helion.pl
KSIĘGARNIA INTERNETOWA · WYDAWNICTWO

IDŹ DO
PRZYKŁADOWY ROZDZIAŁ
SPIS TREŚCI

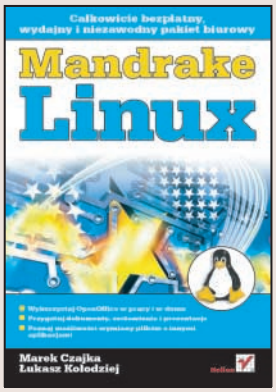
KATALOG KSIĄŻEK
KATALOG ONLINE
ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK
DODAJ DO KOSZYKA

CENNIK I INFORMACJE
ZAMÓW INFORMACJE O NOWOŚCIACH
ZAMÓW CENNIK

CZYTELNIA
FRAGMENTY KSIĄŻEK ONLINE

Mandrake Linux



Autorzy: Marek Czajka, Łukasz Kołodziej
ISBN: 83-7361-367-6
Format: B5, stron: 360

Całowicie bezpłatny, wydajny i niezawodny pakiet biurowy

Zalety Linuksa znają już chyba wszyscy. Jego popularność jest coraz większa. Z prostego systemu napisanego przez studenta w ramach zajęć na uczelni, Linux stał się jednym z najdynamiczniej rozwijających się produktów informatycznych. Korzystają z niego nie tylko pasjonaci i użytkownicy domowi, ale także firmy i koncerny. Wszyscy użytkownicy doceniają jego stabilność, uniwersalność, a przede wszystkim – nieodpłatny dostęp zarówno do samego systemu, jak i jego kodu źródłowego.

Madrake Linux to, obok systemów operacyjnych firmy Red Hat jedna z najpopularniejszych dystrybucji tego systemu operacyjnego. Książka „Mandrake Linux" opisuje tę właśnie dystrybucję. Przedstawia instalację i konfigurację systemu oraz możliwości wykorzystania go w zastosowaniach domowych i profesjonalnych. Opisuje także zasady administrowania systemem Mandrake Linux oraz sposoby używania go w roli serwera sieciowego.

- Instalacja w trybie tekstowym i graficznym
- Konfiguracja systemu
- Graficzne środowiska pracy
- Korzystanie z WWW i poczty elektronicznej
- Pakiet biurowy OpenOffice.org
- Możliwości multimedialne Linuksa
- Narzędzia do archiwizowania danych
- Gry
- Praca z konsolą systemową
- Administracja kontami użytkowników
- Linux w sieci – serwer WWW Apache, firewalle i VPN
- Programowanie w języku powłoki
- Podstawowe zasady programowania w C

Poznaj fenomen Linuksa. Przekonaj się, że bezpłatne oprogramowanie wcale nie musi być gorsze od komercyjnego.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Część I Start systemu 7

Rozdział 1. Instalacja systemu 9

Zbieranie informacji o systemie 11
Wiele systemów operacyjnych 12
Instalacja w trybie tekstowym 13
Instalacja w trybie graficznym 13
Instalacja pakietów w środowisku systemu 33
Instalacja pakietów w środowiskach graficznych KDE oraz GNOME 33
Instalacja pakietów w konsoli systemowej 36

Rozdział 2. Konfiguracja 43

Narzędzia konfiguracyjne 43
Ustawienia języka i ustawienia regionalne 49
Konfiguracja urządzeń 52

Rozdział 3. Środowiska graficzne 61

KDE 62
GNOME 65
WindowMaker 67
IceWM 68
Failsafe 68

Część II Programy użytkowe 69

Rozdział 4. Menedżery plików, przeglądarki WWW i poczta e-mail 71

Konqueror 72
Nautilus 83
Mozilla 88
Galeon 91
Midnight Commander 94
gFTP 100
NCFtp 102
Ximian Evolution 103
Mutt 108

Rozdział 5. Pakiet biurowy OpenOffice.org 113
Edytor tekstu — Writer 113
Arkusz kalkulacyjny Calc 122
Impress 129

Rozdział 6. Narzędzia multimedialne 135
KsCD 135
Xmms 136
Noatun 137
XMovie 138
GIMP 139
Paint 143
GQview 144
Kuickshow 145
K3b — narzędzie do nagrywania płyt 146

