

Artur Arciuch

Instytut Automatyki i Robotyki

Wydziału Cybernetyki WAT

**Wykorzystanie programu PGP
w pracy biurowej**

SPIS TREŚCI

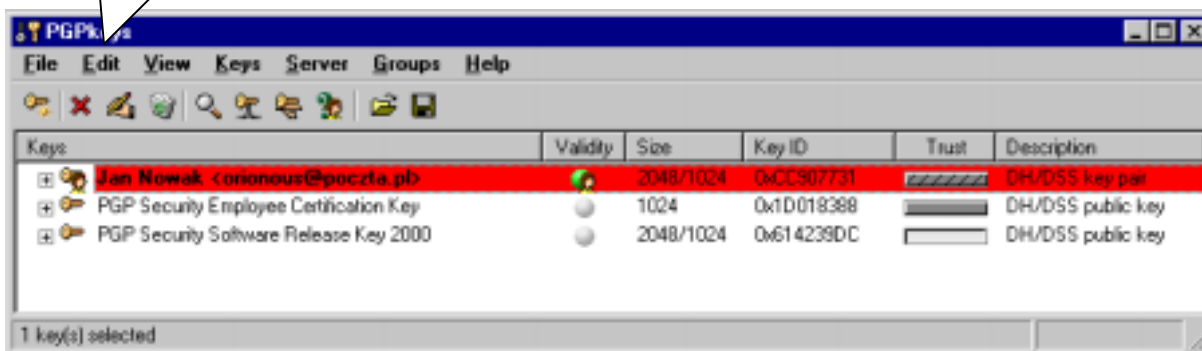
1. PRZECHOWYWANIE I OCHRONA KLUCZY.....	3
2. UDOSTĘPNIANIE WŁASNEGO KLUCZA PUBLICZNEGO INNYM UŻYTKOWNIKOM.	6
3. POBIERANIE KLUCZY PUBLICZNYCH INNYCH UŻYTKOWNIKÓW.....	11
4. WYSYŁANIE ZASZYFROWANYCH WIADOMOŚCI POCZTOWYCH	16
5. ODCZYTYWANIE ODEBRANYCH ZASZYFROWANYCH WIADOMOŚCI POCZTOWYCH	19
6. SZYFROWANIE PLIKÓW	22
7. ODCZYTYWANIE ZASZYFROWANYCH PLIKÓW	24
8. SZYFROWANIE TEKSTU Z WYBRANEGO OKNA LUB ZE SCHOWKA	25
9. PODPISYWANIE TEKSTU	30
10. ODCZYTANIE ZASZYFROWANEGO TEKSTU Z OKNA LUB ZE SCHOWKA	31
11. GENEROWANIE PARY KLUCZY.....	34
12. SPIS RYSUNKÓW, WYJAŚNIENIE NIEKTÓRYCH ZAPISÓW	40

1. Przechowywanie i ochrona kluczy.

Informację o tym gdzie są przechowywane klucze: prywatny oraz publiczny można uzyskać w następujący sposób:

- Uruchomić program PGPkeys: **Start->Programy->PGP->PGPkeys**. Wynikiem wykonania tej czynności będzie pojawienie się okna podobnego do okna przedstawionego na rysunku 1.
- Wyświetlić okno opcji programu PGPkeys: **Edit->Options**. Wynikiem wykonania tej czynności będzie pojawienie się okna podobnego do okna przedstawionego na rysunku 2.
- Wybrać zakładkę **Files**. Wynikiem wykonania tej czynności będzie pojawienie się w oknie PGP Options informacji dotyczących miejsca przechowywania kluczy. (Rysunek 3)

Edit->Options



Rysunek 1 Okno główne programu PGKkeys

W oknie przedstawionym na rysunku 3 są przedstawione informacje dotyczące lokalizacji plików, w których są zapisane klucze. Okno zawiera trzy grupy informacji:

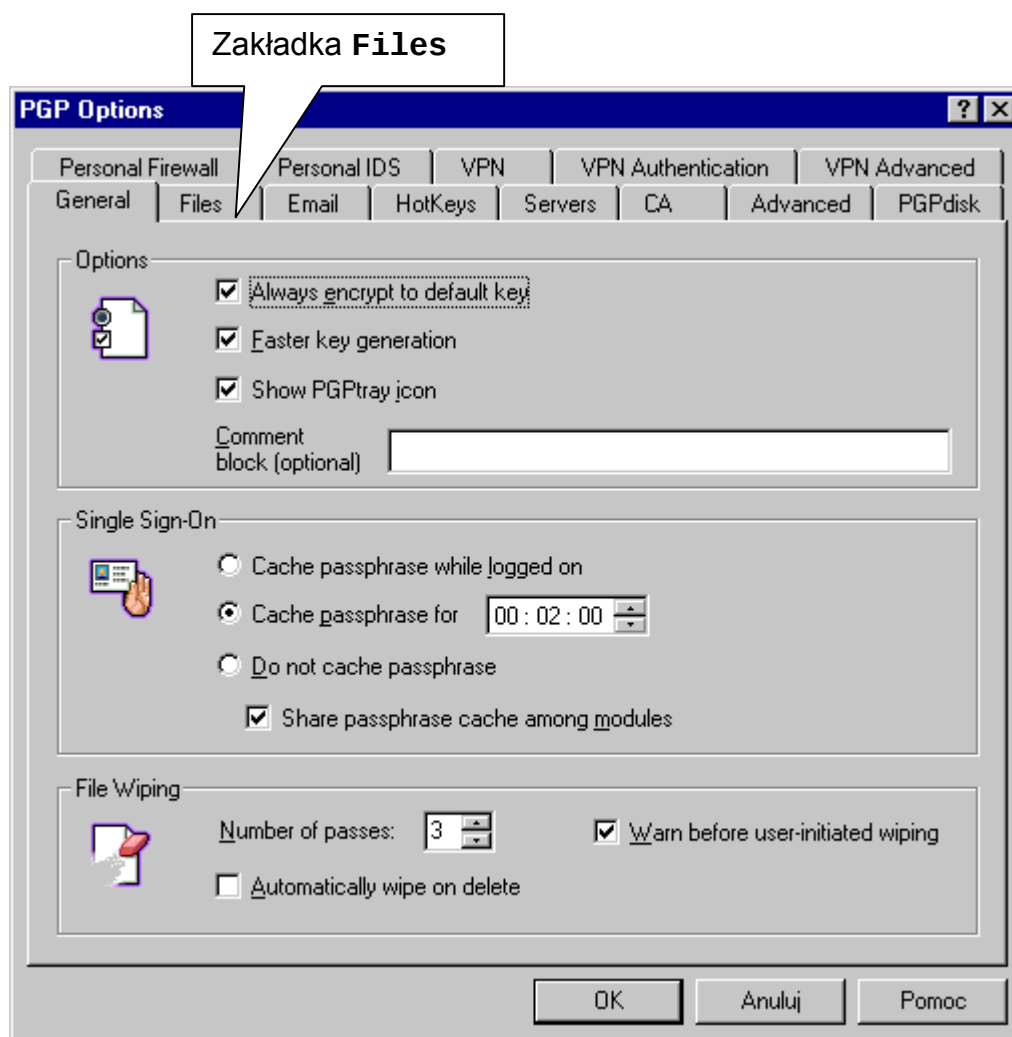
- PGP Keyring Files
 - Public Keyring File – okienko edycyjne zawierające lokalizację i nazwę pliku, w którym są przechowywane informacje o kluczu publicznym. Jeżeli użytkownik zamierza zmienić nazwę pliku lub jego lokalizację powinien uaktualnić te informacje w tym okienku edycyjnym. Aby zmienić informacje dotyczące lokalizacji klucza publicznego należy wprowadzić ścieżkę do pliku zawierającego informacje o kluczu publicznym lub zlokalizować ten plik poprzez kliknięcie przycisku **Browse**.
 - Private Keyring File – okienko edycyjne zawierające lokalizację i nazwę pliku, w którym są przechowywane informacje o kluczu prywatnym. Jeżeli użytkownik zamierza zmienić nazwę pliku lub jego lokalizację powinien uaktualnić te informacje w tym okienku edycyjnym. Niektórzy użytkownicy dla lepszej ochrony swego pliku z informacją o kluczu prywatnym przechowują ten plik na dyskiecie, której używają wtedy, gdy zachodzi potrzeba użycia podpisu (sign) lub odszyfrowania wiadomości. Ta lokalizacja jest również używana do automatycznego składowania kopii klucza publicznego. Aby zmienić informacje dotyczące lokalizacji klucza prywatnego należy wprowadzić ścieżkę do pliku zawierającego informację o kluczu

prywatnym lub zlokalizować ten plik poprzez kliknięcie przycisku **Browse**.

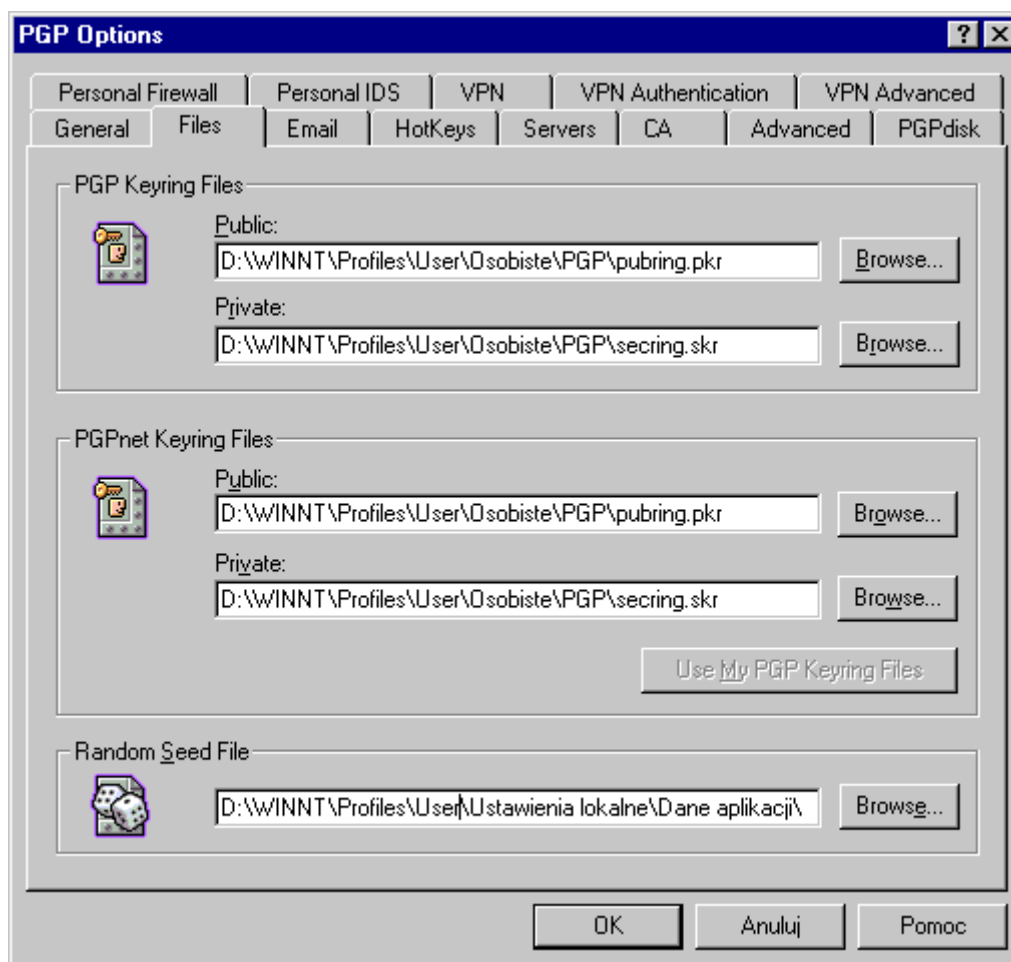
- PGPnet Keying Files
- Random Seed file

W celu dokładnego ustawienia pozostałych opcji w tym oknie należy się skontaktować z administratorem PGP.

Pliki zawierające informacje o kluczu prywatnym i publicznym należy chronić przed niepowołanym dostępem. Należy też utworzyć kopie zapasowe tych plików, aby w ten sposób zapobiec utracie kluczy w wyniku awarii dysku itp.



Rysunek 2 Okno główne opcji programu PGPkeys



Rysunek 3 Okno zawierające informacje o położeniu kluczy

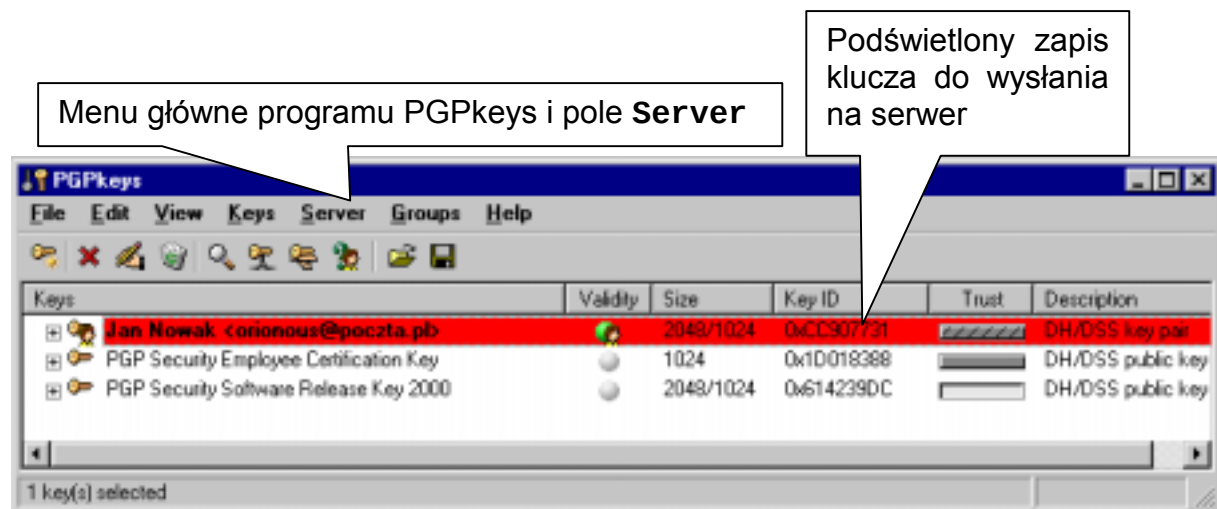
2. Udostępnianie własnego klucza publicznego innym użytkownikom.

Aby użytkownik mógł odbierać zaszyfrowane wiadomości od innych użytkowników musi im udostępnić swój klucz publiczny. Można to zrobić na kilka sposobów:

- 1) poprzez wysłanie swego klucza publicznego na serwerze kluczy;
- 2) poprzez dołączenie swego klucza publicznego do poczty elektronicznej;
- 3) poprzez wyeksportowanie swego klucza publicznego lub skopiowanie go do pliku i dołączenie do poczty.

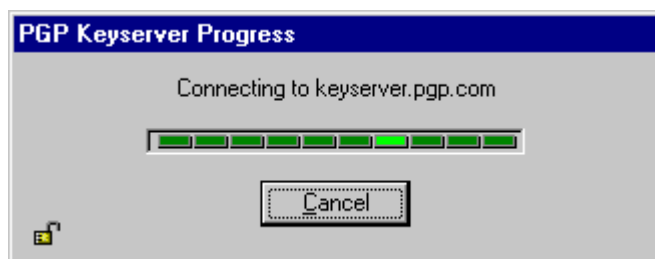
1) Aby wysłać własny klucz publiczny na serwer kluczy należy postępować według poniższych wskazówek:

- Podłączyć komputer do internetu;
- Uruchomić program PGPkeys: **Start ->Programy ->PGP ->PGPkeys;**
- W oknie edycyjnym programu podświetlić zapis reprezentujący własny klucz publiczny, który użytkownik chce umieścić na serwerze kluczy.

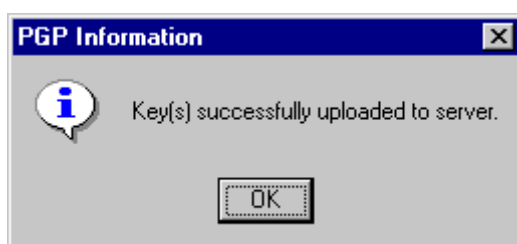


Rysunek 4 Okno zawierające informacje o położeniu kluczy

- Z menu głównym programu PGPkeys wybrać pole **Server**, a w podmenu pole **Send To**, czyli **Server->Sent To->wybrać_serwer_kluczy**. Wybranie serwera kluczy spowoduje wyświetlenie się okna przedstawionego na rysunku 4;
- Jeżeli klucz został pomyślnie dodany to wyświetli się okno informujące użytkownika o pomyślnym zakończeniu operacji. Klucz publiczny użytkownika jest udostępniony na serwerze kluczy (Rysunek 6).



