

# Podpis elektroniczny

Powszechne stosowanie dokumentu elektronicznego i systemów elektronicznej wymiany danych oprócz wielu korzyści, niesie również zagrożenia. Niebezpieczeństwa korzystania z udogodnień wprowadzanych przez elektroniczne systemy przesyłania danych są różnorakie: począwszy od technologicznych (wirusy, utrata integralności danych) po biznesowe (naruszenie poufności transmisji, niejednoznacznie określony czas utworzenia dokumentu).

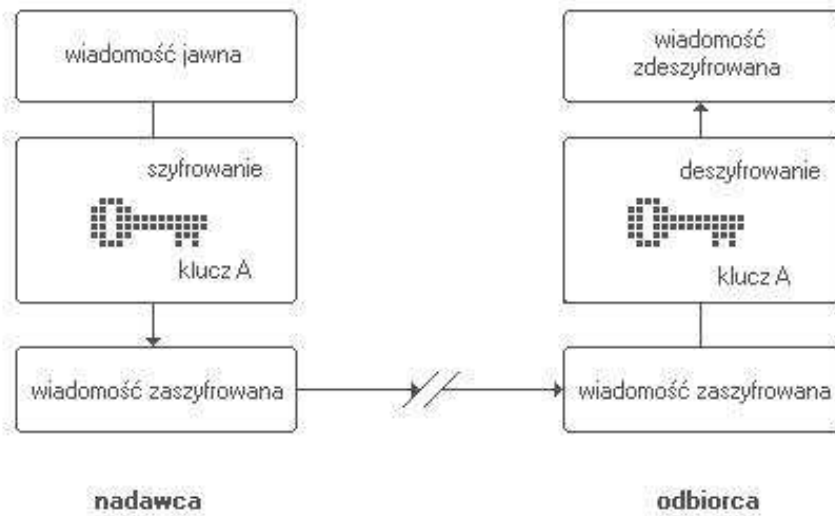
Pewnym rozwiązaniem jest stosowanie technologii PKI (Public Key Infrastructure infrastruktura klucza publicznego), nazywana potocznie technologią podpisu elektronicznego.

Infrastruktura klucza, to nowoczesne rozwiązanie dostarczające usługi bezpieczeństwa użytkownikom elektronicznej wymiany danych, wykorzystujące mechanizmy kryptografii asymetrycznej. W jej skład wchodzi oprogramowanie, sprzęt oraz zasady funkcjonowania zgodne z obowiązującymi standardami światowymi.

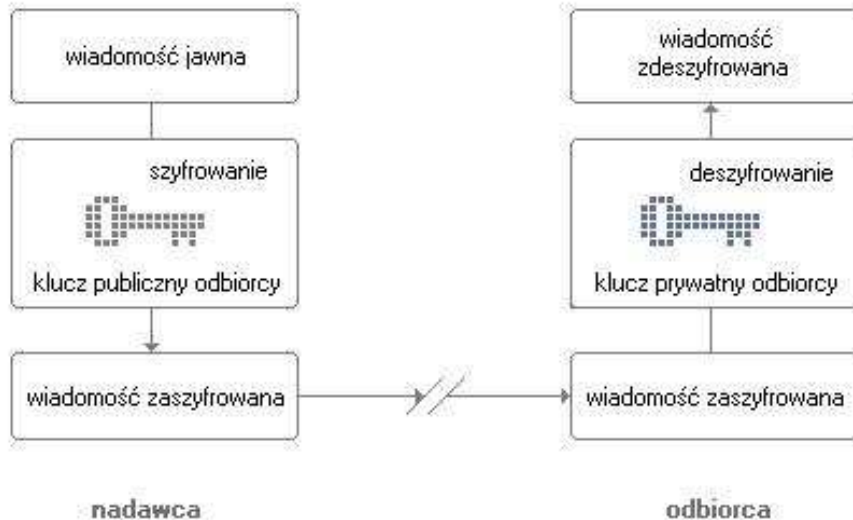
Tak jak listy tradycyjne ewoluowały do postaci elektronicznej, tak i ich zabezpieczenia autentyczności danych i szyfrowania treści muszą mieć swoje odpowiedniki elektroniczne. Zwykły podpis składany na papierze powinien zostać zastąpiony podpisem elektronicznym. Tylko jedna osoba może posługiwać się takim podpisem, co zapewnia autentyczność nadawcy. Autentyczna musi być również treść. Nie może zdarzyć się sytuacja, że ktoś będzie w stanie zmienić treść przesyłanych danych.