Rozdział 7. Archiwizacja danych 149
Ark 149
File Roller 152
Tar 153

Rozdział 8. Gry w Mandrake 157
Frozen Bubble 157
Asteroidy 158
Wyścig węży 159
Pasjans 159
Poker 160
Tuxracer 161
Gnome Mahjongg 161
Miny 161
Inne gry 163

Część III Konsola systemu 165

Rozdział 9. Tryb poleceń, konsola systemowa i dostępne powłoki 167
Powłoki 169
Powłoka BASH 170
Dokańczanie poleceń 171
Historia sesji 171
Zmienne 171
Aliasy 175
Symbole wieloznaczne 175
Przekierowanie wyjścia oraz wejścia 176
Potoki 177
Konfiguracja powłoki 177

Rozdział 10. Obsługa plików i katalogów 179
Struktura katalogów 179
Przeglądanie plików i katalogów 180
Tworzenie, kasowanie, kopiowanie plików i katalogów 183
Prawa dostępu i atrybuty plików 186
System plików i katalogów 189
Procesy 190

Część IV Administracja 195

Rozdział 11. Hasła 197
Grupy i użytkownicy systemu 198
quota 204

Rozdział 12. KCron 207

Rozdział 13. Montowanie urządzeń 211
Montowanie wymienialnego dysku twardego 211
Montowanie CD-ROM-u oraz stacji dyskietek 215
Pliki konfiguracyjne 215
Tworzenie kopii zapasowej 217

Rozdział 14. Zagrożenia i sposoby zabezpieczeń 221
Programy antywirusowe typu Open Source 221
Firewall 226
Szyfrowanie 228
PGP 228
SSL 232

Rozdział 15. Sieć i Internet 237
Nowe połączenie 238
Usuwanie połączenia 239
Zarządzanie połączeniami 240
Monitorowanie połączeń 240

Część V LAN, Internet oraz usługi sieciowe 243

Rozdział 16. OpenSSH 245
VPN 255

Rozdział 17. Apache — Advanced Extranet Server 257
Plik konfiguracyjny serwera Apache 258
Dokumentacja Apache 261

Rozdział 18. DNS 263

Część VI Programowanie 267

Rozdział 19. Programowanie w shellu 269
Słowa kluczowe 271
Zmienne 272
Parametry 274
Instrukcje warunkowe 275
Pętle 277
Przekierowania oraz potoki 279
Wyrażenia matematyczne 280
Funkcje 281
Okna dialogowe 281

Rozdział 20. Programowanie w C 287
Kompilator oraz techniki kompilacji 287
Składnia języka C 291

Rozdział 21. Wstęp do Qt Designer — narzędzie dla programisty 299
Tworzenie 299
Wstawianie obiektu 301
Otwieranie plików 301
Okna dialogowe 302

Dodatki 305

Dodatek A Emulatory 307

Dodatek B Mandrake w internecie i na grupach dyskusyjnych 319

Dodatek C Licencje 323
GNU GENERAL PUBLIC LICENSE 323
Powszechna Licencja Publiczna GNU 329
GNU LESSER GENERAL PUBLIC LICENSE 337

Skorowidz 347

Rozdział 14.

Zagrożenia i sposoby zabezpieczeń

W dzisiejszych czasach, kiedy niemal wszystkie komputery posiadają dostęp do internetu, niezwykle ważną rzeczą jest bezpieczeństwo zarówno komputerów, jak i danych zawartych na ich dyskach. Oddzielnym zagadnieniem jest fizyczny dostęp osoby niepowołanej do systemu. W rozdziale tym zajmiemy się podstawowymi zagadnieniami bezpieczeństwa systemu, ochroną antywirusową oraz programami firewall typu Open Source. Postaramy się skonfigurować zabezpieczenia naszego systemu na tyle, aby poczuć się bezpiecznymi w sieci.

Programy antywirusowe typu Open Source

Za każdym razem, gdy użytkownik systemu nawiązuje połączenie z internetem, naraża system na infekcję wirusa internetowego. Pomimo tego, że wirusy atakujące systemy Linux są niemalże niespotykane w przeciwieństwie do innych konkurencyjnych systemów operacyjnych, jak na przykład Windows, jednak mogą zagrozić systemowi podczas korzystania z zasobów innych systemów.

Istnienie zagrożenia potwierdzić mogą istniejące programy antywirusowe przeznaczone właśnie do wykrywania wirusów. Jednym z takich programów przeznaczonych do konsoli systemowej jest program *Open Source* o nazwie *AntiVir*.