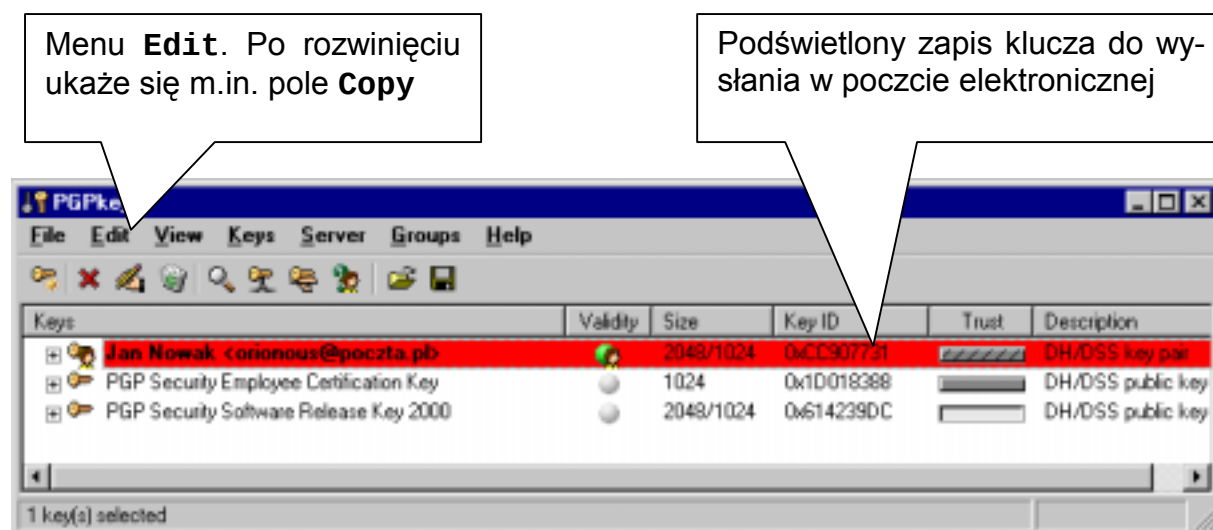
Rysunek 5 Okno informujące o tym, że trwa proces połączenia z serwerem kluczy



Rysunek 6 Okno informujące o umieszczeniu klucza na serwerze kluczy

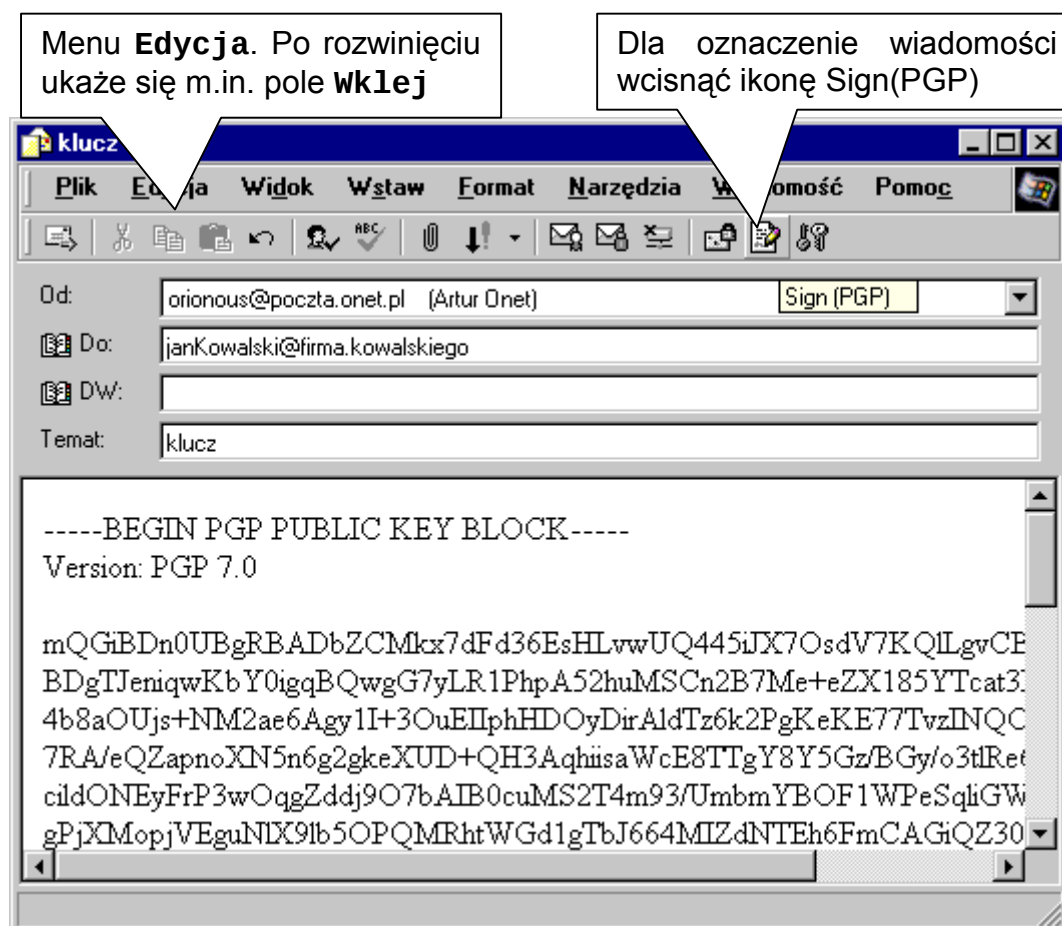
2) Aby wysłać swój klucz publiczny do innego użytkownika za pomocą poczty elektronicznej należy postępować według poniższych wskazówek:

- Uruchomić program PGPkeys: **Start->Programy->PGP->PGPkeys**;
- W oknie edycyjnym zaznaczyć zapis dotyczący własnej pary kluczy;
- Wybrać pole **Copy** z menu, które się rozwinie po wciśnięciu pola **Edit** z menu głównego programu PGPkeys: **Edit->Copy**.

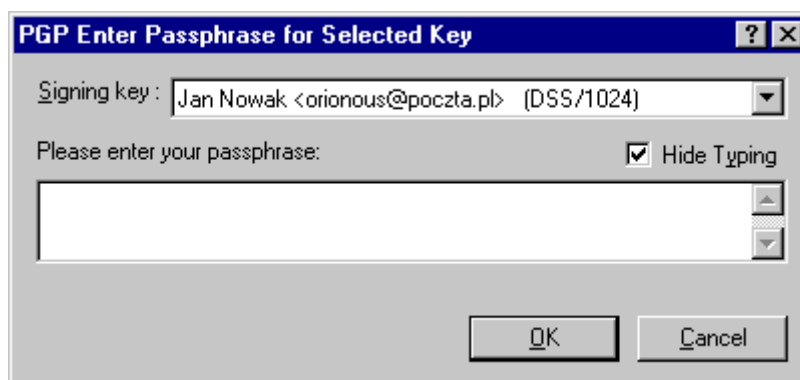


Rysunek 7 Okno PGPkeys w przypadku kopiowania klucza

- Uruchomić program Outlook Express, wpisać adresata i temat wiadomości. Następnie umieścić kursor w miejscu wpisywania treści wiadomości i wybrać pole **wklej** z Menu **Edycja** programu pocztowego: **Edycja->wklej**.
- Wskazane jest oznaczenie wiadomości. Pozwoli to adresatowi zweryfikować nadawcę – wcisnąć ikonę **Sign(PGP)** przed wysłaniem wiadomości.(Rysunek 8)
- Wysłać wiadomość. Jeżeli oznaczono wiadomość podać hasło. (Rysunek 9)



Rysunek 8 Okno Outlook Express w przypadku wysyłania klucza publicznego

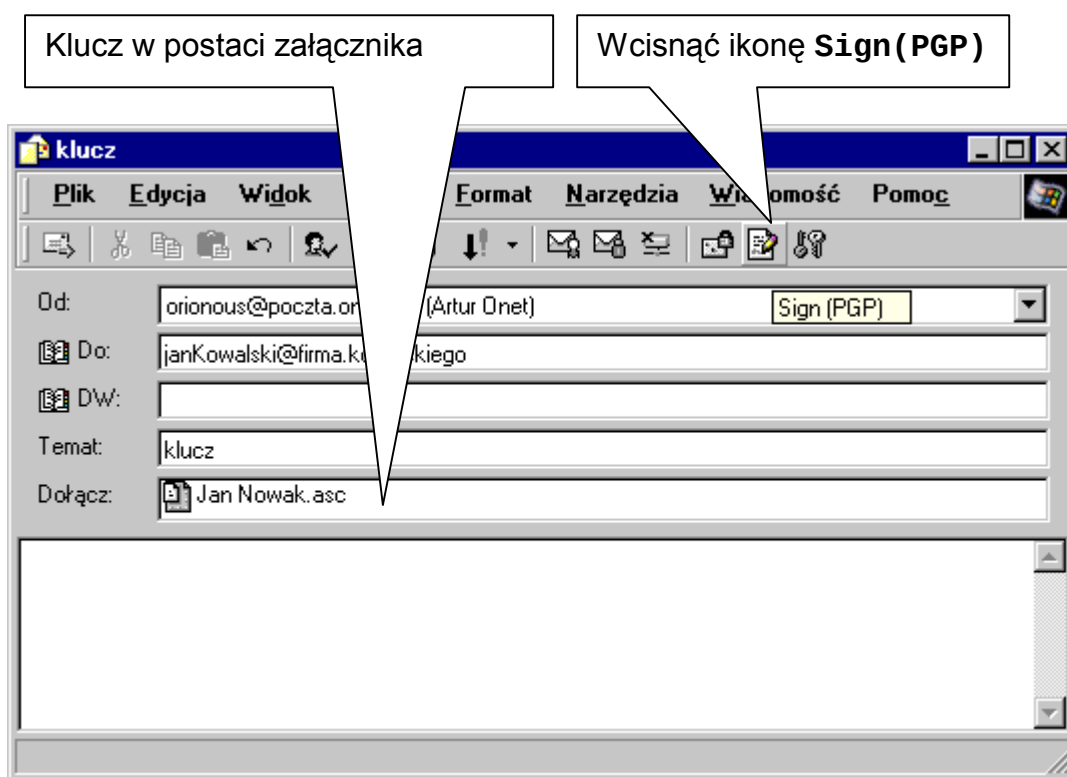


Rysunek 9 Okno do wpisania hasła dla podanego klucza

Można też przeciągnąć zaznaczony opis klucza przedstawiony na rysunku 7 do okna przedstawionego na rysunku 8. Wtedy klucz zostanie wysłany w postaci załącznika. Inne czynności przeprowadzić analogicznie. Wcześniej należy wyeksportować klucz publiczny do pliku, tzn.

wybrać klucz i za pomocą menu **Keys** przejść do pola **Export: Keys->Export**(patrz podpunkt 3) Podać nazwę pliku. Czynności do wykonania:

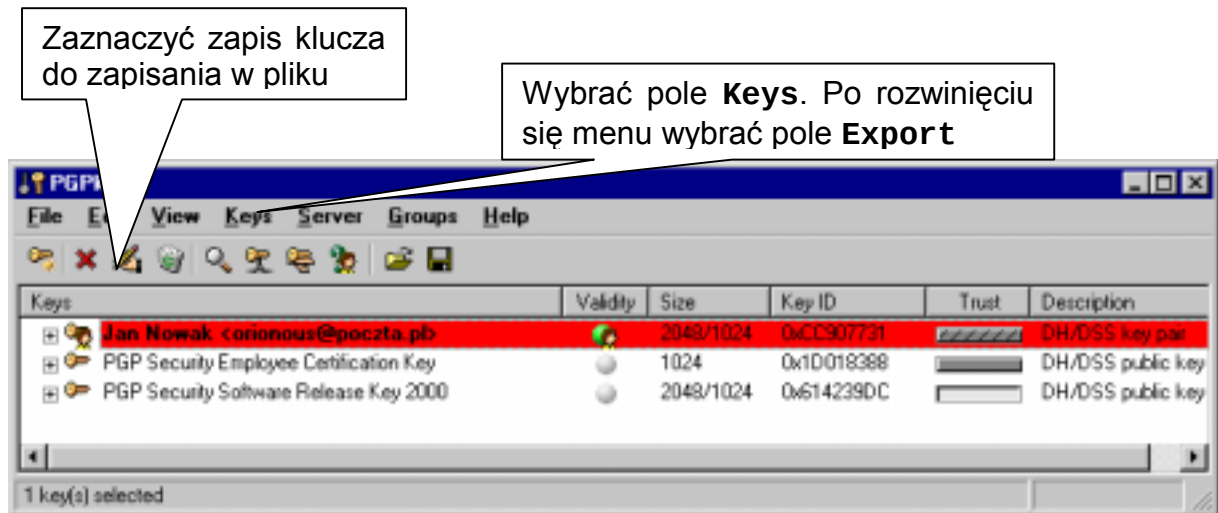
- Uruchomić program PGPkeys;
- Uruchomić Outlook Express i utworzyć nową wiadomość;
- Rozmieszczyć oba okna na ekranie monitora, tak aby były widoczne;
- W oknie PGPkeys:
 - o Zaznaczyć klucz do wysłania;
 - o Wskazać ten klucz kursorem myszki, nacisnąć lewy przycisk myszy;
 - o Nie zwalniając lewego przycisku myszki przeciągnąć klucz do okna Outlook Express;
 - o W okienku edycyjnym dla załączników pojawi się napis postaci nazwa.asc (Rysunek 10);
- Oznaczyć wiadomość;
- Wysłać. Podać hasło przypisane do klucza (Rysunki: 8, 9);



Rysunek 10 Okno Outlook Express przy wysyłaniu klucza po przeciągnięciu go z okna PGPkeys

3) Aby wyeksportować lub skopiować do pliku klucz publiczny i wysłać go w postaci załącznika do poczty należy postępować według poniższych wskazówek:

- Uruchomić program PGPkeys: **Start ->Programy->PGP->PGPkeys**;
- Zaznaczyć zapis reprezentujący klucz umieszczony w oknie programu PGPkeys, a następnie wybrać pole **Export** z menu **Keys Keys->Export** ;
- Podać lokalizację i zapisać klucz przy pomocy okna dialogowego, które się pojawi po wykonaniu kroku poprzedniego.
- Wysłać klucz publiczny w postaci załącznika do poczty.



Rysunek 11 Okno PGPkeys z opisem do wyeksportowania klucza do pliku

Istnieje też możliwość skopiowania klucza do pliku tekstowego. W tym celu należy:

- Skopiować klucz (Rysunek 7);
- Utworzyć plik tekstowy;
- Wkleić skopiowany klucz do pliku tekstowego:
 - o Ustawić kursor w oknie utworzonego pliku tekstowego;
 - o Wcisnąć kombinację **Edycja->wklej** w oknie edytora utworzonego pliku;
 - o Zapisać plik z rozszerzeniem *.txt.

Tak zapisany klucz może być wysłany jako plik załączony do wiadomości pocztowej.

3. Pobieranie kluczy publicznych innych użytkowników.

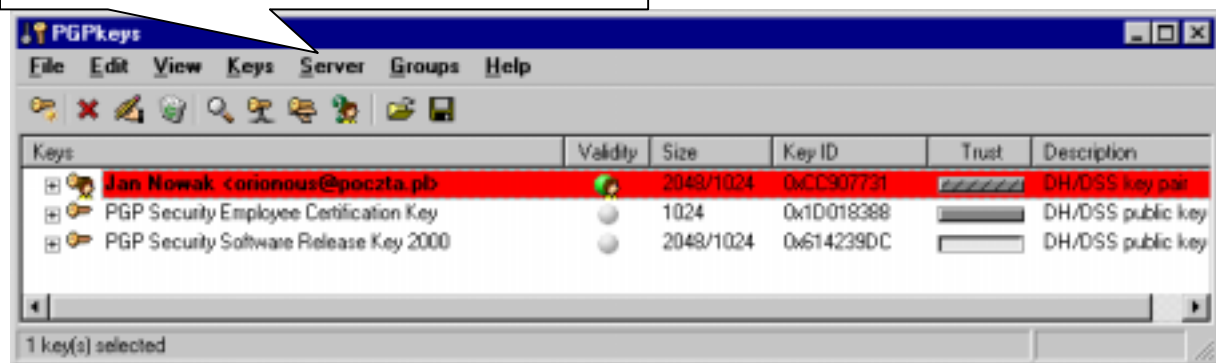
W celu wymiany zaszyfrowanych informacji pomiędzy użytkownikami, konieczne jest posiadanie kluczy publicznych adresatów przesyłek pocztowych. Klucz publiczny innego użytkownika można uzyskać poprzez:

- 1) pobranie klucza danego użytkownika z serwera kluczy;
- 2) pobranie klucza z wiadomości pocztowej przysłanej przez użytkownika udostępniającego klucz publiczny;
- 3) pobranie klucza z pliku udostępnionego przez użytkownika udostępniającego klucz publiczny.

1) Aby pobrać klucz publiczny danego użytkownika z serwera kluczy należy postępować według poniższych wskazówek:

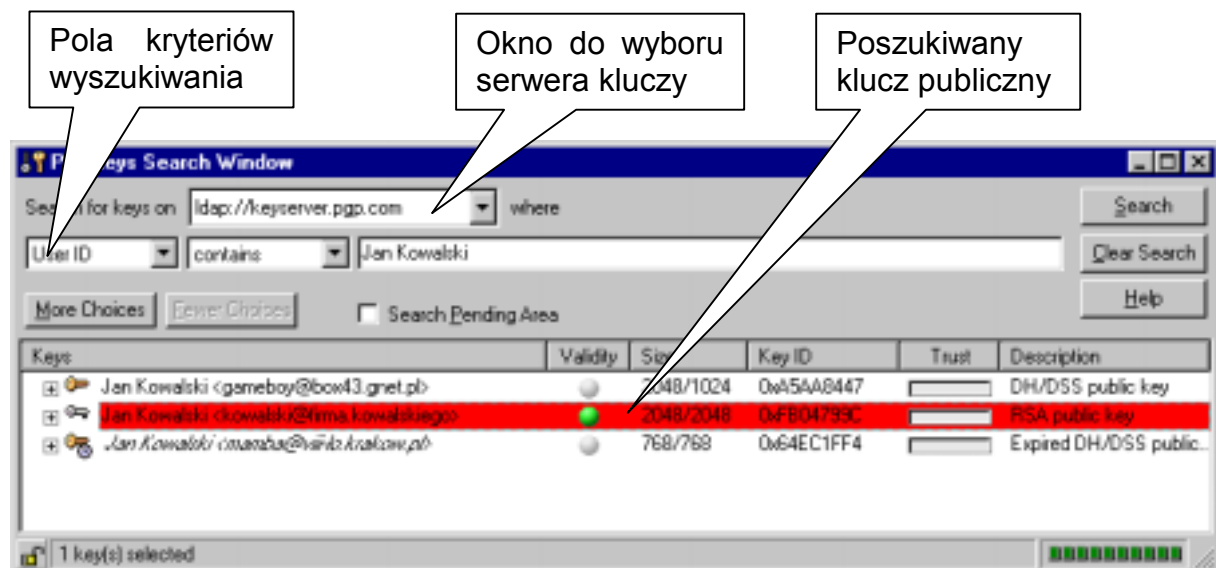
- Uruchomić program PGPkeys : **Start->Programy->PGP->PGPkeys**;
- Kliknąć na pole **Search** z menu **Server: Server->Search** (Rysunek 12);

Z menu **Server** wybrać pole **Search**

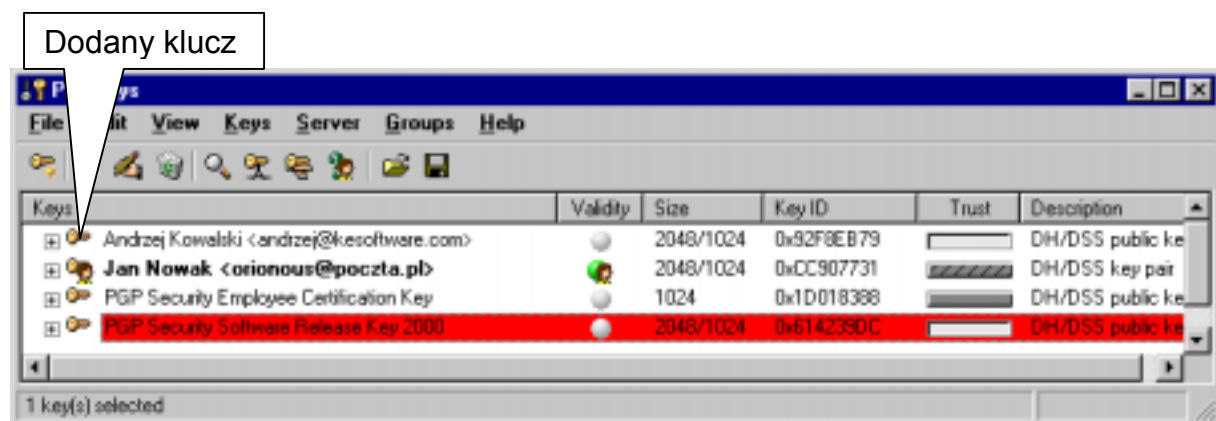


Rysunek 12 Okno PGPkeys i opis do wyboru serwera w celu pobrania klucza

- Po otwarciu okna dialogowego **Search** w polu **Search for Keys On** wybrać lokalizację lub serwer, na którym znajduje się klucz publiczny użytkownika. (Rysunek 13).
- Wprowadzić kryteria potrzebne do określenia klucza publicznego użytkownika. Jeżeli klucz został znaleziony można go przenieść do okna PGPkeys, tzn. Zaznaczyć kursorem myszki konkretny opis klucza, nacisnąć lewy przycisk myszki i nie zwalniając przycisku z lewego przycisku myszki przeciągnąć kursor myszy do okna PGPkeys.(Rysunki 13,12);
- Przeniesiony klucz pojawi się w oknie PGPkeys.