W technologii PGP (Pretty Good Privacy) podpis cyfrowy nie modyfikuje treści wychodzącej wiadomości. Szyfrowanie poczty jest przetwarzaniem wysyłanej treści, więc jest to ingerencja w materię tekstu. Szyfrowanie dokonywane jest przy pomocy klucza publicznego (jawnego) osoby, do której kierowany jest list. Deszyfracja następuje z użyciem klucza prywatnego (tajnego) przez jego posiadacza (szyfrowanie asymetryczne). Szyfrowanie i deszyfrowanie może następować również przy użyciu jednego i tego samego klucza (szyfrowanie symetryczne).

### *szyfrowanie symetryczne*



### *szyfrowanie asymetryczne*



Tak jak każdy człowiek ma wyrobiony swój charakter pisma odróżniający jego pismo od pisma innych ludzi, tak i w przypadku elektronicznego przekazu danych nie może być mowy o wyparciu się autorstwa dokumentu, tzn. zapewniona musi zostać niezaprzeczalność nadania i odbioru - gwarancja na to, że dokument na pewno został wysłany przez tego, kto figuruje na nim jako nadawca i trafił na pewno do tej osoby, która przez nadawcę została wskazana jako adresat przesyłki. Dodatkowo takie dokumenty mogą być stemplowane znacznikiem czasu, który określa moment ich wysłania.

Naszym zadaniem podczas wykonywania ćwiczenia było zapoznanie się z systemem szyfrowania PGP oraz weryfikacją, tworzeniem i zarządzaniem kluczami. Podczas pracy wygenerowaliśmy cztery klucze, każdy z nas posiada obecnie swój klucz prywatny i publiczny ważny do czerwca roku następnego.

Jesteśmy świadomi, że wygaśnięcie ważności klucza jest niezbędne, gdyż dłuższy czas i zaangażowanie dużej mocy obliczeniowej może spowodować złamanie naszego klucza przez osoby trzecie, nieupoważnione do tego. Obsługa programu jest intuicyjna, lecz pewne trudności nastęrcza brak interfejsu w języku polskim. Ponadto bez posiadania sporej wiedzy teoretycznej, program na niewiele się zdaje. Wadą PGP jest to, że odbiorca musi mieć wygenerowany wcześniej klucz, by móc deszyfrować informacje, które zamierzamy mu przesłać. Ponadto musi mieć zainstalowane w swoim komputerze odpowiednie oprogramowanie obsługujące technologię PGP. Natomiast ogromną zaletą tego typu rozwiązania jest długość słowa kodowego, która obecnie wynosi 1024/2048 bitów.

Podczas trwania pracowni wykonaliśmy ćwiczenie polegające na zaszyfrowaniu wiadomości przesyłanej via e-mail. Poniższe zrzuty ekranu ilustrują wyniki naszego doświadczenia:

*Zrzut ilustrujący naszą wiadomość, po sprawdzeniu zawartości skrzynki pocztowej:*

The screenshot shows a webmail interface with a navigation bar at the top containing links like 'poczta', 'opcje', 'adresy', 'płatność', 'pomoc', and 'wyloguj'. On the left, there is a sidebar with 'foldery' (folders) and 'na skróty' (shortcuts). The main content area displays an email header with the following information:

- Data:** Czwartek, 4 Grudnia 2003 14:12
- Od:** marcin mizera <mizi11@wp.pl>
- Do:** radek łochowski <losiupanther@wp.pl>
- Temat:** spotkanie