Program AntiVir może zostać pobrany ze strony internetowej znajdującej się pod adresem *http://packetstorm.linuxsecurity.com*. Z programu można korzystać w dwóch opcjach: darmowej — w której zablokowane są niektóre opcje, oraz komercyjnej — udostępniającej wszystkie opcje wyszukiwania wirusów. W celu korzystania z pełnej wersji należy wykupić licencję w firmie oferującej program.

Zgodnie z deklaracjami programu, wykrywa on oraz usuwa następujące rodzaje wirusów:

- *Wirusy sektora rozruchowego* — działanie wirusów sektora rozruchowego (*boot sector*) polega na infekowaniu plików inicjalizujących system, odpowiadających za poprawne uruchamianie systemu.
- *Wirusy rozprzestrzeniające się za pomocą wiadomości e-mail* — program wyszukuje wirusy zawarte w przesyłanych wiadomościach e-mail.
- *Wirusy znajdujące się w makrach* — są to wirusy zawarte w dokumentach różnych pakietów biurowych, jak na przykład OpenOffice czy też StarOffice.
- *Demony ataków DOS* — AntiVir wyszukuje demony służące do przeprowadzania rozproszonych ataków DDoS.

Program AntiVir wyszukuje wirusy we wskazanych przez użytkownika lokalizacjach wykorzystując do tego celu bazę wirusów znajdujących się w katalogu */usr/lib/AntiVir/antivir.vdf*.

Jak każdy program uruchamiany w konsoli systemowej, również AntiVir posiada kilka pożytecznych opcji pozwalających na przyspieszenie jego działania.

Jeżeli zostanie on uruchomiony przez użytkownika bez podania żadnej opcji, zeskanuje on pliki znajdujące się w bieżącej lokalizacji pod kątem znalezienia wirusa.

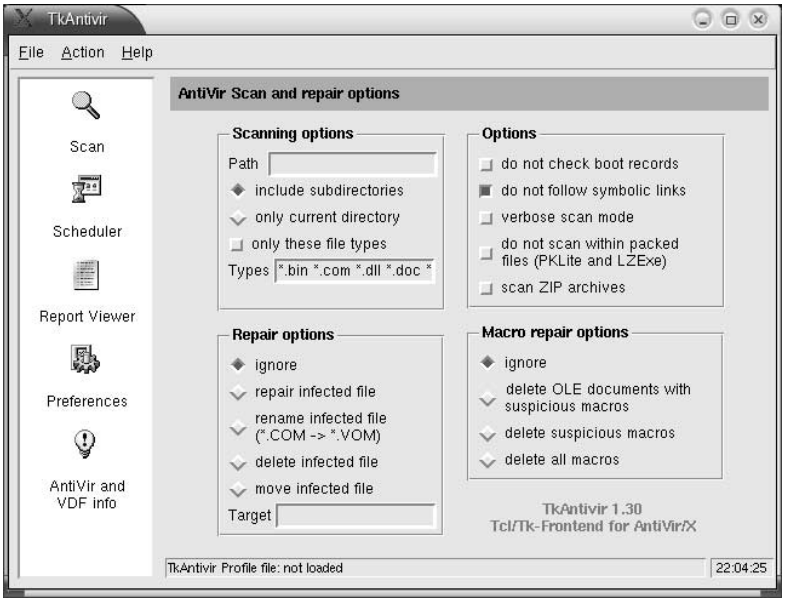
Składnia polecenia służącego do wywoływania programu ma następującą strukturę:

```
antivir [-opcje] [sciezka]
```

Najważniejsze dostępne opcje programu AntiVir:

- `-allfiles` — sprawdza wszystkie pliki znajdujące się w bieżącej lokalizacji.
- `-del` — usuwa zainfekowane pliki.
- `-h` — wyświetla listę wszystkich opcji oraz argumentów programu.
- `-onefs` — sprawdza napędy podłączone do systemu lokalnie.
- `-noboot` — nie sprawdza sektora rozruchowego.
- `-nopack` — nie sprawdza plików znajdujących się w spakowanych archiwach.
- `-r4` — wyświetla bardzo szczegółowe dane wyjściowe o sprawdzanych plikach; jeżeli włączone jest zapisywanie plików dziennika, wszystkie wyświetlone informacje zostaną w nim zapisane.
- `-ren` — zmienia nazwy zainfekowanych plików, których nie udało się naprawić.
- `-ro` — nadpisuje istniejące pliki dziennika, powodując utratę istniejących w nich informacji.
- `-ra` — dopisuje do informacji zawartych w plikach dziennika nowe informacje dotyczące przeprowadzonego skanowania.
- `-rf` — pozwala na określenie ścieżki dostępu do plików dziennika programu.
- `-s` — sprawdzanie podkatalogów odbywa się rekurencyjnie.
- `-z` — skanuje pliki znajdujące się w określonym przez użytkownika archiwum.

Innym programem antywirusowym przeznaczonym dla systemów z rodziny Linux, w tym również dla Mandrake Linux 10.0, jest program *TkAntivir*. Jest to program, który w odróżnieniu od AntiVir pracuje w środowisku graficznym oferując użytkownikowi wygodny w pracy interfejs. Wygląd programu TkAntivir przedstawia rysunek 14.1.



Rysunek 14.1. *Główne okno programu TkAntivir*

Program TkAntivir może zostać pobrany z witryny internetowej znajdującej się pod następującym adresem:

http://www.sebastian-geiges.de/tkantivir/index_en.html.

Jak widać na rysunku, interfejs programu nie jest zbyt skomplikowany, pozwoli on użytkownikowi na intuicyjne obsługiwanie programu.

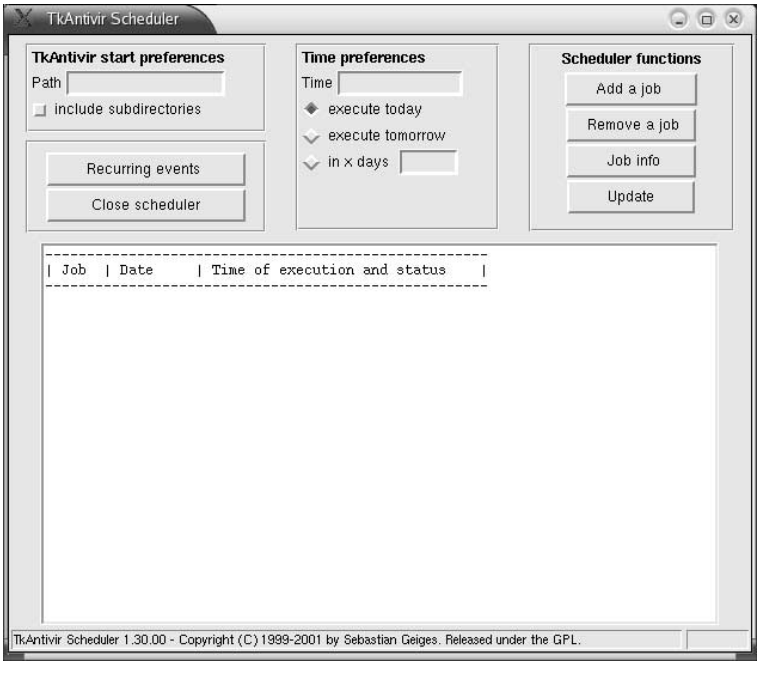
Lewa część okna zawiera wszystkie dostępne opcje programu. Zajmijmy się na początku poleceniem *Scan*, którego opcje domyślnie zostały podzielone na sekcje i znajdują się w prawej części okna. Pierwsza sekcja — *Scanning options* — pozwoli na dokładne określenie lokalizacji, która ma zostać sprawdzona przez system. Chcąc sprawdzić konkretną lokalizację, należy w polu *Path* wpisać odpowiednią ścieżkę wskazującą na wybrany katalog. Zaznaczenie opcji *includes subdirectories* sprawi, że podczas sprawdzania wybranej lokalizacji zostaną uwzględnione również jej podkatalogi. Sekcja ta może posłużyć również do sprawdzenia tylko wybranych typów plików (plików o wybranych rozszerzeniach) — służy do tego opcja *only these file types*.

Kolejną sekcją jest sekcja *Options* —pozwalająca na pominięcie sprawdzania sektora rozruchowego oraz pominięcie sprawdzania plików, do których odnoszą się linki symboliczne, co z całą pewnością skróci czas skanowania. W tej sekcji użytkownik może również określić, czy chce, żeby były sprawdzane pliki znajdujące się w archiwach PKLite, LZExe oraz ZIP. Zaznaczenie opcji *verbose scan mode* pozwoli na wyświetlanie przez program dokładniejszych komunikatów o sprawdzanych plikach i zapisywanie ich w plikach dzienników.