Rysunek 13 Okno do wyszukiwania klucza publicznego danego użytkownika

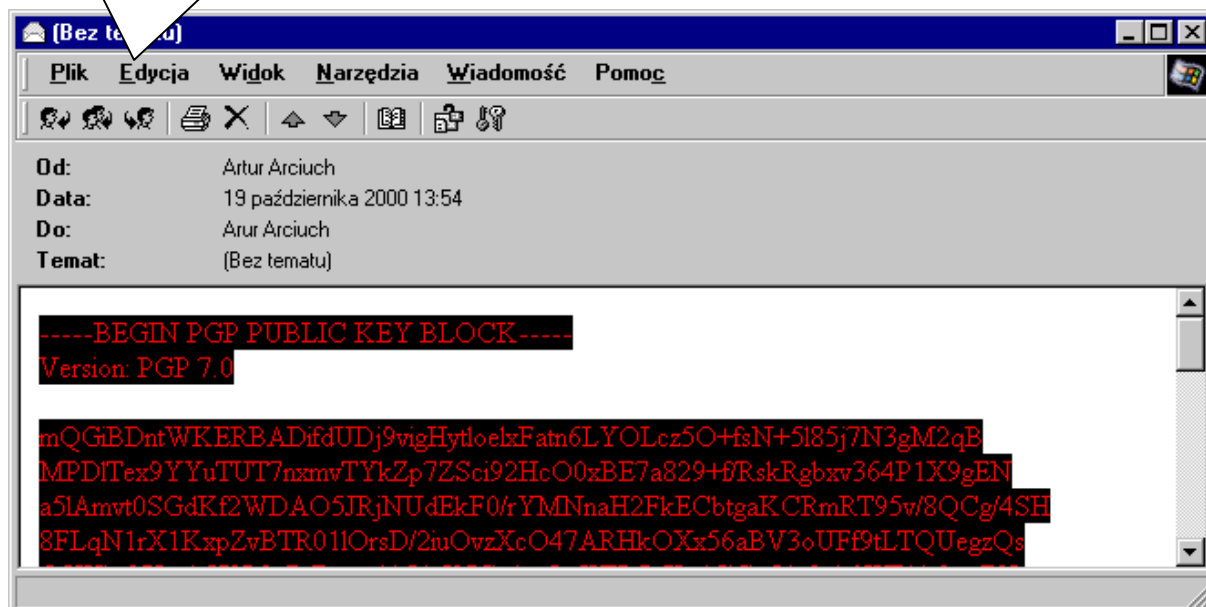


Rysunek 14 PGPkeys po dodaniu klucza publicznego użytkownika Kowalskiego

2) Aby pobrać klucz z wiadomości tekstowej należy postępować według poniższych wskazówek:

- Skopiować z okna Outlook Express obszar, który przedstawia klucz publiczny:
 - o Zaznaczyć myszką obszar klucza;
 - o W menu **Edycja** Kliknąć na pole **Kopiuj: Edycja->Kopiuj**;
 - o Wyjść z programu Outlook Express; (Rysunek 15)

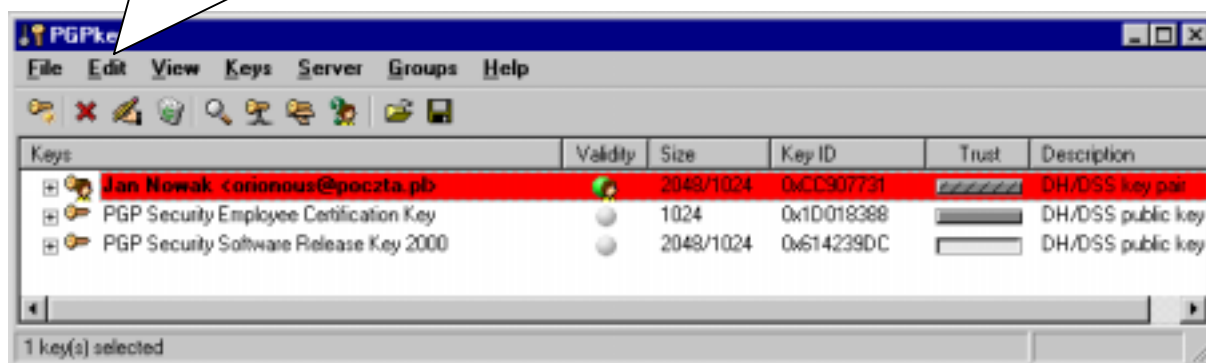
Z menu **Edycja** wybrać **Kopiuj**



Rysunek 15 Sposób skopiowania zawartości klucza publicznego z programu pocztowego

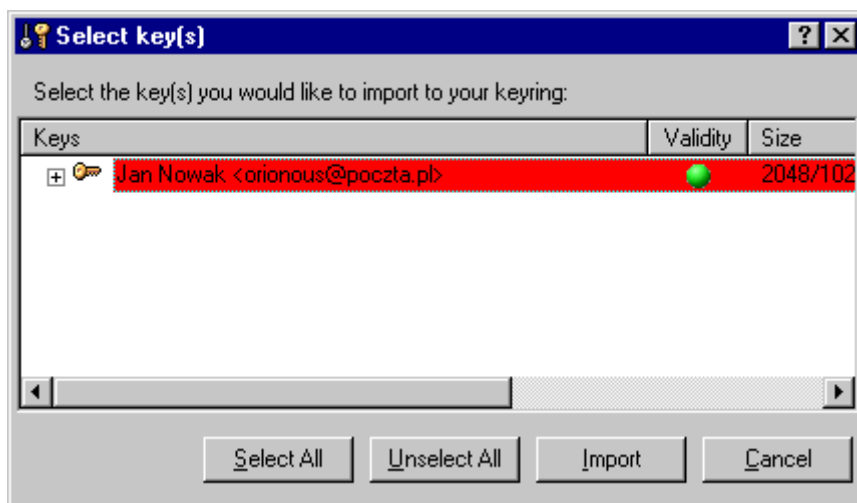
- Uruchomić program PGPkeys: **Start ->Programy->PGP->PGPkeys**
- Kliknąć na pole **Paste** z menu **Edit: Edit -> Paste**.

Wybrać **Paste** z menu **Edit**



Rysunek 16 Elementy okna PGPkeys istotne przy dodawaniu klucza

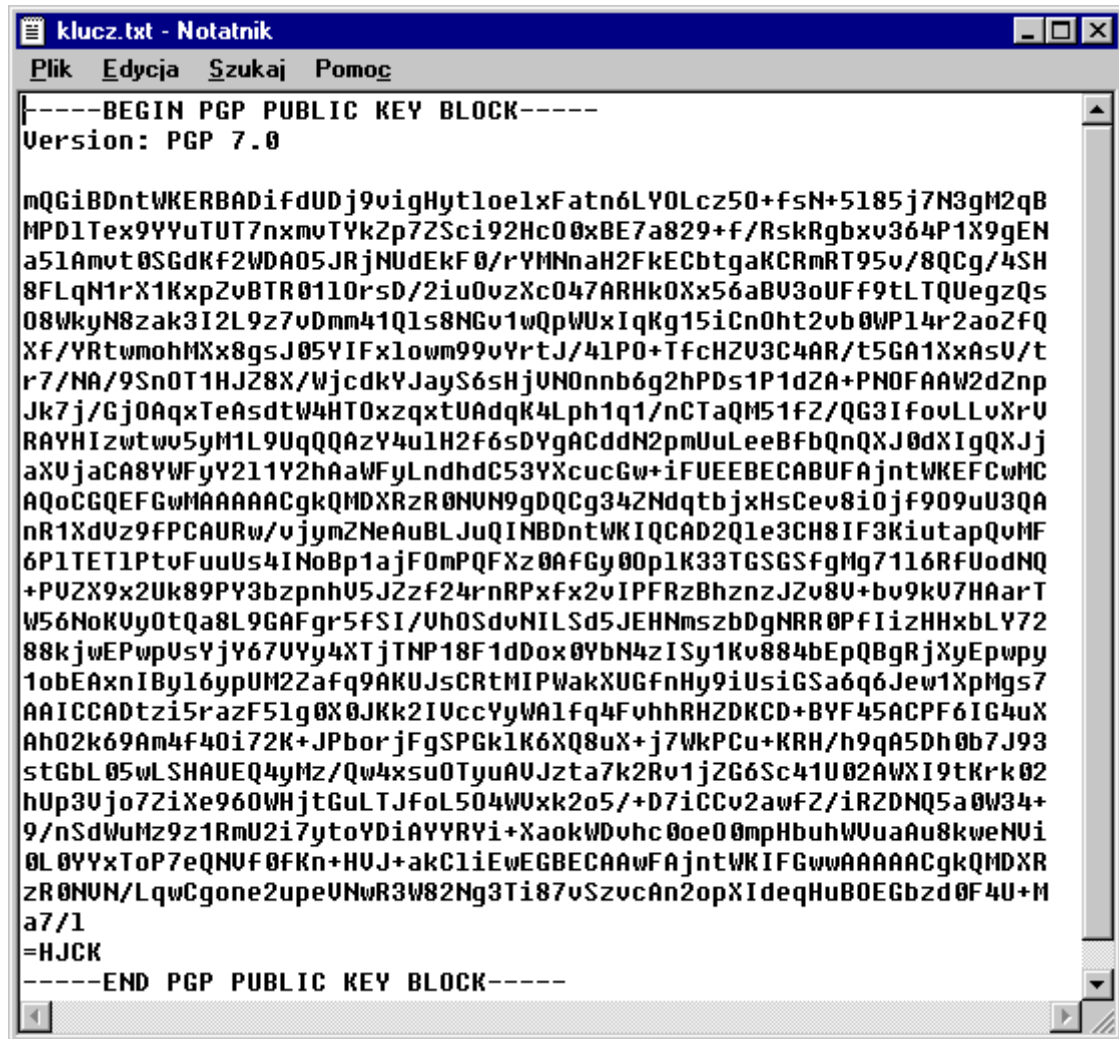
- Po ukazaniu się okna Select Key(s) Kliknąć na klucz i wcisnąć przycisk **Import**(Rysunek 17);



Rysunek 17 Okno służące do importowania klucza

- Nowy klucz pojawi się w oknie programu GPGkeys.
- 3) Aby dołączyć klucz publiczny z pliku należy postępować według poniższych wskazówek:
- Uruchomić program GPGkeys: **Start ->Programy ->PGP ->GPGkeys;**
 - Otworzyć plik zawierający klucz publiczny(Rysunek 18);
 - Zaznaczyć i skopiować blok tekstu reprezentujący klucz publiczny (korzystając z menu **Edycja** Notatnika: **Edycja->Zaznacz wszystko, Edycja->Kopiuj**);
 - Użyć pola **Paste** z menu **Edit** programu GPGkeys: **Edit->Paste**. Spowoduje to ukazanie się okna jak na rysunku 16.
 - Po ukazaniu się okna **Select Key(s)** wybrać klucz i wcisnąć przycisk **Import**(Rysunek 17);
 - Nowy klucz pojawi się w oknie programu GPGkeys.

Można też przeciągnąć plik tekstowy z kluczem do okna GPGkeys. Dalej postępować tak jak w momencie pojawienia się okna przedstawionego na rysunku 17.



```

klucz.txt - Notatnik
Plik  Edycja  Szukaj  Pomoc

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 7.0

mQGIBDntWKERBADiFdUDj9vigHytloelxFatn6LY0Lcz50+fsN+5185j7N3gM2qB
MPD1Tex9YYuTUT7nxmvTYkZp7ZSci92Hc00xBE7a829+f/RskRgxbv364P1X9gEN
a51Amvt0SGdKF2WDA05JRjNUdEkF0/rYMNnaH2FkECbtgaKCRmRT95v/8QCg/4SH
8FLqN1rX1KxpZvBTR0110rsD/2iu0vzXc047ARHk0Xx56aBU3oUFF9tLTQUegzQs
08WkyN8zak3I2L9z7vDmm41Q1s8NGv1wQpWUxIQKg15iCn0ht2vb0WP14r2aoZfQ
XF/YRtwmohMXx8gsJ05YIFxlowm99vYrtJ/41P0+TfCHZU3C4AR/t5GA1XxAsU/t
r7/NA/9Sn0T1HJZ8X/WjcdkYJayS6sHjVN0nnb6g2hPDs1P1dZA+PN0FAAW2dZnp
Jk7j/Gj0AqxTeAsdtW4HT0xzqxUAdqK4Lph1q1/nCTaQM51fZ/QG3IfovLLvXrU
RAYHIzwtwv5yM1L9UqQAZy4u1H2f6sDYgACddN2pmUuLeeBfbQnQXJ0dXIgQXJj
aXUjaCA8YWFyY211Y2hAaWYyLndhdC53YXcucGw+ifUEEBECABUFAjntWKEFCwMC
AQoCGQEFgwMAAAACgkQMDXRzR0NUN9gDQCg34ZNdqtbjxHsCev8i0jf909uU3QA
nR1XdUz9FPCAURw/vjymZNeAuBLJuQINBDntWKIQCAD2Qle3CH8IF3KiutapQvMF
6P1TET1PtFuuUs4INoBp1ajF0mPQFXz0AFgy00p1K33TGSgSfgMg7116RFUodNQ
+PUZX9x2Uk89PY3bznphU5JZzF24rnRPxfx2vIPFRzBhzJZv8U+bu9kU7HAarT
W56NoKvU0tQa8L9GAFgr5FSI/Vh0SdvNILSd5JEHNmszbDgNRR0PFiizHHxbLY72
88kjwEPwU5YjY67VYy4XTjTNP18F1dDox0YbN4zISy1Kv884bEpQBGRjXyEpwpy
1obEAXnIByl6ypUM2Zafq9AKUJsCRtMIPWakXUGfnHy9iUsiGSa6q6Jew1XpMgs7
AAICCADtzi5razF5lg0X0JKk2IvccYyWAlfq4FvhhRH2DKCD+BYF45ACPF6IG4uX
Ah02k69Am4f40i72K+JPborjFgSPGk1K6XQ8uX+j7WkPCu+KRH/h9qA5Dh0b7J93
stGbL05wLSHAUEQ4yMz/Qw4xsu0TyuAVJzta7k2Rv1jZG6Sc41U02AWX19tKrK02
hUp3Ujo7ZiXe960WHjtGuLTJfoL504WUxk2o5/+D7iCCv2awfZ/iR2DNQ5a0W34+
9/nSdWuMz9z1RmU2i7ytoYDiAYRYi+XaokWDvhc0oe00mpHbuhWUuaAu8kweNui
0L0YYxToP7eQNUF0FKn+HUVJ+akC1iEwEGBECAAWFAjntWKIFGwAAAAACgkQMDXR
zR0NUN/LqwCgone2upeUNwR3W82Ng3Ti87vSzvCAn2opXIdeqHuB0EGbzd0F4U+M
a7/1
=HJCK
-----END PGP PUBLIC KEY BLOCK-----

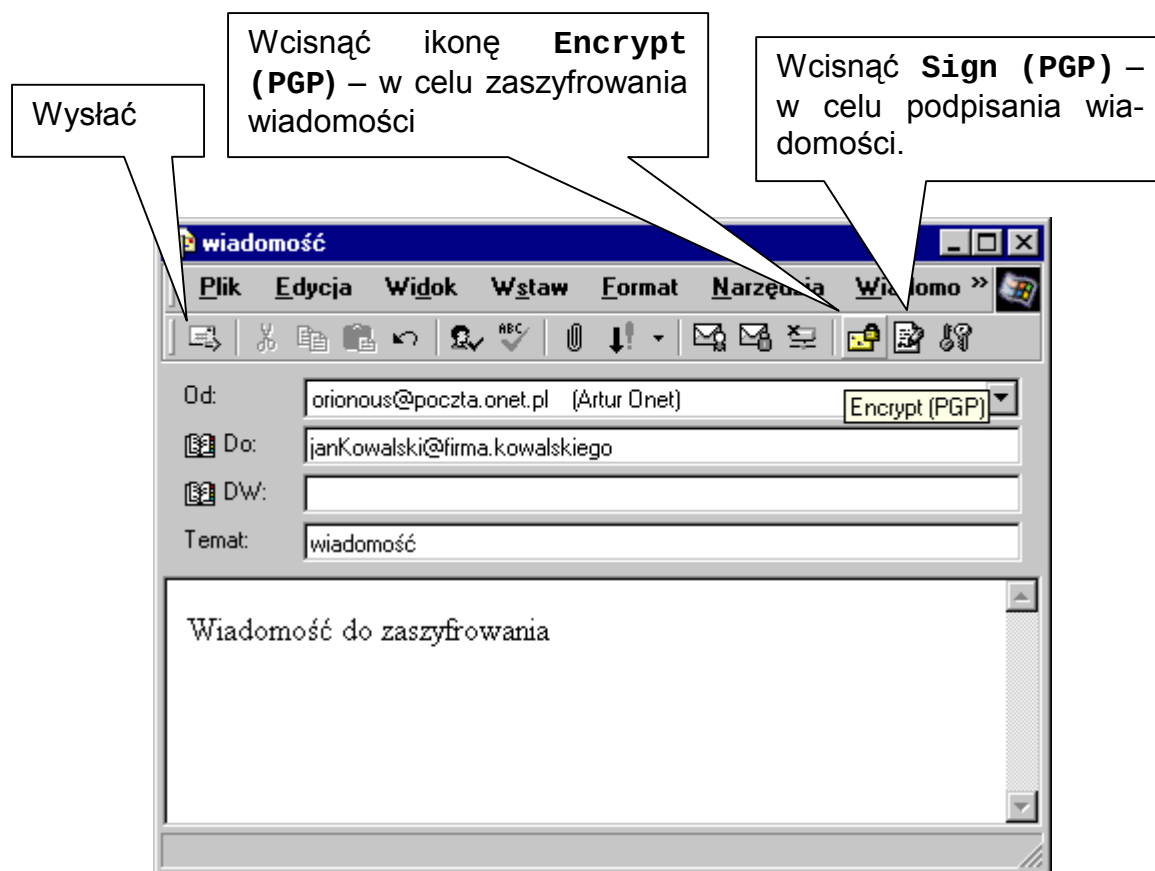
```