Below the header, the email body contains a PGP message:

```

-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 7.0.3 for non-commercial use
<http://www.pgp.com>

qANQR1DBwU4DgChyuXy2rCkQCADN3AZZavuu3jtyjEkIru46xHciB+LqFWA6rCOy
eCv/vMIIH+VmrH+9qNIemaRo4hyHgqTHXlmpUfk2Reu5zxwBUslUPRBz48qG/ob5
u7kJBg3oQk30pnGKw+7Kt2LeG5tnaWgdyBx2pvrVKjUosPuVWz+1RZSffFni tmP/
O+B4EKkLtod2AZ0ayk1xJ7IJT0bSSf/Iat2KcxUi7tyBKeWQeS+MgXFV8VtHze+0
eMHLLucbk/XNqWCKN180wYXsKK2SjnGvFMKSf2dTr0TY6nLh23zEQgbYJI1QH34F
rEop1gCmQC8ZxbrrFkfvM1BcSA11CkMGpepJ/hI81ITA76U8B/wIqMwBxferxtMU
GCoRz5ioYbC7H+aP0qzt2828B9/sTN2Ygh0xCdPWkmTWNrQ8EMYxan36I9kJQ4Ty
1099+qB0QLWlumWYGXXS1j0+d5uyl9TnRNwHaYj/UV0iVCWLcpjxUI7s9JR5S0S
B0xpC03xzPoh0LmaOXQJsKQBo2rM15bzW1iIdHfJFLzKHE8x0t1Umc8YmVPMP/YN
rofSoVrGMh0ANKJzqBN5CqZR4f+st+2EKVS/Khjuy0fut1GptI2IoxUj1g2868dq
g/uM5Crcfj3WGoDoYhV0jb4yHc7doytV1IQAIzpZbhNKMw0zojuWL1V4ChJgvfU
k3QoAQY+yUBU3EJjXTj695CUsjGvcPC01mTEitu7ChuuiXfvTuBdgjy43uLV//yk
927Huhm3kECWAcKJG8PX9sCwfLcc2DBi
=M0mI
-----END PGP MESSAGE-----

```

Teraz już widok przechwyconych w sieci ramek. Bez szyfrowania nasza wiadomość wygląda następująco:

Microsoft Network Monitor - [Przechwytywanie: 2 (Szczegółowe)]

Ramka	Godzina	Źród MAC Adr	Cel adr MAC	Protokół	Opis	Źród Inne Adr	Cel inny adr	Wpisz ir
5	1.822621	LOCAL	00D09595...	HTTP	-----7d316362201fc00Content-...	KOMPHIGH	212.77.101...	IP

Frame: Base frame properties  
 ETH: ETHTYPE = 0x0800 : Protocol = IP: DOD Internet Protocol  
 IP: ID = 0xcd7; Proto = TCP; Len: 602  
 TCP: .AP..., len: 562, seq:1394168878-1394169440, ack:3363247195, win:17520, src: 1470  
 HTTP: -----7d316362201fc00Content-Disposition: Request (from client user)  
 HTTP: Request Method = -----7d316362201fc00Content-Disposition:  
 HTTP: Uniform Resource Identifier = form-data;  
 HTTP: Protocol Version = name="mail(vcard)"  
 HTTP: Data: Number of data bytes remaining = 471 (0x01D7)

```

e="html"
-----7d316362201fc00Content-
t-Disposition: f
orm-data; name="
mail(body)"
ez wodke, duzo w
odki, mnostwo wo
dki, zagryche te
z
7d316362201fc00C
ontent-Dispositi
on: form-data; n
  
```

Po wykonaniu szyfrowania za pomocą PGP, nasza wiadomość wyglądałaby w sposób pokazany niżej. Nie można z niej wywnioskować nic:

Microsoft Network Monitor - [Przechwytywanie: 3 (Szczegółowy)]

