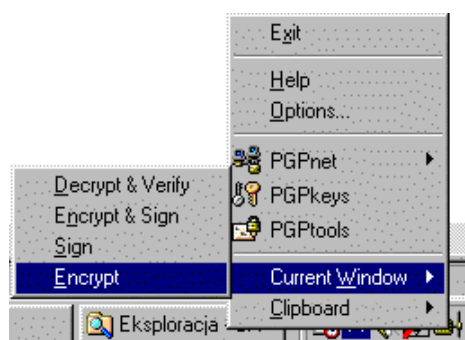


Rys.11. Podpisany tekst w oknie notatnika.

## 6. SZYFROWANIE PODPISANEGO PLIKU TEKSTOWEGO DLA OSOBY Z KTÓRĄ CHCEMY SIĘ KOMUNIKOWAĆ

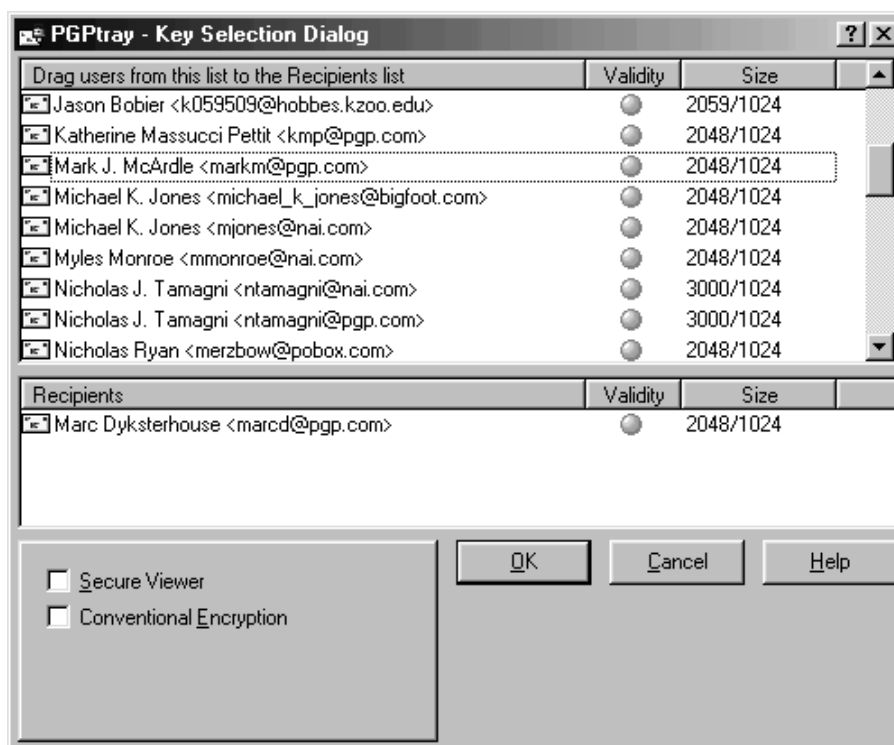
W tym zadaniu podpisany w poprzednim ćwiczeniu plik chcemy zaszyfrować by można go było wysłać do naszego znajomego. Klikamy w tym celu ikonkę PGP  na pasku zadań, poczym wybieramy opcję:

Current Window > Encrypt



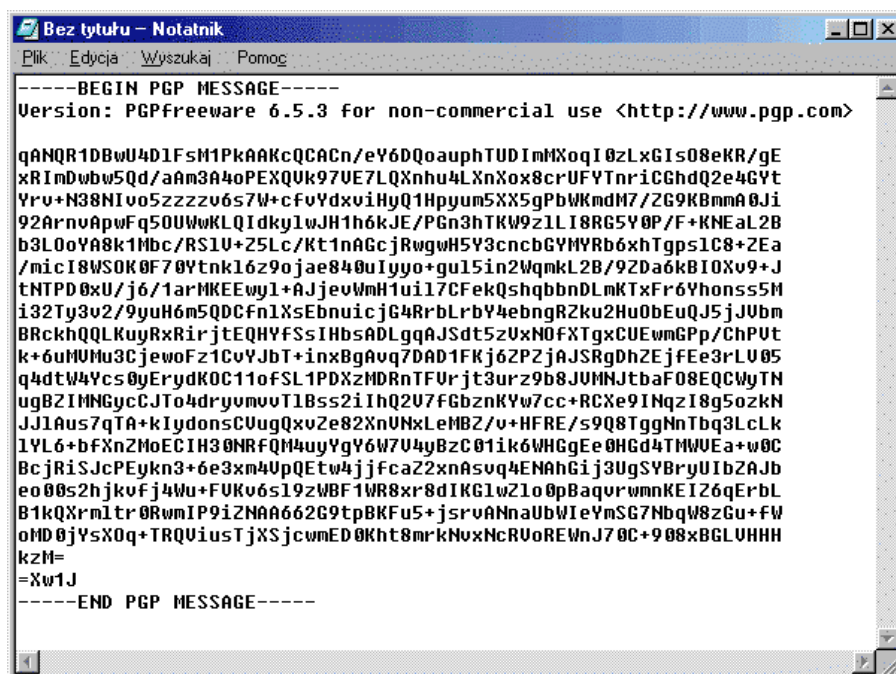
Rys.12. Widok menu programu PGP z paska zadań – wybrana opcja Encrypt.

Należy pamiętać aby wcześniej uaktywnić okno Notatnika, w którym znajduje się podpisany tekst wiadomości. Następnie wybieramy osobę, dla której będzie przeznaczona wiadomość.



Rys.13. Okno wyboru adresata wiadomości.

Po wybraniu osoby, do której chcemy wysłać wiadomość wciskamy klawisz OK. System automatycznie pobierze klucz jawny wybranej osoby i dokona szyfrowania. Poniżej przedstawiono szyfrogram wiadomości podpisanej w poprzednim ćwiczeniu.



Rys.14. Zaszzyfrowany tekst w oknie notatnika

## LITERATURA

1. B. Schneier Ochrona poczty elektronicznej, WNT, Warszawa 1996
2. E. Kuriata, M. Jędraszek, R. Barańczak, Zagrożenia fałszowania dokumentu elektronicznego, str. 423-437 w Zastosowania rozwiązań informatycznych w bankowości, Wydawnictwo Akademii Ekonomicznej im. O. Langego, Wrocław 2000
3. W. Gryciuk, Podstawy e-biznesu, TELEINFO nr 20/1999, wyd. internetowe
4. Valerie A. Leyland, Elektroniczna Wymiana Danych, WNT, Warszawa 1995
5. M. Mejssner, Trudny start elektronicznej gospodarki, TELEINFO 40/98 wyd. internetowe