Rysunek 18 Klucz publiczny w pliku tekstowym

4. Wysyłanie zaszyfrowanych wiadomości pocztowych

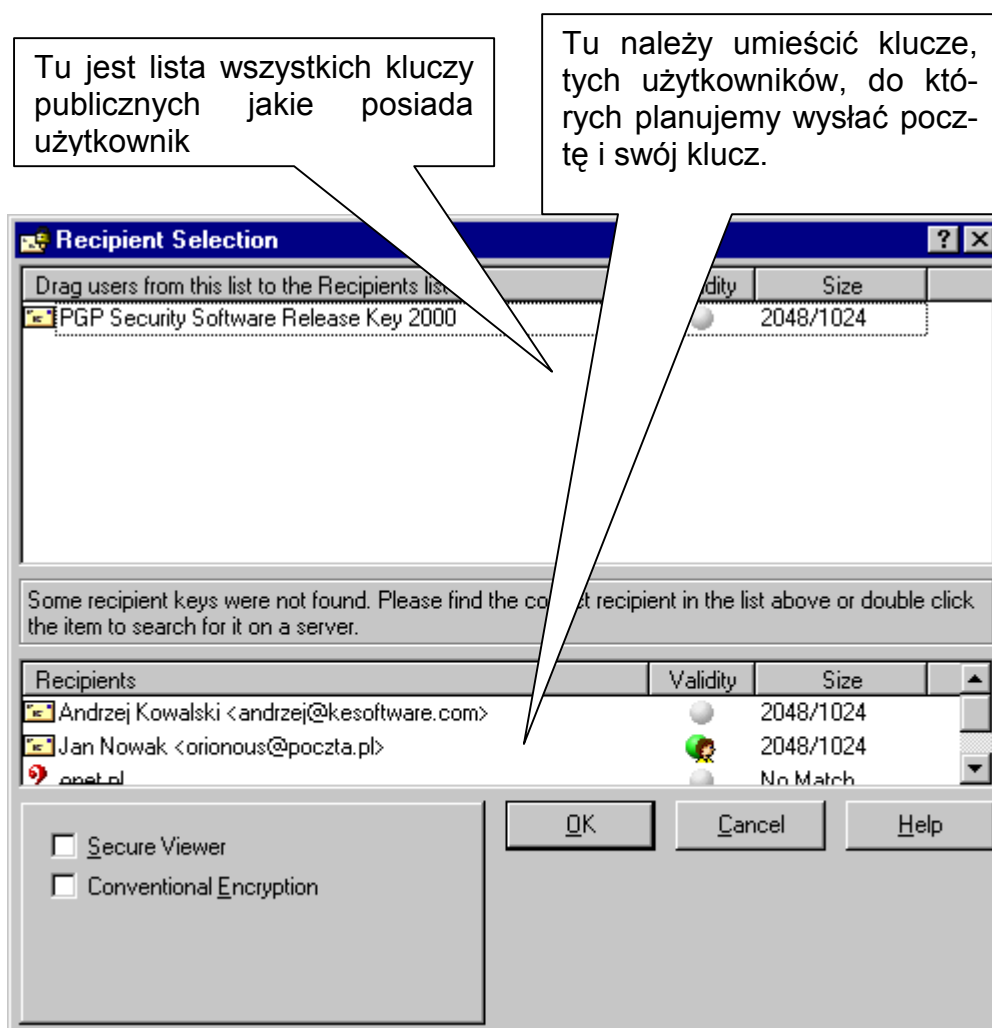
Aby wysłać zaszyfrowaną wiadomość do wybranego użytkownika przy użyciu programu Outlook Express należy postępować według poniższych wskazówek:

- Pobrać klucz publiczny adresata wiadomości (sposób pobierania klucza publicznego danego użytkownika opisano w rozdziale 3 instrukcji);
- Uruchomić program Outlook Express;
- Wypełnić pola nadawcy, adresata, tematu wiadomości;
- Wpisać wiadomość;
- Wcisnąć ikony **Encrypt (PGP)** – w celu zaszyfrowania wiadomości i ikonę **Sign (PGP)** – w celu podpisania wiadomości. (Rysunek 19)



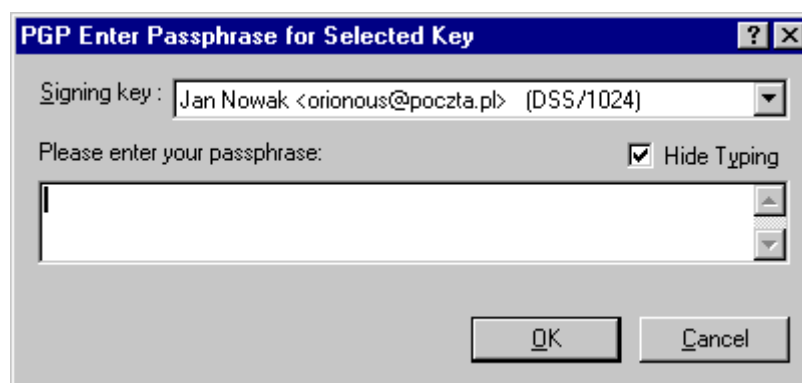
Rysunek 19 Sposób wysłania zakodowanej wiadomości

- Wysłać wiadomość. Po tej czynności ukaze się okno w którym tak jak na rysunku 20. Należy wybrać jakimi kluczami publicznymi zakodować wiadomość;



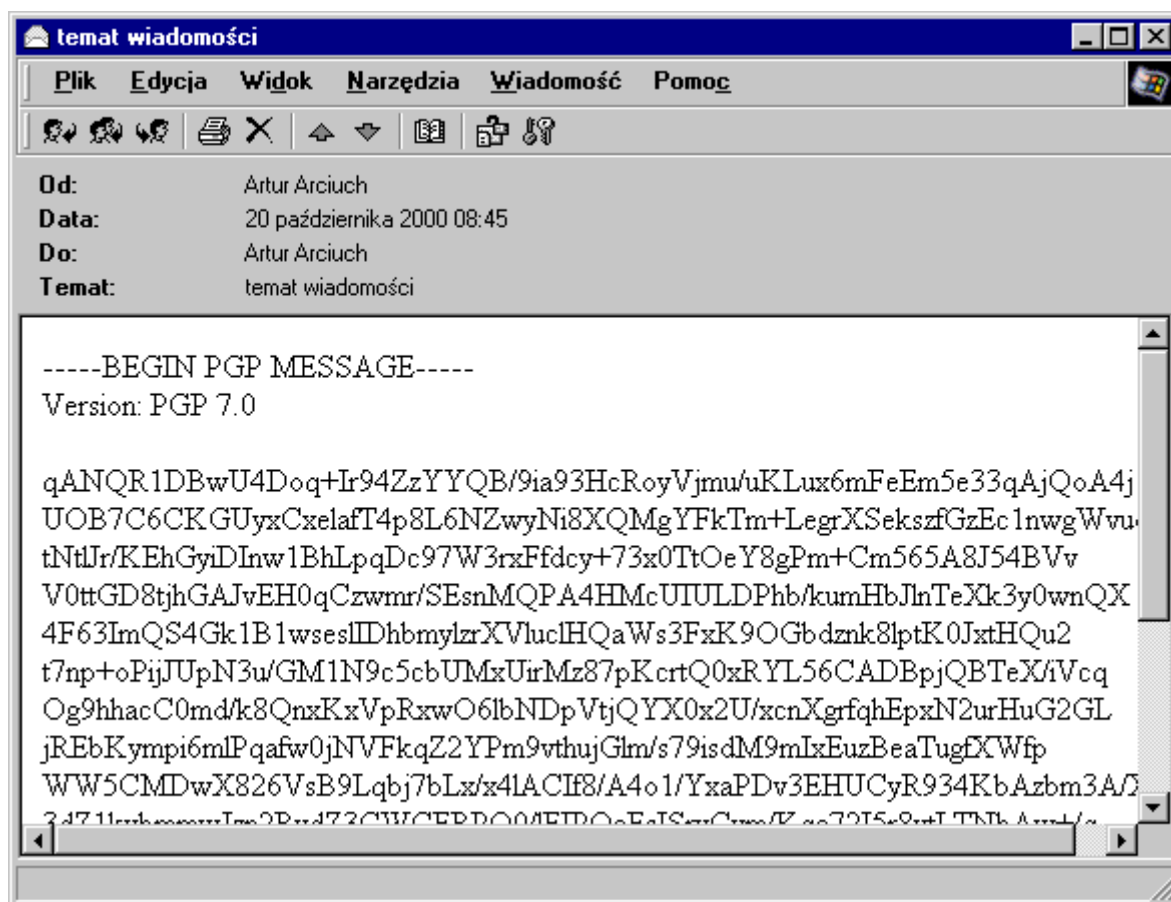
Rysunek 20 Wybór kluczy publicznych adresatów poczty

- Teraz trzeba podać hasło (Rysunek 21).



Rysunek 21 Okno do wpisania hasła

- Następnie wiadomość zostanie zaszyfrowana i wysłana. Rysunek 22 przedstawia zaszyfrowaną wiadomość po stronie odbiorcy.

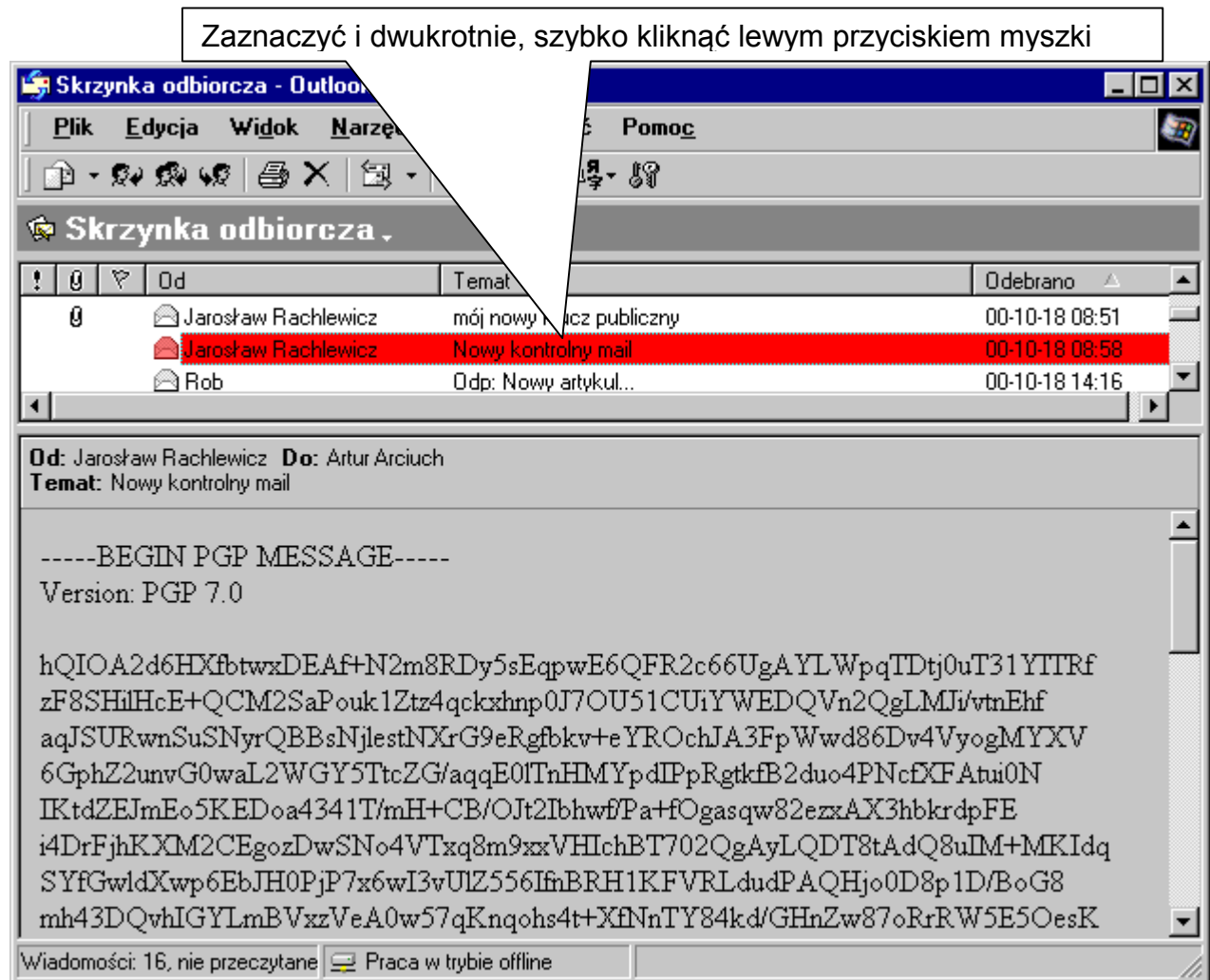


Rysunek 22 Zaszyfrowana wiadomość po stronie adresata

5. Odczytywanie odebranych zaszyfrowanych wiadomości pocztowych

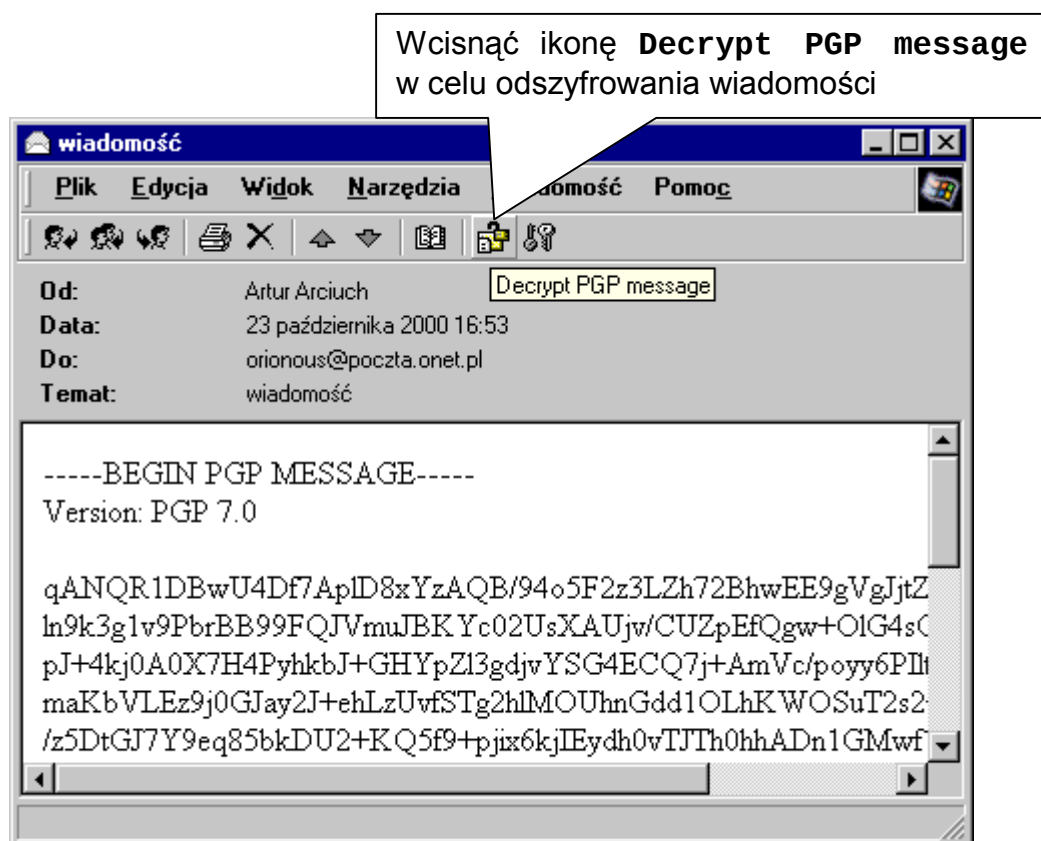
Aby odszyfrować zaszyfrowaną wiadomość pocztową należy postępować według poniższych wskazówek:

- Uruchomić program Outlook Express w oknie „Skrzynka odbiorcza”;
- Zaznaczyć wiadomość do odszyfrowania i dwukrotnie kliknąć lewym przyciskiem myszki (Rysunek 23).