Sekcja *Repair options* (opcje naprawy) pozwala użytkownikowi na dokładne określenie działania programu TkAntivir w momencie wykrycia wirusa. Domyślnie zaznaczoną opcją jest opcja *ignore*, która sprawi, że program po odnalezieniu pliku będącego potencjalnym zagrożeniem oprócz powiadomienia o tym w stosownym komunikacie nie podejmie żadnych działań. Zalecalibyśmy, aby opcja ta pozostała zaznaczona, wynika to z faktu, iż skaner antywirusowy może być podatny na fałszywe alarmy. Usuwanie więc lub zmienianie nazwy każdego pliku uznanego za zainfekowany może wiązać się z przykrymi konsekwencjami, szczególnie wtedy, gdy usunięty plik okaże się ważnym plikiem systemowym lub ważnym dokumentem jednego z użytkowników systemu.

Ostatnią już sekcją znajdującą się w tym oknie jest *Macro repair options*; opcje znajdujące się w tej sekcji są analogiczne do tych omówionych powyżej, z tą tylko różnicą, że odnoszą się do wirusów pojawiających się w makrach złożonych dokumentów.

Kolejną ikoną znajdującą się w lewej części okna jest *Scheduler*, po wybraniu której zostanie automatycznie uruchomiony terminarz (rysunek 14.2).



Rysunek 14.2. *Oko terminarza programu*

Za pomocą terminarza można wykonać następujące czynności:

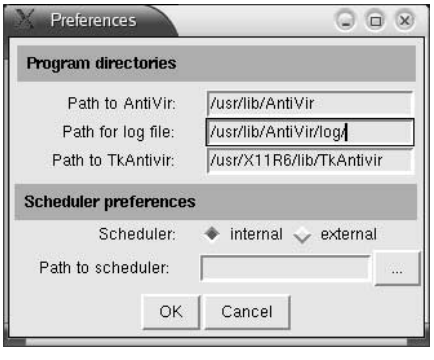
- *Wybrać ścieżkę, do której odnosić się będzie wybrane zadanie* (*TkAntivir start preferences*) — wpisanie odpowiedniej ścieżki w polu *Path* pozwoli określić lokalizację, której dotyczyć będzie dodane w terminarzu zadanie.
- *Określić, kiedy program ma zostać automatycznie uruchomiony* (*Time preferences*) — w tym miejscu użytkownik może dokładnie zdefiniować, kiedy program będzie automatycznie uruchamiany. W polu *Time* należy wpisać dokładną godzinę, a następnie zaznaczyć jedną z opcji pozwalających

na uruchomienie programu dzisiaj (*execute today*), w następny dzień (*execute tomorow*) lub przez następne kilka dni (*in x days*). Kliknięcie przycisku *Recuring events* sprawi, że wybrane zadanie będzie uruchamiane z określoną częstotliwością, np. raz w tygodniu.

- *Skorzystać z jednej z funkcji terminarza* (*Scheduler functions*) — użytkownik ma do wyboru jedną z czterech dostępnych opcji — może dodać nowe zadanie (*Add a job*), usunąć istniejące zadanie (*Remove a job*), uzyskać szczegółowe informacje o wybranym zadaniu (*Job info*) oraz zaktualizować listę zadań (*Update*).

Zakładka *Preferences* (właściwości – rysunek 14.3) znajdująca się w lewej części głównego okna programu umożliwia zamianę położenia (ścieżki dostępu) do pliku wykonywalnego programu, biblioteki zawierającej listę wirusów oraz plików z logami programu.

Rysunek 14.3.
Okno Preferences



Aby móc korzystać z terminarza znajdującego się w programie TkAntivir, należy podać odpowiednią ścieżkę do katalogu mającego zawierać przyszłe logi programu. W tym celu przed jego uruchomieniem z konsoli systemowej należy utworzyć odpowiedni katalog — posłuży do tego polecenie:

```
mkdir /usr/lib/Antivir/log/
```

Następnie w oknie *Preferences* programu należy wpisać ścieżkę `/usr/lib/Antivir/log/`, zakończy to konfigurację programu i pozwoli na korzystanie ze wszystkich jego możliwości.