Ramka	Godzina	Źród MAC Adr	Cel adr MAC	Protokół	Opis	Źród Inne Adr	Cel inny adr	Wpisz ir
5	4.877013	LOCAL	00D09595...	HTTP	-----7d333951102e000		212.77.101...	IP
6	4.877013	LOCAL	00D09595...	HTTP	-7d333951102e00-00 Request (from		212.77.101...	IP
7	5.838107	LOCAL	00D09595...	TCP	A len: 0 seq:1473586072		212.77.101...	TP

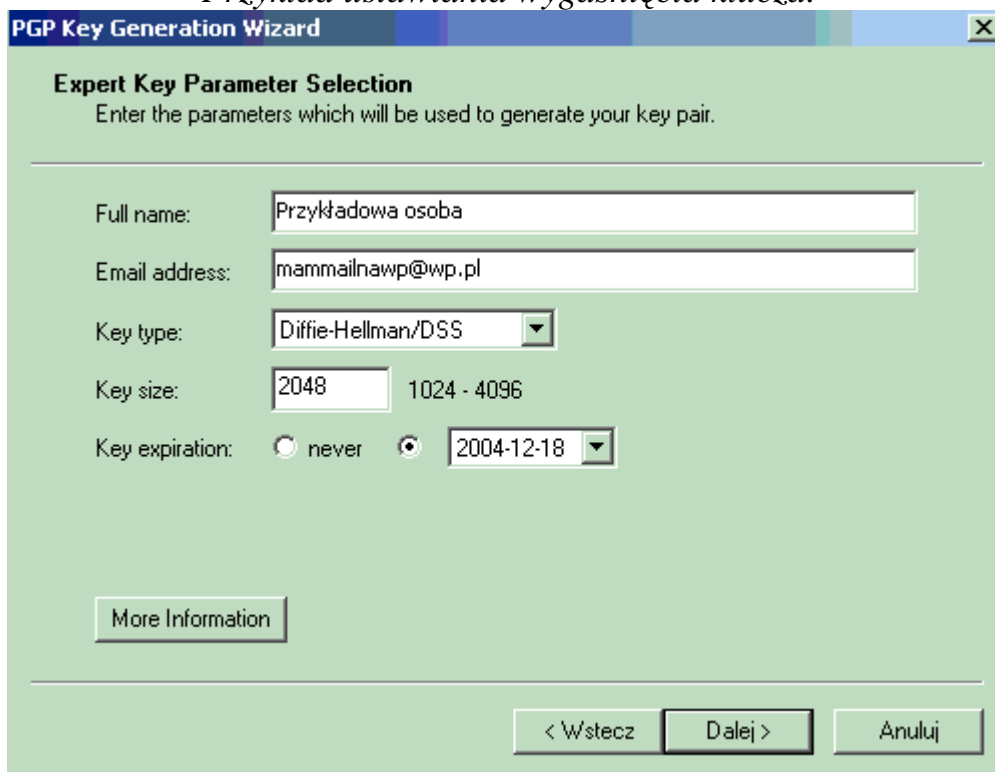
Frame: Base frame properties  
 ETH: ETHTYPE = 0x0800 : Protocol = IP: DOD Internet Protocol  
 IP: ID = 0xf69; Proto = TCP; Len: 1500  
 TCP: A..., len: 1460, seq:1473584594-1473586054, ack:1013763937, win:17520, src: 1566  
 HTTP: -----7d333951102e000Content-Disposition: Request (from client user)  
 HTTP: Request Method = -----7d333951102e000Content-Disposition:  
 HTTP: Uniform Resource Identifier = form-data;  
 HTTP: Protocol Version = name="mail(vcard)"  
 HTTP: Data: Number of data bytes remaining = 1369 (0x0559)

```

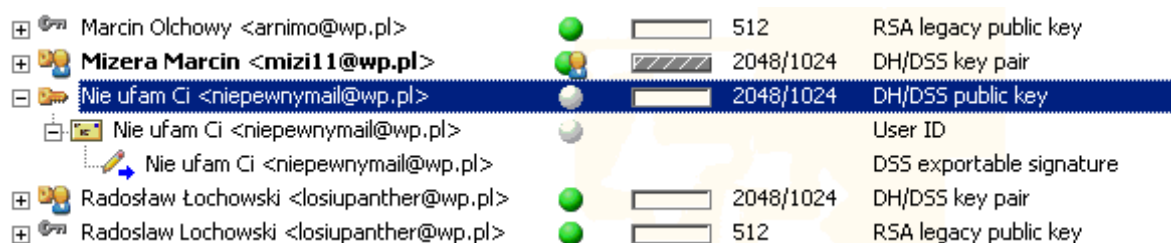
orm-data; name="
mail(body)"
-----BEGIN PGP ME
SSAGE-----
ion: PGPfreeware
7.0.3 for non-c
ommercial use
http://www.pgp.
com/
wU4DgChyuXyZrCkQ
CADN3AZZavuu3jty
jEkIru46xHciB+Lq
FWA6rCOyJMeCv/vM
---BEGIN PGP ME
SSAGE-----
ion: PGPfreeware
7.0.3 for non-c
ommercial use
http://www.pgp.
com/
wU4DgChyuXyZrCkQ
CADN3AZZavuu3jty
jEkIru46xHciB+Lq
FWA6rCOyJMeCv/vM
IIH+VmrH+9qNIema
Ro4hyHggqTHXlmpUf
kZReu5zxwBUslUPR
Bz48qC/ob5M0u7kJ
Bg3oQk30pnGKw+7K
tZLeC5tmaWgdyBxZ
rsvrvKjUosPuWw+1
RZSffFnitmp/
B4BRkLtodZAZ0ayk
lxJ7IJT0bSSf/Iat
ZKcxUi7tyBKeWQeS
+MgXfV8VtHze+0.
eMHHLucbk /XNqWcK
N180wYXsKK2SjnCW
  