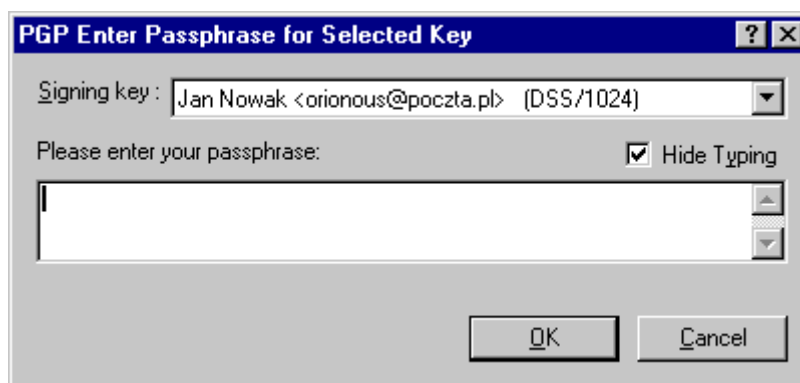


Rysunek 23 Widok zaszyfrowanej wiadomości w oknie Skrzynka odbiorcza Outlook Express

- W oknie które się pojawi wcisnąć ikony **Decrypt PGP message** – w celu odszyfrowania (Rysunek 24);
- Gdy pokaże się okno jak na rysunku 25 – podać hasło;

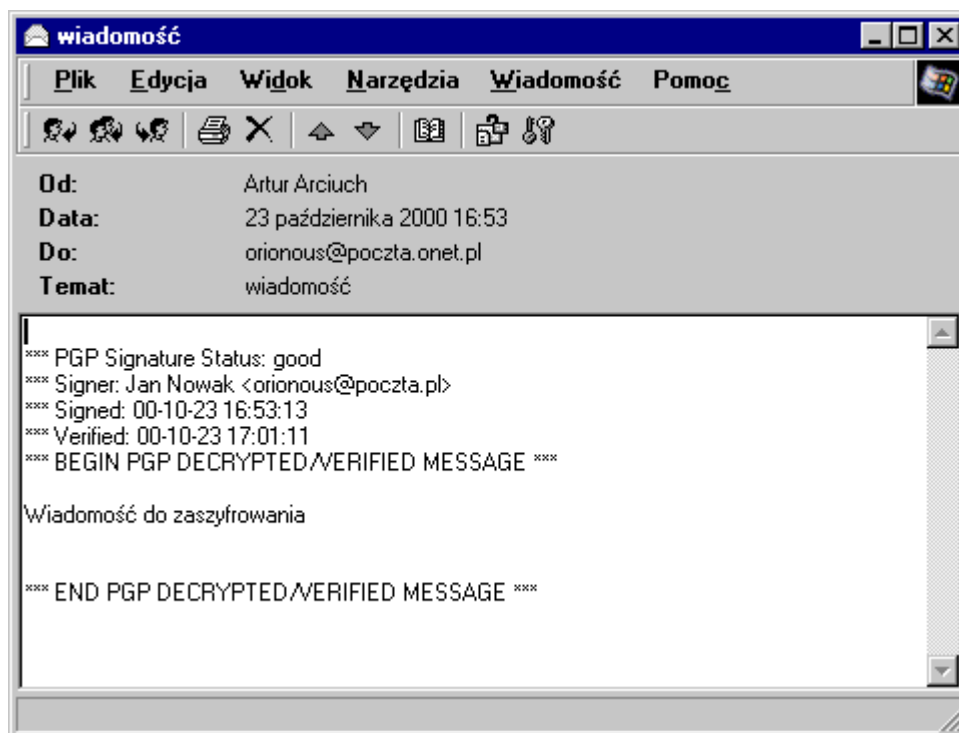


Rysunek 24 Okno Outlook Express do odszyfrowania wiadomości



Rysunek 25 Okno do wpisania hasła

- Okno z odszyfrowaną wiadomością wygląda jak na rysunku 26:

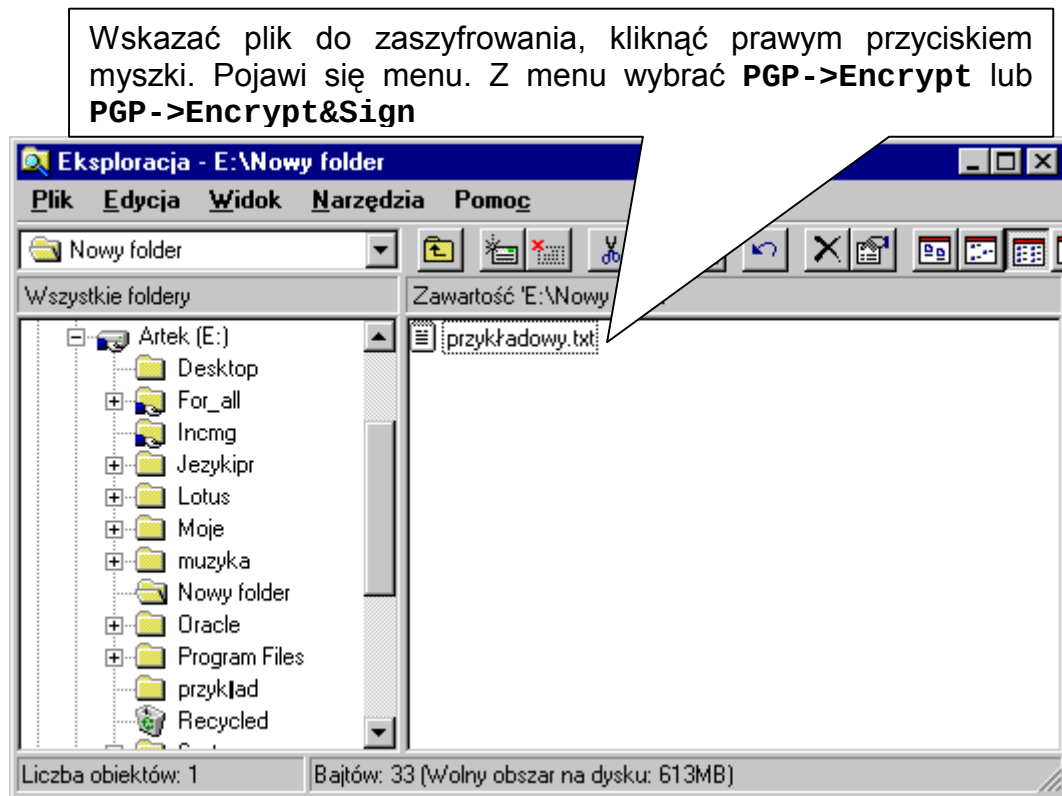


Rysunek 26 Okno z rozszyfrowaną wiadomością

6. Szyfrowanie plików

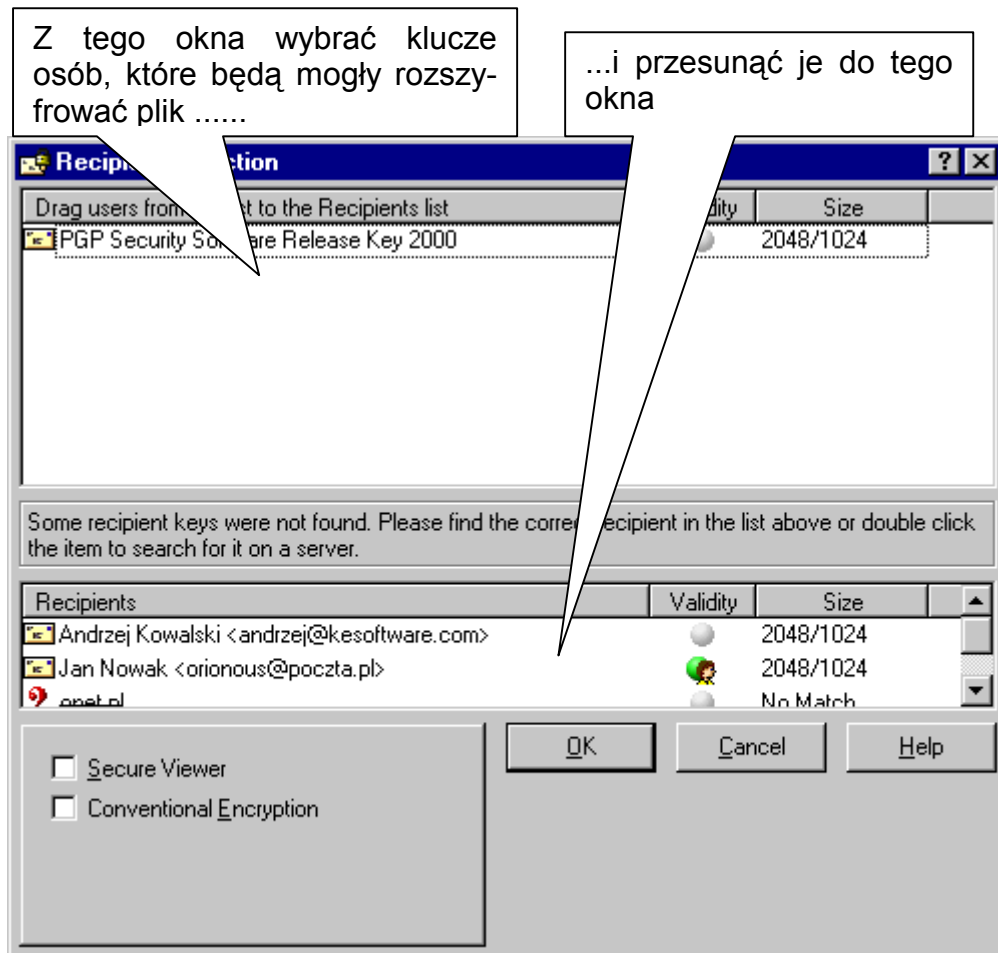
Aby zaszyfrować plik należy postępować według poniższych wskazówek:

- Uruchomić Explorator Windows NT: **Start -> Programy -> Explorator Windows NT**. Wskazać plik do zaszyfrowania (Rysunek 27);
- Wskazać kursorem myszki plik i kliknąć prawym przyciskiem myszki. Pojawi się menu. Z menu wybrać **PGP -> Encrypt** lub **PGP -> Encrypt&Sign**

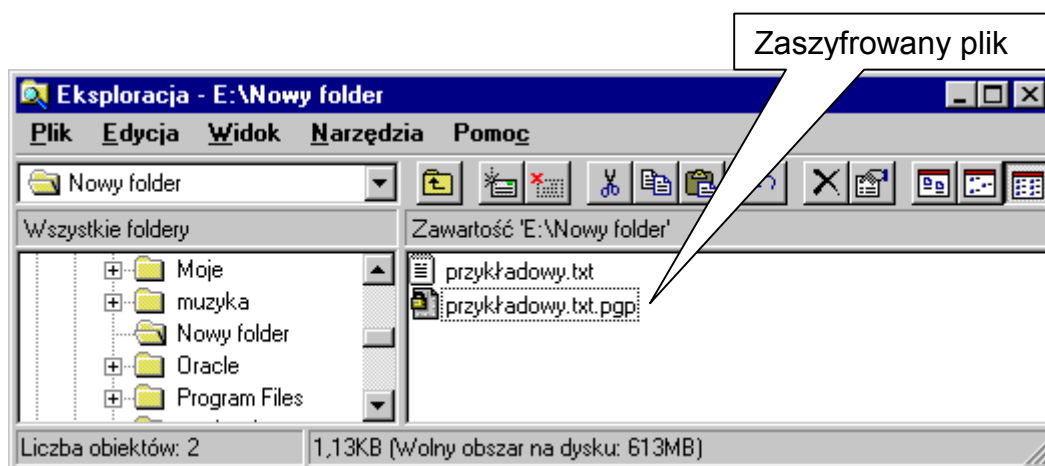


Rysunek 27 Okno Eksploratora Windows NT, z wybranym do zaszyfrowania plikiem

- Pokaże się okno jak na rysunku 28. Wybrać klucze publiczne, którymi użytkownik chce zaszyfrować plik.
- Podać hasło w oknie jak na rysunku 25.
- Zaszyfrowany plik jest umieszczony w bieżącym katalogu; (Rysunek 29)



Rysunek 28 Okno do wyboru osób uprawnionych do rozszyfrowania pliku

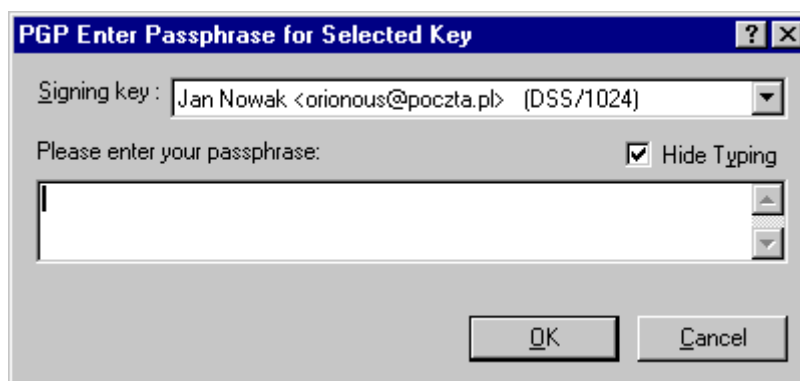


Rysunek 29 Widok zaszyfrowanego pliku

7. Odczytywanie zaszyfrowanych plików

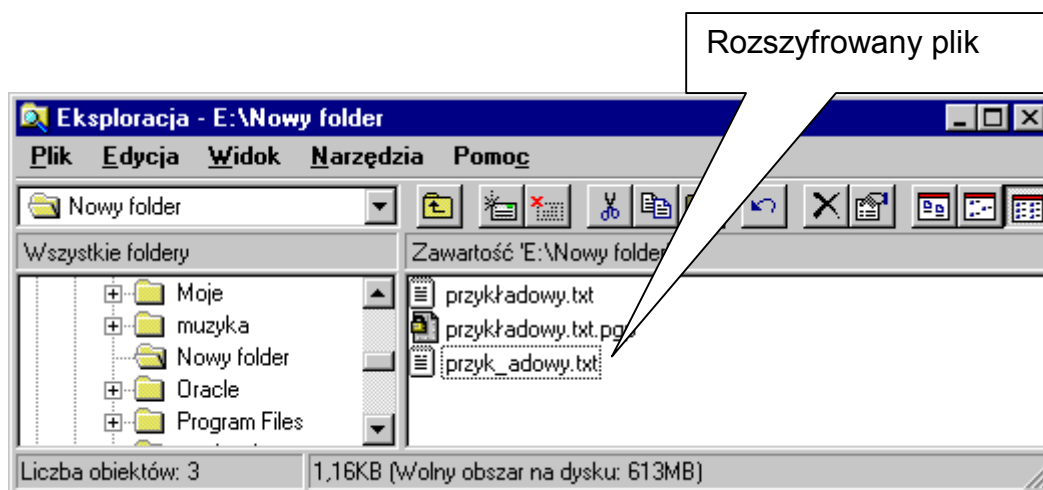
Aby odczytać plik zaszyfrowany kluczem publicznym danego użytkownika należy postępować według poniższych wskazówek:

- Uruchomić Explorator Windows NT: **Start->Programy->Explorator Windows NT**. Wskazać plik do rozszyfrowania.(Rysunek 29);
- Wskazać kursorem myszki plik i kliknąć prawym przyciskiem myszki. Pojawi się menu. Z menu wybrać **PGP->Decrypt&Verify**
- Jeżeli się okno jak na rysunku 30 podać hasło;



Rysunek 30 Okno: Podać hasło

- Rozszyfrowany plik znajduje się w bieżącym katalogu.(Rysunek 31)

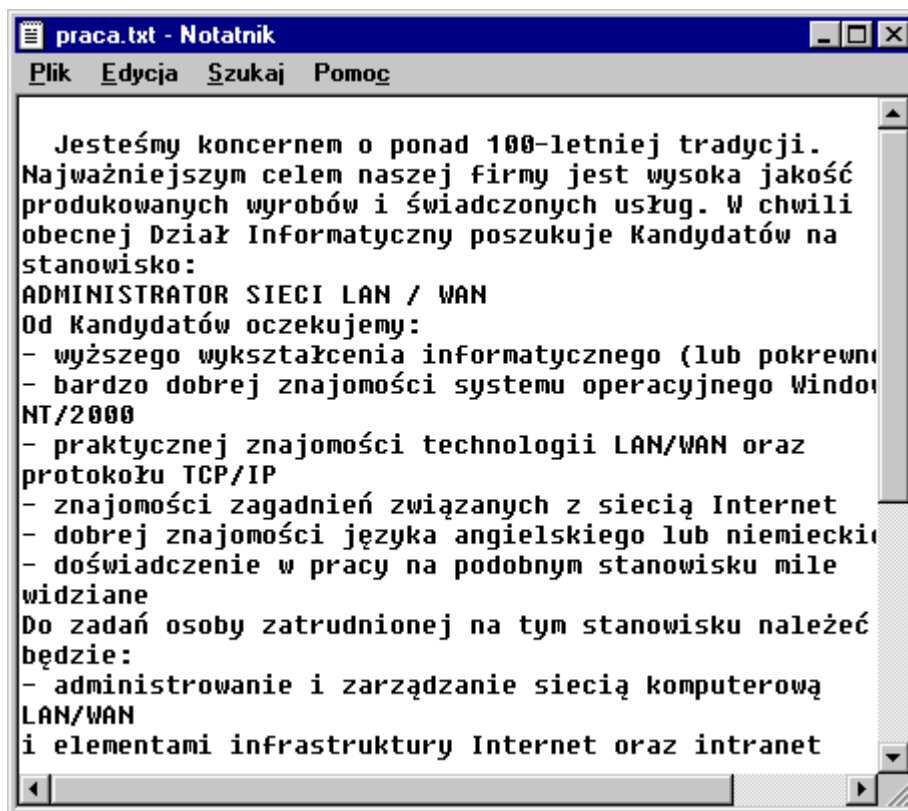


Rysunek 31 Okno pokazujące lokalizację rozkodowanego pliku

8. Szyfrowanie tekstu z wybranego okna lub ze schowka

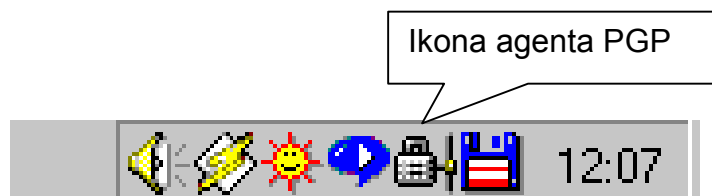
W celu zaszyfrowania tekstu umieszczonego w wybranym oknie np. w Notatniku należy postępować według poniższych wskazówek:

- Wskazać na okno edytora np. Notatnika tak, aby było aktywne;