Wybór zakładki *Scan* spowoduje rozpoczęcie skanowania wybranej lokalizacji przez program TkAntivir, po zakończeniu procesu sprawdzania zostanie wyświetlone nowe okno zawierające informacje o przeprowadzonym procesie. Przykładowy log odnoszący się do zakończonego procesu skanowania przedstawiony został poniżej.

```
AntiVir/Linux Version 6.7.0.1, (Apr 22 2001, 19:14:45)
Copyright(c) 1994-2001 by H+BEDV

Datentechnik GmbH

Report created on 02/12/2004 16:27:08

Command line: // -allfiles -nolnk

-rf/usr/lib/AntiVir/log//avlinux.log
-ro
```

```
Loading /usr/lib/AntiVir/antivir.vdf ...

AntiVir is running in non-key-mode.

The option -nolnk is not supported in non-key-mode.
VDF

version: 6.7.0.1 - FUP(0), created 04/19/2001

checking drive/path (list): //

----- scan

results -----
 directories:        652
       files:        5693
    infected:        0
   scan

time: 00:04:51
--------------------------
```

Najważniejsza dla użytkownika część logu znajduje się po słowie `scan`, ponieważ poniżej tego słowa zostały zamieszczone informacje o rezultatach działania programu. Użytkownik może dowiedzieć się na przykład, ile katalogów objęło skanowanie oraz ile plików zostało sprawdzonych. Na samym końcu statystyki znajduje się czas, w jakim zostało przeprowadzone skanowanie.

Korzystając z programu antywirusowego — niezależnie od tego, czy będzie to program AntiVir lub TkAntivir, czy też inny program antywirusowy — użytkownik powinien pamiętać o regularnym aktualizowaniu bazy definicji wirusów. Aktualizacja bazy wirusów odbywa się najczęściej poprzez połączenie się programu z internetem i automatycznym pobraniu przez niego odpowiednich plików. Jeżeli program nie posiada opcji automatycznej aktualizacji, użytkownik będzie musiał odwiedzić stronę główną programu i pobrać z niej odpowiednie uaktualnione definicje wirusów. Należy umieścić je w odpowiednim katalogu programu usuwając już nieaktualne pliki i zastępując je nowymi pobranymi z internetu.

Dopiero program antywirusowy z aktualną bazą wirusów będzie mógł skutecznie chronić nasz system przed różnego rodzaju wirusami oraz makrami.

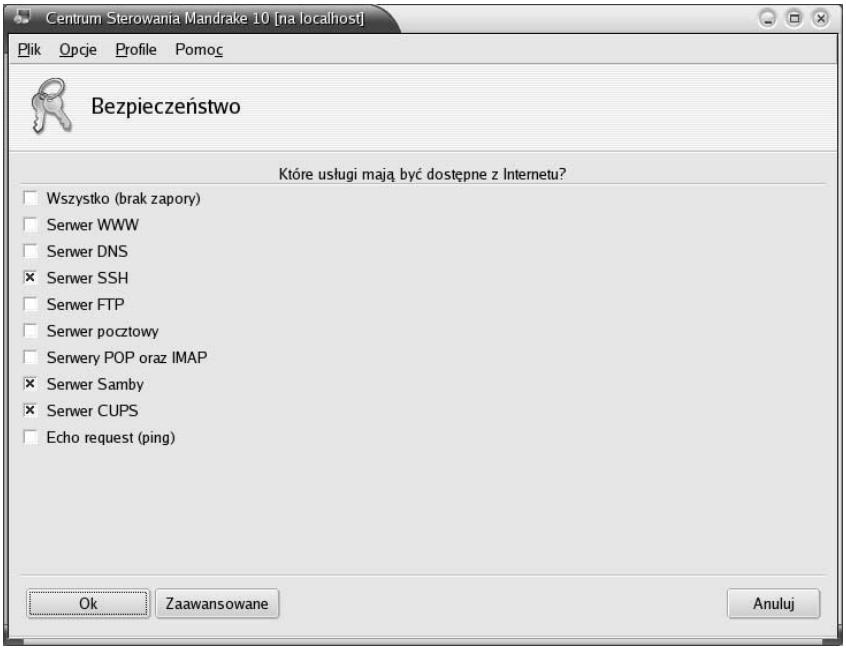
Firewall

Łącząc się globalną siecią, jaką jest internet, narażamy swój system na różnego rodzaju zagrożenia, wśród których można wyróżnić m.in. włamania do systemu oraz blokadę usług *DoS*. Nie zawsze jesteśmy świadomi, że ktoś miał nieautoryzowany dostęp do naszego systemu. Jeżeli chodzi natomiast o blokowanie usług (DoS), to ma ona na celu uniemożliwić naszemu komputerowi poprawne działanie.