```

PGP umożliwia naprawdę dobrą ochronę naszych danych, gdyż klucz kodowy w chwili obecnej jest na tyle długi, że złamanie go przy dostępnym sprzęcie komputerowym trwałoby około 6 mln lat. Jednak powinniśmy myśleć przyszłościowo, ponieważ błyskawicznie zwiększa się moc obliczeniowa komputerów. W tym celu ustawiamy czas wygasania naszego klucza. Jest to w połączeniu z długością słowa kodowego, wystarczające zabezpieczenie.

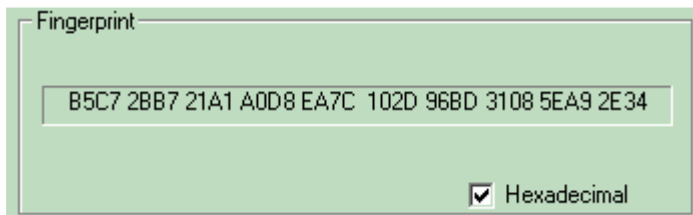
*Przykład ustawiania wygaśnięcia klucza.*



Kolejną rzeczą, jaką musimy wziąć pod uwagę jest weryfikacja klucza. Gdy otrzymujemy od kogoś klucz publiczny, musimy go podpisać, wyrażając w ten sposób zaufanie do tej osoby. Po podpisaniu pojawi się zamiast szarego koła, zielone.



Autentyczność klucza publicznego możemy potwierdzić, prosząc o podanie „odcisku palca” osoby wysyłającej nam klucz. Fingerprint jest skrótem oryginalnego klucza utworzonym wg. algorytmu zapewniającego jego niepowtarzalność.



Kolejną rzeczą, o której nie pomyśleli programiści jest domyślne ustawienie zapamiętywania haseł i przechowywanie ich w pamięci operacyjnej naszego komputera przez kilka minut. Te udogodnienie oszczędza nasz czas, jednakże stwarza niebezpieczeństwo przechwycenia haseł przez osoby niepowołane. Przez kilka minut są w stanie podpisywać dokumenty za nas.

*Ta opcja powinna zostać zaznaczona, żeby program nie zapamiętywał hasła*