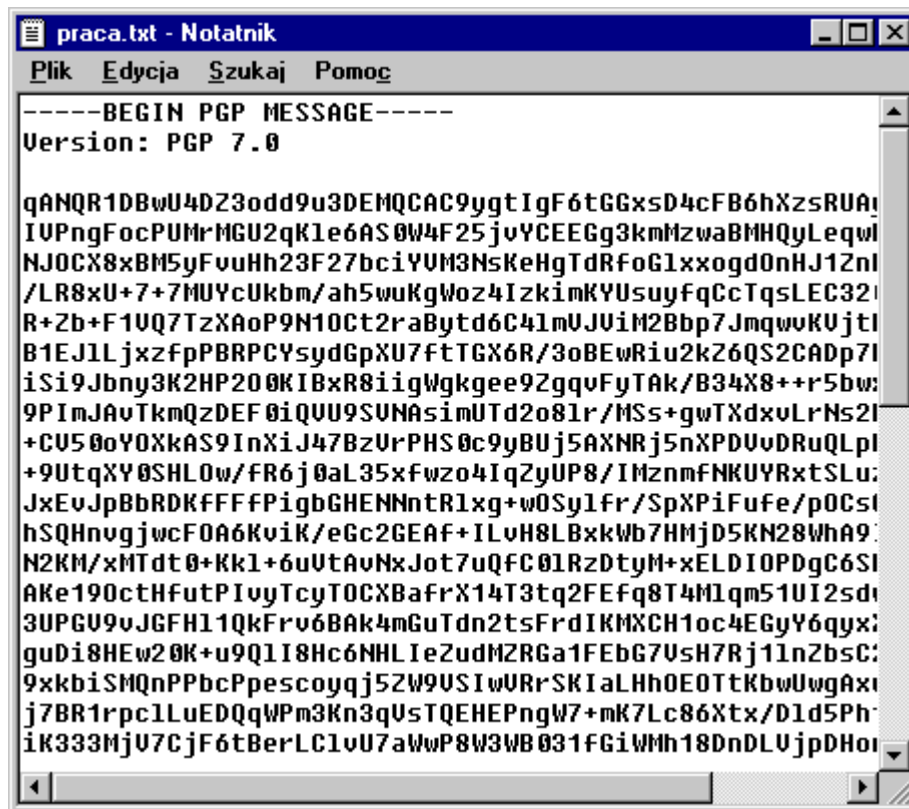
Rysunek 32 Okno notatnika z tekstem do zaszyfrowania

- Kliknąć dowolnym klawiszem myszki na ikonie agenta PGP umieszczoną w prawym dolnym rogu ekranu w pasku zadań na ikonie przypominającej żółtą kłódkę przyłączoną do drutu (Rysunek 33)



Rysunek 33 Ikona PGP agenta na pasku zadań

- Po rozwinięciu się paska menu wybrać: **Current Window->Encrytp** lub **Current Window->Encrytp&Sign**
- W następnym oknie przedstawionym na rysunku 28 wskazać klucze uprawnione do odszyfrowania tego tekstu;
- Padać hasło w oknie przedstawionym na rysunku 30.
- Zakodowany tekst przedstawiono na rysunku 34:

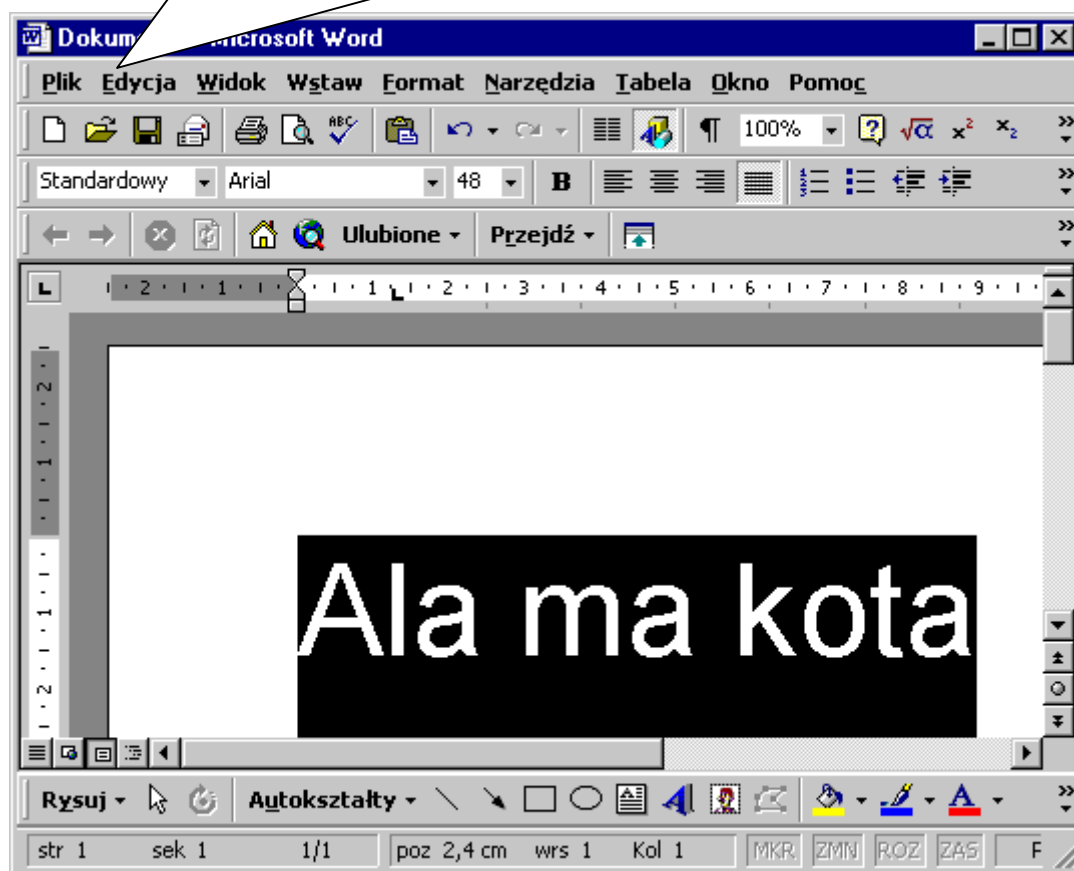


Rysunek 34 Okno edytora Notatnik z zaszyfrowanym tekstem

Jeżeli użytkownik chce przenieść tekst z jednego dokumentu do drugiego posługuje się schowkiem (Clipboard). PGP daje możliwość zaszyfrowania tekstu pochodzącego ze schowka. W celu zaszyfrowania tekstu ze schowka należy postępować według poniższych wskazówek:

- Skopiować tekst do schowka: tzn zaznaczyć tekst myszką i korzystając z menu **Edycja->Kopiuje** lub **Edit->Paste** skopiować tekst (Rysunek 35).
- Kliknąć dowolnym klawiszem myszki na ikonie PGP agenta umieszczoną w prawym dolnym rogu ekranu w pasku zadań na ikonie przypominającej żółtą kłódkę przyłączoną do drutu (Rysunek 33)
- Po rozwinięciu się paska menu wybrać: **Clipboard->Encrytp** lub **Clipboard->Encrytp&Sign**
- W następnym oknie przedstawionym na rysunku 28 wskazać klucze uprawnione do odszyfrowania tego tekstu;
- Padać hasło w oknie przedstawionym na rysunku 30.

Zaznaczyć tekst myszką i korzystając z menu **Edycja** -> **Kopiuj** lub **Edit** -> **Paste** skopiować tekst



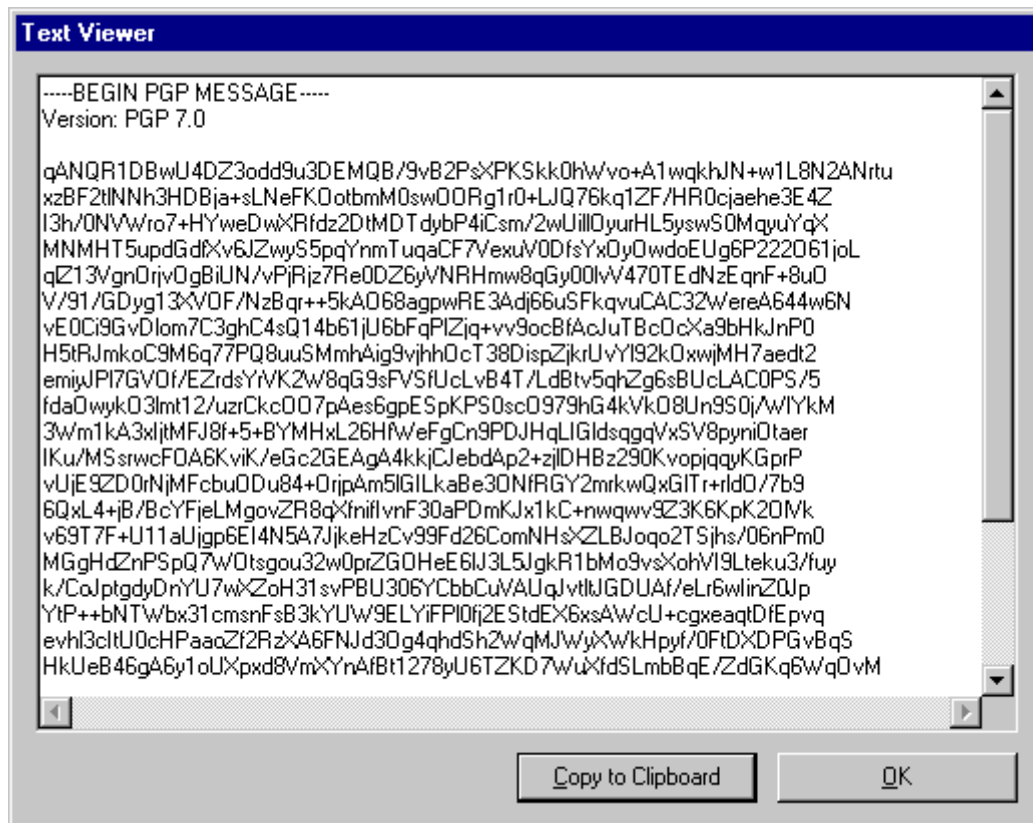
Rysunek 35 Sposób kopiowania tekstu do schowka

Zaszyfrowany tekst można wkleić np. do bieżącego dokumentu. Z menu **Edycja** należy kliknąć na pole **wklej**: **Edycja** -> **wklej**. Oto zaszyfrowany tekst z okna przedstawionego na rysunku 35, wklejony ze schowka.

-----BEGIN PGP MESSAGE-----
Version: PGP 7.0

```
qANQR1DBwU4DZ3odd9u3DEMQB/9vB2PsXPKSkk0hWvo+A1wqkhJN+w1L8N2ANrtu
xzBF2tiNNh3HDBja+sLNeFKOotbmM0swOORg1r0+LJQ76kq1ZF/HR0cjae3E4Z
I3h/0NVWro7+HYweDwXRfdz2DtMDTdybP4iCsm/2wUillOyurHL5yswS0MqyuYqX
MNMHT5updgdfXv6JZwyS5pqYnmTuqaCF7VexuV0DfsYxOyOwdoEUg6P222O61joL
qlZ13VgnOrjvOgBiUN/vPJRjz7Re0DZ6yVNRHmw8qGy00lvV470TEdNzEqnF+8uO
V/91/GDyg13XVOF/NzBqr++5kAO68agpwRE3Adj66uSFkqvuCAC32WereA644w6N
vE0Ci9GvDlom7C3ghC4sQ14b61jU6bFqPIZjq+vv9ocBfAcJuTBcOcXa9bHkJnP0
H5tRJmkoC9M6q77PQ8uuSMmhAig9vjhhOcT38DispZjkrUvYI92kOxwjMH7aed2
emiyJPI7GVOF/EZrdsYrVK2W8qG9sFVSfUcLvB4T/LdBtv5qhZg6sBUcLAC0PS/5
fdaOwykO3lmt12/uzrCkcOO7pAes6gpESpKPS0scO979hG4kVko8Un9S0j/WIYkM
3Wm1kA3xljtMFJ8f+5+BYMHxL26HfWeFgCn9PDJHqLIGlssggqVxSV8pyniOtaer
IKu/MSsrwcFOA6KviK/eGc2GEAgA4kkjCJebdAp2+zjIDHBz290KvopjqyKGprP
vUjE9ZD0rNjMFcbuODu84+OrjpAm5iGILkaBe3ONfRGY2mrkwQxGitr+rldO/7b9
```

```
6QxL4+jB/BcYFjeLMgovZR8qXfniflvnF30aPDmKJx1kC+nwqww9Z3K6KpK2OIVk
v69T7F+U11aUjgp6EI4N5A7JjkeHzCv99Fd26ComNHsXZLBJoqo2TSjhs/06nPm0
MGgHdZnPSPQ7W0tsgou32w0prZGOHeE6IJ3L5JgkR1bMo9vsXohVI9Lteku3/fuy
k/CoJptgdyDnYU7wXZoH31svPBU306YCbbCuVAUqJvlttJGDUAf/eLr6wlinZ0Jp
YtP++bNTWbX31cmSnFsB3kYUW9ELYIFPI0fj2EStdEX6xsAWcU+cgxeaqtDfEvpq
evhl3cltU0cHPaaoZf2RzXA6FNjd3Og4qhdSh2WqMJWYXWkHpyf/0FtDXDPGvBqS
HkUeB46gA6y1oUXpxd8VmXYnAfBt1278yU6TZKD7WuXfdSLmbBqE/ZdGKq6WqOvM
PSLddMBEMRoalLkoPygnzfAwqLGEehANPZQSZufo5DdmV/qSFAMChz7ZKlZHOHhC
zQIP1DhirR/7GzB5+/T+lldNtdjZ09v7RqEPU6ynsR9RKi4miStzjU1fJct7oN+D
/OeAPWUr8lvFNBtp5tdBIsLN9jHimpRpwz4Lg8u2H496WygBcdcyE1GtqvsRBGd
dkxo1kBomVLjd3+jScsVisHaPg0K19dgs9ydkeXwFxFk4AMw6iBzUcOdtZgeLn40
CSj1Y3BJvXLpWgFQ1LXK7A3yPdmMxnLu
=iOdg
-----END PGP MESSAGE-----
```

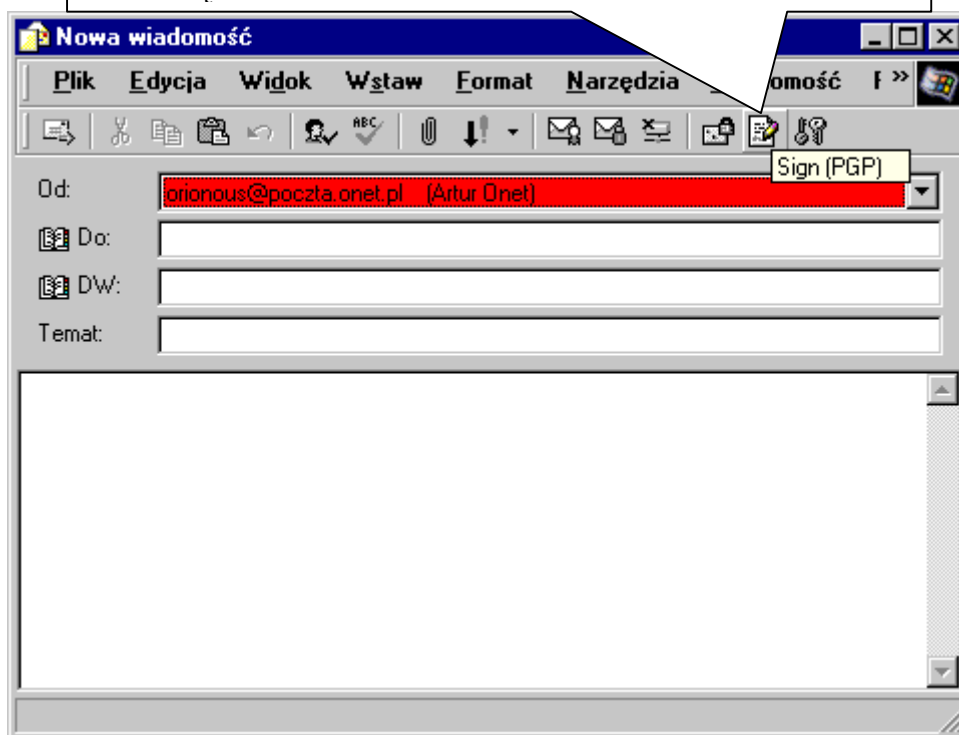


Rysunek 36 Schowek PGP z zaszyfrowanym tekstem: „Ala ma kota”

Aby podejrzeć zawartość schowka należy kliknąć ikonę agenta PGP (Rysunek 33) i przejść do pola **Cipboard->Edit**. Okno schowka PGP po wklejeniu poniższego tekstu przedstawiono na rysunku 36.

W celu usunięcia zawartości schowka należy kliknąć ikonę agenta PGP (Rysunek 33) i przejść do pola **Cipboard->Empty**.

Wciśnięcie ikony Sign (PGP) przed wysłaniem wiadomości spowoduje dołączenie sygnatury identyfikującej nadawcę wiadomości



Rysunek 37 Podpis wiadomości pocztowej

9. Podpisywanie tekstu

Aby podpisać poniższy tekst:

Tekst do podpisania

Należy:

- Skopiować tekst do schowka: tzn zaznaczyć tekst myszką i korzystając z menu **Edycja->Kopiuj** lub **Edit->Paste** skopiować tekst (Rysunek 35).
- Kliknąć dowolnym klawiszem myszki na ikonie agenta PGP umieszczoną w prawym dolnym rogu ekranu w pasku zadań na ikonie przypominającej żółtą kłódkę przyłączoną do drutu (Rysunek 33).
- Po rozwinięciu się paska menu wybrać: **Clipboard->Sign**.
- Padać hasło w oknie przedstawionym na rysunku 30.