Dlatego też aby zapobiec takim zagrożeniom, zaleca się instalowanie w systemach programów firewall (zapór sieciowych), które są podstawowym mechanizmem zabezpieczenia systemów przed agresją pochodzącą z internetu.

Systemy operacyjne z rodziny Linux, w tym również Mandrake Linux 10.0, wspierają tworzenie zapór sieciowych w systemach poprzez na przykład przekazywanie, maskaradę (zmianę nagłówków IP) czy też filtrowanie pakietów oraz wykorzystanie Ipchains i Iptables w celu stworzenia firewalla.

Dystrybucja Mandrake Linux zawiera standardowo dołączoną aplikację firewall o nazwie *Ściana ogniowa*. Znajduje się ona w *Centrum Sterowania Mandrake* w części *Bezpieczeństwo* i jej głównym zadaniem jest pomoc użytkownikowi i usprawnienie procesu konfiguracji zapory sieciowej. Po uruchomieniu programu *Ściana ogniowa* zostanie wyświetlony komunikat, aby przed kontynuowaniem konfiguracji zapory sieciowej upewnić się, że zostało skonfigurowane połączenie z internetem, a jeżeli to nie zostało zrobione, żeby takie połączenie utworzyć. Kolejne okno konfiguracyjne widoczne na rysunku 14.4 pozwala na wybór usług, które będą dostępne podczas połączenia z internetem. Pozwala tym samym na wykluczenie usług mogących obniżyć bezpieczeństwo systemu.



Rysunek 14.4. *Okno konfiguracji zapory sieciowej*

Wśród usług znajdujących się na liście są między innymi takie usługi, jak:

- *Serwer WWW*.
- *Serwer DNS*.
- *SSH*.

- *FTP*.
- *Serwer pocztowy*.
- *Serwer POP oraz IMAP*.
- *Telnet*.
- *SAMBA*.

Zaawansowani administratorzy systemu mogą kliknąć przycisk *Zaawansowane* — spowoduje to pojawienie się dodatkowego pola tekstowego, w którym mogą wpisać kolejne porty, które mają być otwarte podczas połączenia z internetem. Należy je wpisać oczywiście tylko wtedy, gdy odpowiadające portom usługi nie znalazły się na umieszczonej wyżej liście. Przyciśnięcie przycisku *OK.* spowoduje zakończenie procesu konfiguracji standardowej zapory sieciowej systemu Mandrake Linux.

Szyfrowanie

Szyfrowanie jest jednym z ważniejszych zagadnień związanych z bezpieczeństwem przesyłanych przez internet pod różnymi postaciami danych. Nie stanowi ono stuprocentowego zabezpieczenia, jednak znacznie utrudnia wykorzystanie danych po ich przechwyceniu przez osobę niepowołaną. Podstawą poprawnego szyfrowania przesyłanych informacji jest poprawna konfiguracja narzędzi szyfrujących, a do tego celu niezbędna jest znajomość kilku podstawowych terminów i informacji związanych z szyfrowaniem.

Na początku przyjrzyjmy się dwóm podstawowym typom szyfrowania, wśród których możemy wyróżnić szyfrowanie:

- *Symetryczne* — ten typ szyfrowania wykorzystuje jeden pojedynczy klucz zarówno do szyfrowania, jak i deszyfrowania informacji. Ten sposób szyfrowania jest najprostszym i najbardziej popularnym sposobem szyfrowania danych, jednak wiąże się z nim pewne niebezpieczeństwo. Jeżeli podczas transmisji klucz zostanie przechwycony, to osoba będąca w jego posiadaniu może rozszyfrować przesyłane wiadomości.
- *Asymetryczne* — szyfrowanie to wykorzystuje dwie powiązane ze sobą pary kluczy do szyfrowania i deszyfrowania informacji. Ten rodzaj szyfrowania jest powszechnie stosowany podczas przesyłania danych w internecie i sieciach lokalnych.