Poniżej przedstawiono podpisany tekst: *Tekst do podpisania*

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Tekst do podpisania

-----BEGIN PGP SIGNATURE-----

Version: PGP 7.0

iQA/AwUBOfA3FzA10c0dDVTfEQLPwQCfejTSo5BuE4ddJlcGYJY+BCIkTC0An2Y+
Oh7HNjV5LezZNI1ITfIYUVGo
=xJx6

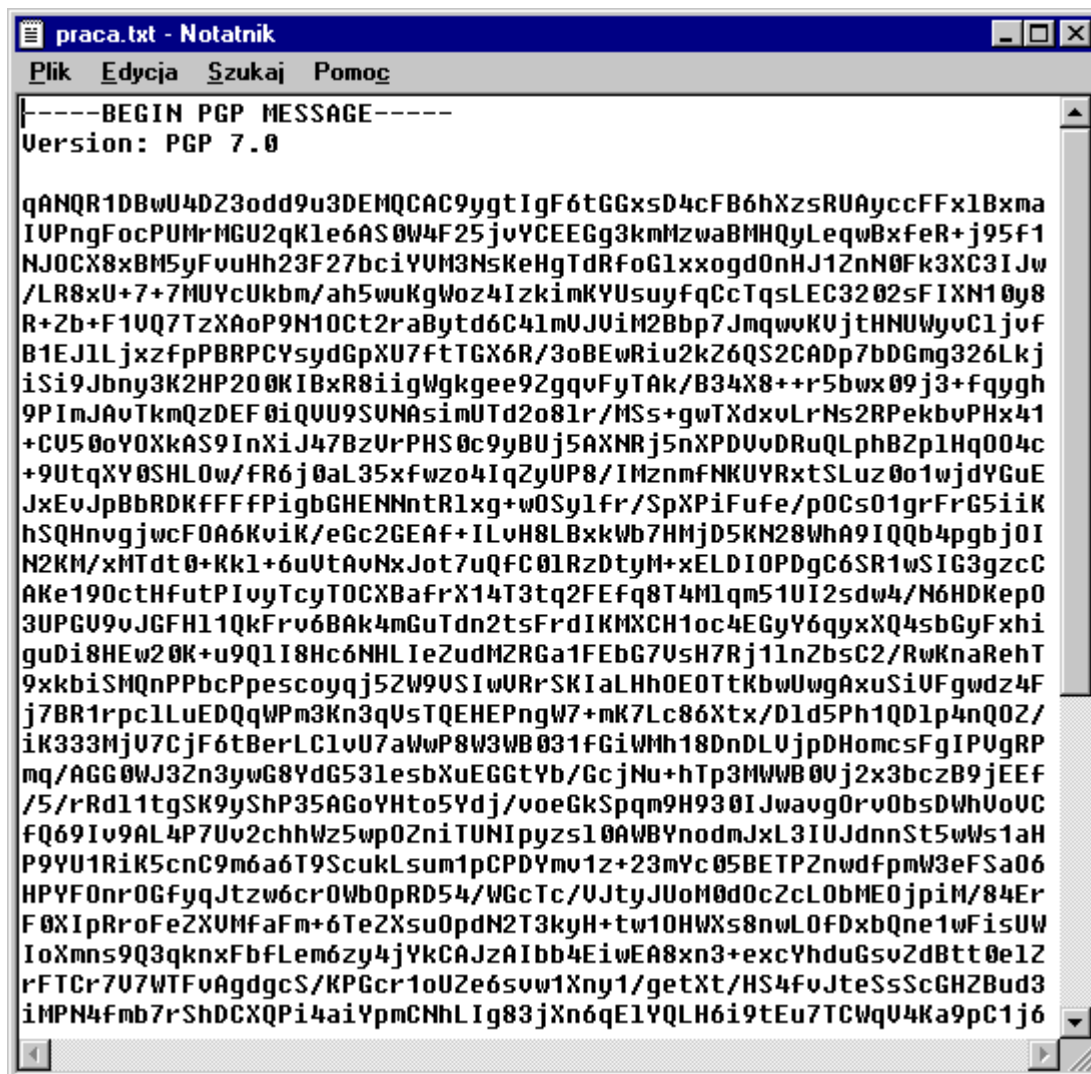
-----END PGP SIGNATURE-----

Podpisanie wiadomości do wysłania pocztą polega na wciśnięciu ikony Sign (PGP) w menu ikon programu Outlook Ekspres. Rysunek 37.

10. Odczytanie zaszyfrowanego tekstu z okna lub ze schowka

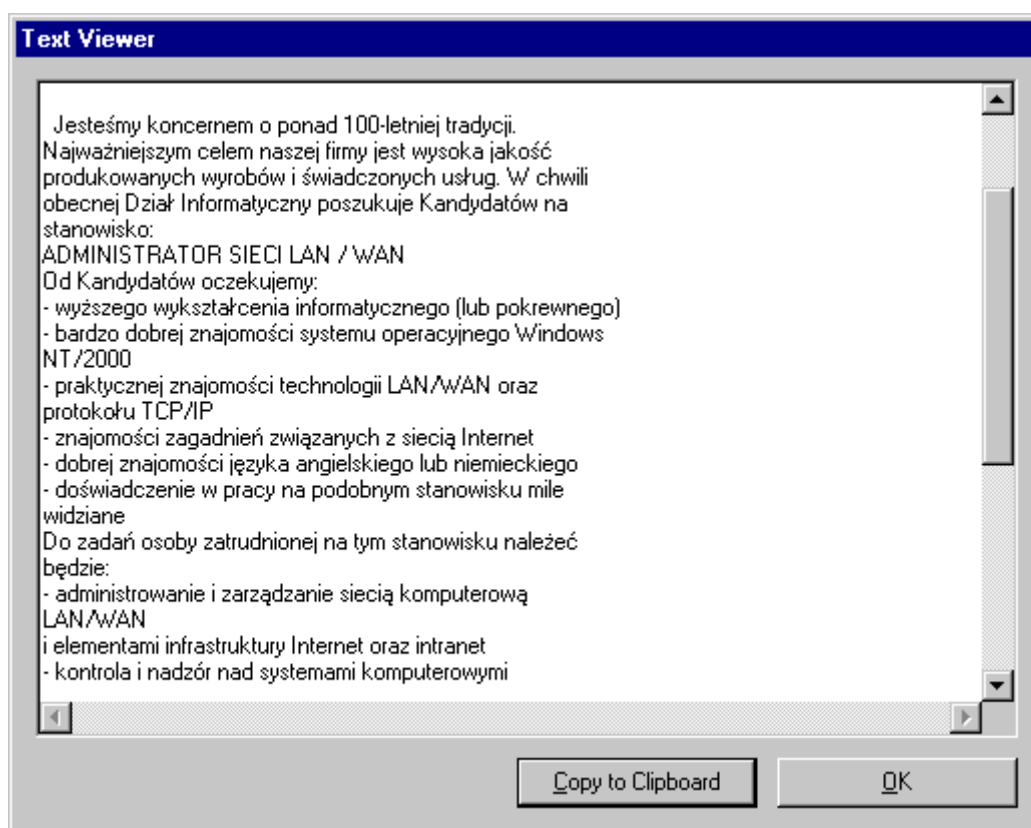
W celu odczytania zaszyfrowanego tekstu z okna należy postępować według poniższych wskazówek:

- Przejść do okna z zaszyfrowanym tekstem – uaktywnić okno z zaszyfrowanym tekstem.



Rysunek 38 Okno z zaszyfrowanym tekstem

- Kliknąć dowolnym klawiszem myszki na ikonie agenta PGP (umieszczonej w prawym dolnym rogu ekranu w pasku zadań) na ikonie przypominającej żółtą kłódkę przyłączoną do drutu (Rysunek 33);
- Po rozwinięciu paska menu wybrać: **CurrentWindow->Decrypt&Verify;**
- Padać hasło w oknie przedstawionym na rysunku 30;
- Rozkodowany tekst ukaże się w edytorze PGP; (Rysunek 39)



Rysunek 39 Rozszyfrowany tekst z rysunku 38

Tekst z okna przedstawionego na rysunku 38 można skopiować do schowka (wcisnąć przycisk **Copy to Clipboard**) i wkleić go do dowolnego pliku.

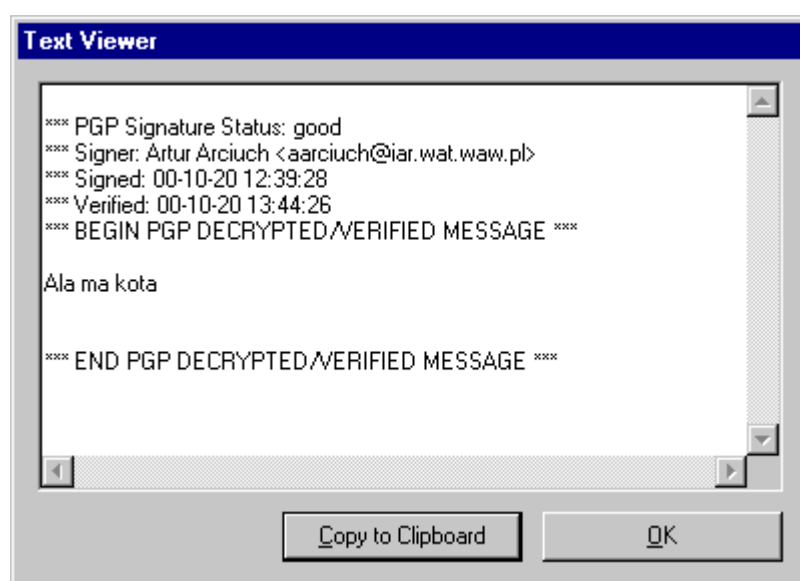
Jeżeli zaszyfrowany tekst znajduje się w schowku (np. zaszyfrowany tekst: „Ala ma kota” z rozdziału 8), to w celu odczytania tego zaszyfrowanego tekstu należy postępować według poniższych wskazówek:

- Kliknąć dowolnym klawiszem myszki na ikonie agenta PGP umieszczoną w prawym dolnym rogu ekranu w pasku zadań na ikonie przypominającej żółtą kłódkę przyłączoną do drutu (Rysunek 33);
- Po rozwinięciu się paska menu wybrać: **Clipboard->Decrypt&Verify;**
- Padać hasło w oknie przedstawionym na rysunku 30;
- Pokaże się okno podobne przedstawione na rysunku 40;
- Tekst można skopiować do schowka i wkleić np. poniżej:

```
*** PGP Signature Status: good
*** Signer: Jan Nowak<orionous@poczta.onet.pl>
*** Signed: 00-10-20 12:39:28
*** Verified: 00-10-20 13:44:26
*** BEGIN PGP DECRYPTED/VERIFIED MESSAGE ***
```

Ala ma kota

```
*** END PGP DECRYPTED/VERIFIED MESSAGE ***
```



Rysunek 40 Okno z rozszyfrowanym tekstem z rysunku 35

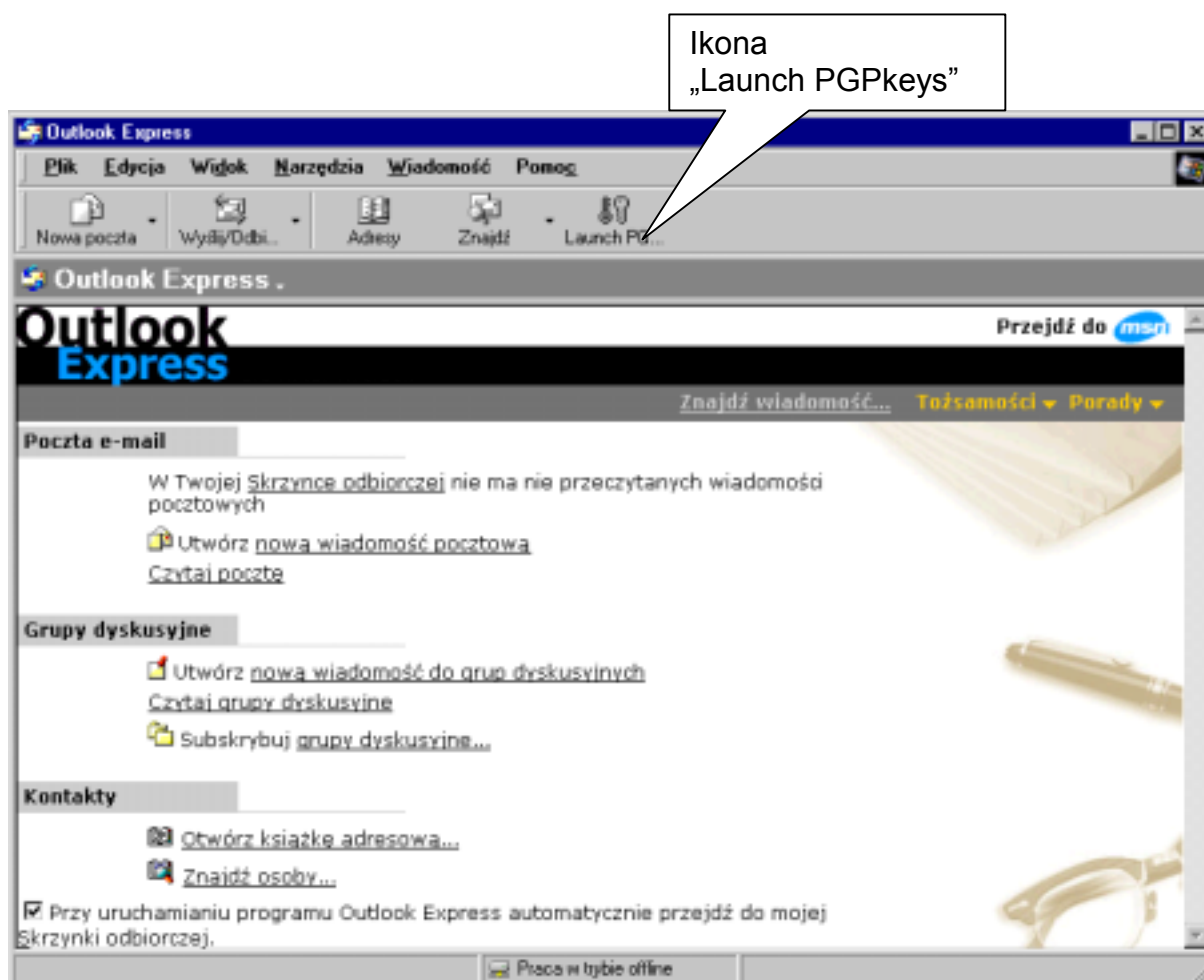
11. Generowanie pary kluczy

UWAGA !

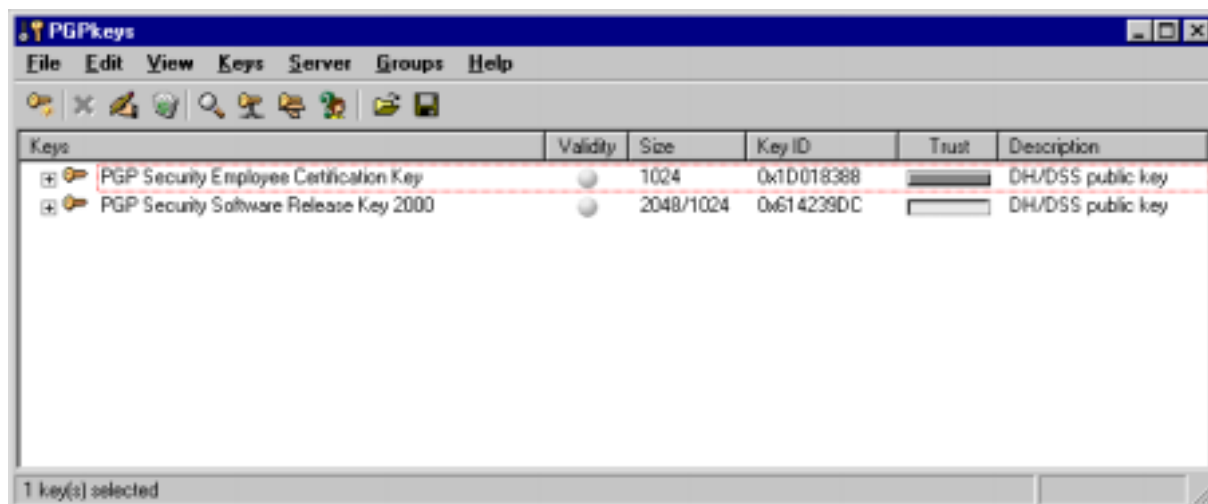
Klucz mógł zostać wygenerowany w trakcie instalacji pakietu PGP.

W celu wygenerowania nowej pary kluczy należy:

- Kliknąć ikonę „Launch PGPkeys” umieszczoną w pasku narzędzi okna głównego Outlook Express przedstawionego na rysunku 41. Przykładowe okno, które się wyświetli na skutek kliknięcia ikony „Launch PGPkeys”, przedstawiono na rysunku 42.



Rysunek 41 Okno główne Outlook Express po zainstalowaniu pakietu PGP

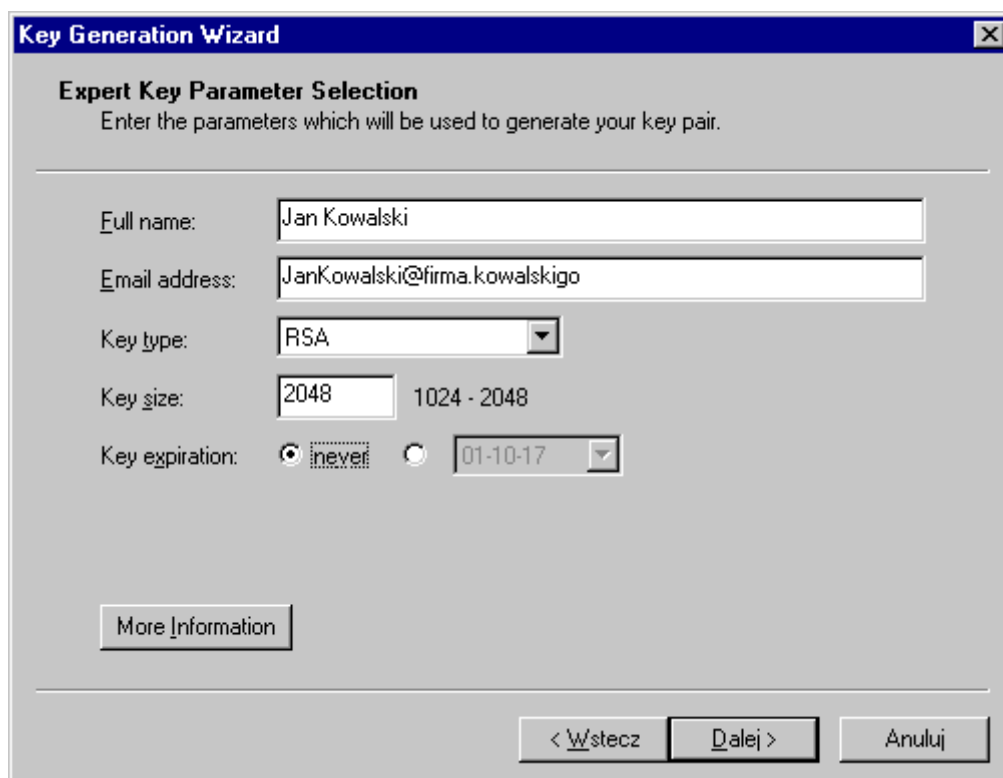


Rysunek 42 Okno PGPkeys

- Z menu tekstowego okna przedstawionego na rysunku 42 za pomocą myszy Kliknąć na pole: **Keys**. Po rozwinięciu podmenu należy wybrać pole: **New Key...Ctrl+N**. Ten sam efekt można uzyskać poprzez użycie klawiszy szybkiego dostępu (należy na klawiaturze jednocześnie nacisnąć klawisze: **Ctrl i N**). Działanie to spowoduje, że uruchomi się program, który przeprowadzi użytkownika przez proces generacji kluczy. Okno tego programu zostało przedstawione na rysunku 43.
- W oknie z rysunku 43 należy kliknąć przycisk **Expert**. Pojawi się okno przedstawione na rysunku 44. W tym oknie należy wypełnić okienka edycyjne w sposób następujący:
 - o **Full name** – wpisać własne imię i nazwisko;
 - o **Email address** – wpisać własny adres skrzynki pocztowej;
 - o **Key type** – wybrać jeden z trzech dostępnych algorytmów kodowania:
 - **Diffie – Hellman/DDS;**
 - **RSA** (obsługiwany tylko przez wersję 7.0 PGP);
 - **RSA – Legacy** (obsługiwany przez wcześniejsze wersje PGP);

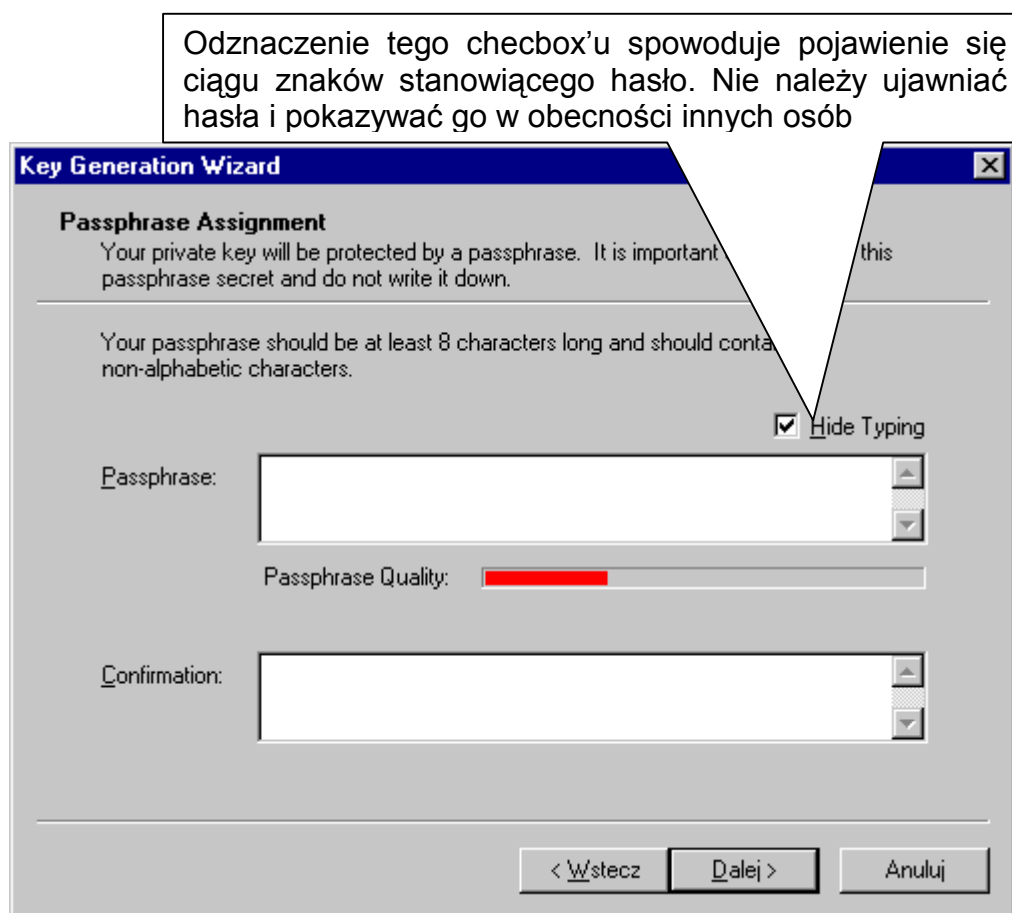


Rysunek 43 Okno programu służącego do generacji klucza



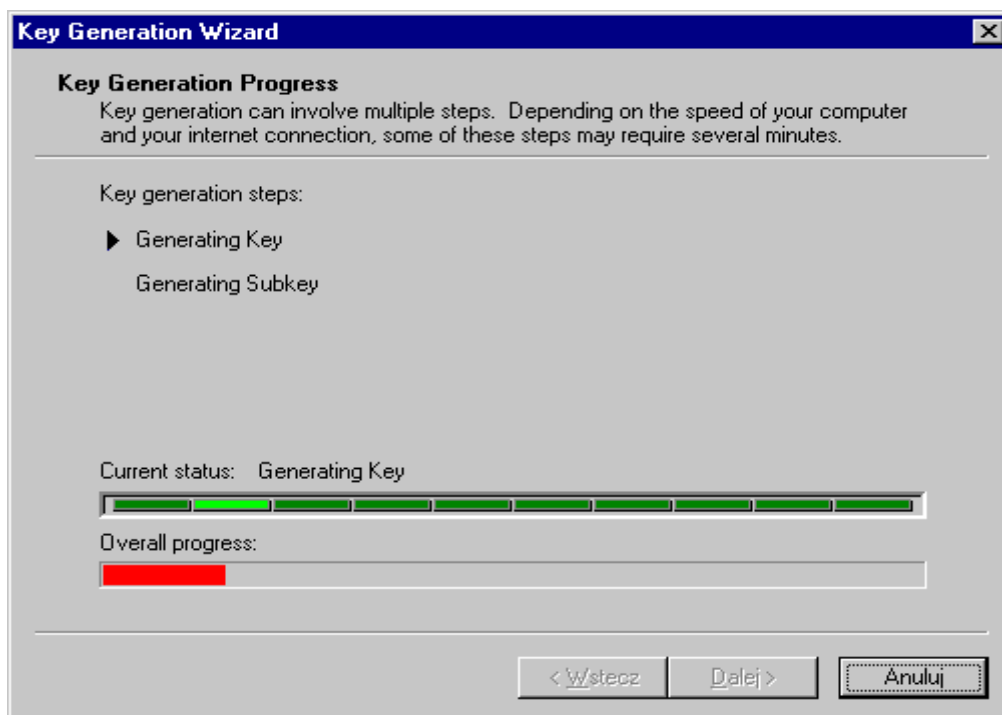
Rysunek 44 Okno programu generowania klucza po wciśnięciu przycisku „Expert”

- **Key size** – długość w bajtach bloku z zakodowaną wiadomością;
 - **Key expiration** – okres ważności klucza;
- Po wciśnięciu klawisza **Dalej** pojawia się okno przedstawione na rysunku 45. W okienku edycyjnym **Passphrase** należy wpisać ciąg znaków złożonych z liter, cyfr itp. i zapamiętać. W okienku edycyjnym **Confirmation** należy jeszcze raz wpisać hasło dokładnie takie jak w poprzednim okienku. Wpisany ciąg stanowi hasło, które będzie potrzebne do kodowania i rozkodowywania wiadomości.

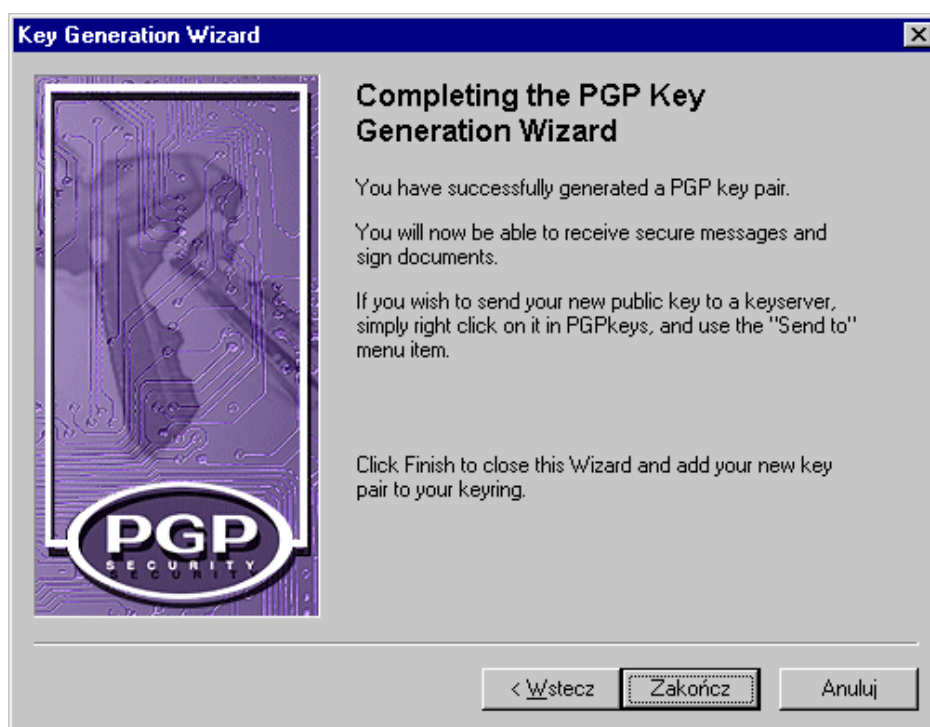


Rysunek 45 Okno służące do wpisania ciągu znaków stanowiącego hasło

- Po wpisaniu i potwierdzeniu hasła wcisnąć przycisk **Dalej**. Po wykonaniu tych czynności i pod warunkiem poprawnego wpisania hasła w dwóch okienkach edycyjnych nastąpi proces generowania pary kluczy. Okno jakie użytkownik zobaczy w tym czasie przedstawiono na rysunku 46.
- Po zakończeniu generowania pary kluczy wcisnąć przycisk **Dalej**, który będzie już dostępny.
- Ukaże się okno informujące o zakończeniu generacji pary kluczy. Należy wcisnąć przycisk **Zakończ**. (Rysunek 47)

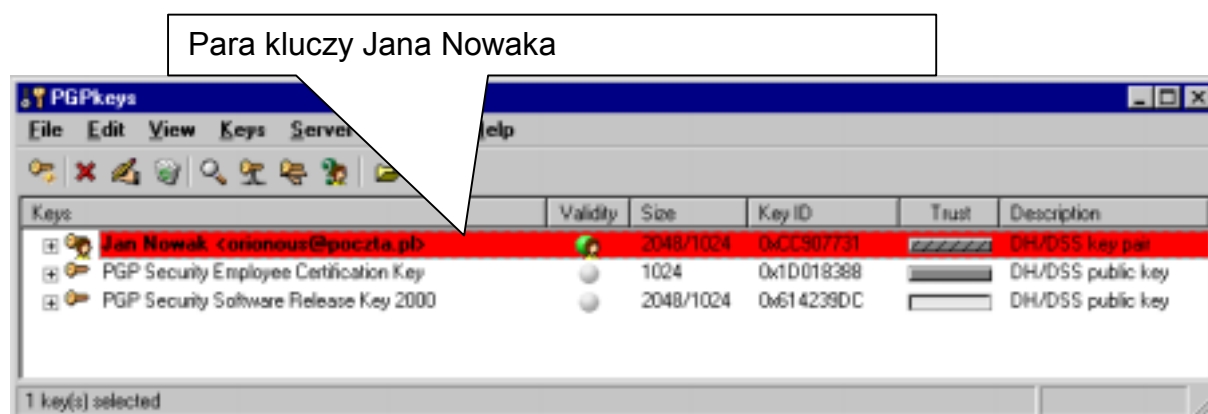


Rysunek 46 Okno pokazujące fakt generowania klucza



Rysunek 47 Okno informujące o wygenerowaniu pary kluczy

- Wygenerowana para kluczy jest przedstawiona w oknie PGPkeys, które ukaże się po wciśnięciu klawisza **Zakończ** w oknie przedstawionym na rysunku 47. Rysunek 48 przedstawia okno PGPkeys po dodaniu pary kluczy Jana Nowaka.



Rysunek 48 Okno PGPkeys po dodaniu klucza

12. Spis rysunków, wyjaśnienie niektórych zapisów

RYSUNEK 1 OKNO GŁÓWNE PROGRAMU PGKKEYS	3
RYSUNEK 2 OKNO GŁÓWNE OPCJI PROGRAMU PGPKEYS	4
RYSUNEK 3 OKNO ZAWIERAJĄCE INFORMACJE O POŁOŻENIU KLUCZY	5
RYSUNEK 5 OKNO INFORMUJĄCE O TYM, ŻE TRWA PROCES POŁĄCZENIA Z SERWEREM KLUCZY	7
RYSUNEK 6 OKNO INFORMUJĄCE O UMIESZCZENIU KLUCZA NA SERWERZE KLUCZY	7
RYSUNEK 7 OKNO PGPKEYS W PRZYPADKU KOPIOWANIA KLUCZA	7
RYSUNEK 8 OKNO OUTLOOK EXPRESS W PRZYPADKU WYSYŁANIA KLUCZA PUBLICZNEGO	8
RYSUNEK 9 OKNO DO WPISANIA HASŁA DLA PODANEGO KLUCZA	8
RYSUNEK 10 OKNO OUTLOOK EXPRESS PRZY WYSYŁANIU KLUCZA PO PRZECIĄgniĘCIU GO Z OKNA PGPKEYS	9
RYSUNEK 11 OKNO PGPKEYS Z OPISEM DO WYKSPORTOWANIA KLUCZA DO PLIKU	10
RYSUNEK 12 OKNO PGPKEYS I OPIS DO WYBORU SERWERA W CELU POBRANIA KLUCZA	11
RYSUNEK 13 OKNO DO WYSZUKIWANIA KLUCZA PUBLICZNEGO DANEGO UŻYTKOWNIKA	12
RYSUNEK 14 PGPKEYS PO DODANIU KLUCZA PUBLICZNEGO PANA KOWALSKIEGO	12
RYSUNEK 15 SPOSÓB SKOPIOWANIA ZAWARTOŚCI KLUCZA PUBLICZNEGO Z PROGRAMU POCZTOWEGO	13
RYSUNEK 16 ELEMENTY OKNA PGPKEYS ISTOTNE PRZY DODAWANIU KLUCZA	13
RYSUNEK 17 OKNO SŁUŻĄCE DO IMPORTOWANIA KLUCZA	14
RYSUNEK 18 KLUCZ PUBLICZNY W PLIKU TEKSTOWYM	15
RYSUNEK 19 SPOSÓB WYSYŁANIA ZAKODOWANEJ WIADOMOŚCI	16
RYSUNEK 20 WYBÓR KLUCZY PUBLICZNYCH ADRESATÓW POCZTY	17
RYSUNEK 21 OKNO DO WPISANIA HASŁA	17
RYSUNEK 22 ZASZYFROWANA WIADOMOŚĆ PO STRONIE ADRESATA	18
RYSUNEK 23 WIDOK ZASZYFROWANEJ WIADOMOŚCI W OKNIE SKRZYŃKA ODBIORCZA OUTLOOK EXPRESS	19
RYSUNEK 24 OKNO OUTLOOK EXPRESS DO ODSZYFROWANIA WIADOMOŚCI	20
RYSUNEK 25 OKNO DO WPISANIA HASŁA	20
RYSUNEK 26 OKNO Z ROZSZYFROWANĄ WIADOMOŚCIĄ	21
RYSUNEK 27 OKNO EKSPLORATORA WINDOWS NT, Z WYBRANYM DO ZASZYFROWANIA PLIKIEM	22
RYSUNEK 28 OKNO DO WYBORU OSÓB UPRAWNIONYCH DO ROZSZYFROWANIA PLIKU	23

RYSUNEK 29 WIDOK ZASZYFROWANEGO PLIKU	23
RYSUNEK 30 OKNO: PODAĆ HASŁO	24
RYSUNEK 31 OKNO POKAZUJĄCE LOKALIZACJĘ ROZKODOWANEGO PLIKU	24
RYSUNEK 32 OKNO NOTATNIKA Z TEKSTEM DO ZASZYFROWANIA	25
RYSUNEK 33 IKONA PGP AGENTA NA PASKU ZADAŃ	25
RYSUNEK 34 OKNO EDYTORA NOTATNIK Z ZASZYFROWANYM TEKSTEM.....	26
RYSUNEK 35 SPOSÓB KOPIOWANIA TEKSTU DO SCHOWKA	27
RYSUNEK 36 SCHOWEK PGP Z ZASZYFROWANYM TEKSTEM: „ALA MA KOTA”	28
RYSUNEK 37 PODPIS WIADOMOŚCI POCZTOWEJ	29
RYSUNEK 38 OKNO Z ZASZYFROWANYM TEKSTEM	31
RYSUNEK 39 ROZSZYFROWANY TEKST Z RYSUNKU 38.....	32
RYSUNEK 40 OKNO Z ROZSZYFROWANYM TEKSTEM Z RYSUNKU 35	33
RYSUNEK 42 OKNO PGPKEYS.....	35
RYSUNEK 43 OKNO PROGRAMU SŁUŻĄCEGO DO GENERACJI KLUCZA	36
RYSUNEK 44 OKNO PROGRAMU GENEROWANIA KLUCZA PO WCIŚNIĘCIU PRZYCISKU „EXPERT”	36
RYSUNEK 45 OKNO SŁUŻĄCE DO WPISANIA CIĄGU ZNAKÓW STANOWIĄCEGO HASŁO	37
RYSUNEK 46 OKNO POKAZUJĄCE FAKT GENEROWANIA KLUCZA	38
RYSUNEK 47 OKNO INFORMUJĄCE O WYGENEROWANIU PARY KLUCZY.....	38
RYSUNEK 48 OKNO PGPKEYS PO DODANIU KLUCZA.....	39

- **Start ->Programy ->PGP ->PGPkeys** oznacza, że należy kursor myszki umieścić w lewym dolnym polu ekranu o napisie **Start** i kliknąć na nim. Rozwinie się pasek menu, z którego należy ponownie kursorem myszy wybrać pole o napisie **Programy**, następnie po ukazaniu się podmenu wybrać pole **PGP** i dalej po rozwinięciu się kolejnego podmenu pole **PGPkeys**. Ostaną operacją spowoduje uruchomienie się programu PGPkeys.