PGP

Jednym z najbardziej popularnych programów służących do szyfrowania przesyłanych informacji w formacie elektronicznym, takich jak na przykład wiadomości e-mail, jest program *PGP* (*Pretty Good Privacy*).

Obrazowo działanie programu PGP można przedstawić jako zamianę tekstu znajdującego się w dokumencie elektronicznym na ciąg odpowiadających znaków. Taki ciąg znaków jest całkowicie nieczytelny, ponieważ litery alfabetu wchodzące w jego skład zostały pozamieniane według określonego schematu. Schemat, według którego następuje zamiana, jest ściśle określony w haśle użytkownika, które jednocześnie staje się pewną regułą, według której następuje zamiana znaków. Oczywiste jest, że to samo hasło musi posiadać osoba szyfrująca dane oraz osoba chcąca te dane odczytać. Pojawia się więc w tym miejscu problem, jak bezpiecznie przekazać hasło służące do odszyfrowywania danych drugiej stronie. Najlepszym rozwiązaniem byłoby osobiste przekazanie klucza, ale nie zawsze taka sytuacja jest możliwa.

Dlatego też zostały utworzone klucze publiczne, za pomocą których można w bezpieczny sposób przekazać hasło — klucz szyfrujący bez konieczności jego osobistego przekazywania. Stosuje się do tego metodę pary kluczy, która opiera się na istnieniu dwóch „pasujących" do siebie kluczy, a mianowicie klucza prywatnego oraz klucza publicznego. Klucz publiczny służy do szyfrowania danych, które mogą zostać odszyfrowane tylko pasującym kluczem prywatnym. Dlatego też klucz publiczny może być dowolnie rozpowszechniany bez obawy, że zaszkodzi to bezpieczeństwu naszych informacji, ponieważ jego posiadanie nie da możliwości odszyfrowania danych, a jedynie ich zaszyfrowania.

Jeżeli chodzi natomiast o klucz prywatny, to należy go przechowywać tylko dla własnego użytku i nie przesyłać innym użytkownikom. Dodatkowo klucz ten jest chroniony osobistym hasłem znanym tylko przez właściciela klucza. Za każdym razem, kiedy będzie on chciał użyć klucza, będzie musiał podać właśnie to hasło.

Instalacja

Program PGP użytkownik może pobrać ze strony znajdującej się pod adresem:

http://web.mit.edu/network/pgp-form.html.

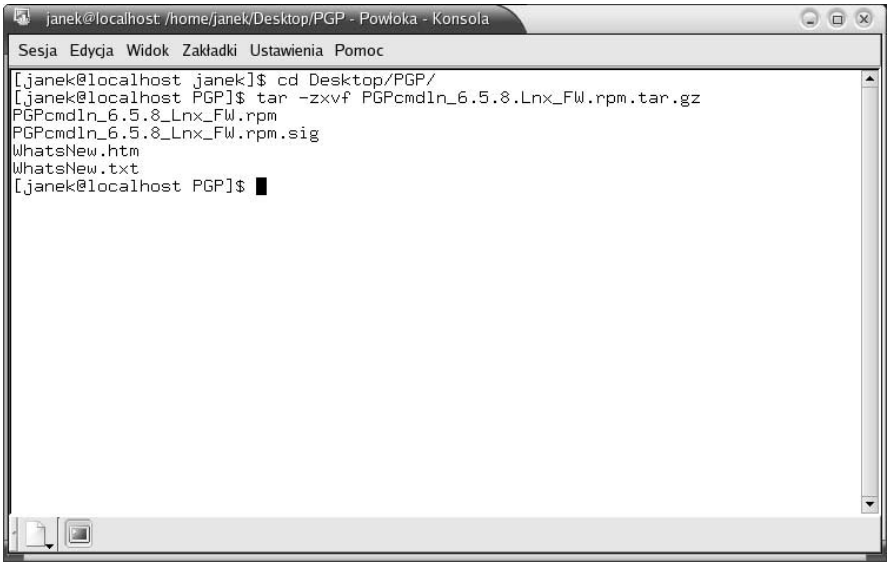
Po pobraniu i zapisaniu na dysku można przejść do instalacji ściągniętego pakietu. Jeżeli ściągnięty plik to pakiet *rpm*, pierwszą czynnością, jaką należy wykonać, jest jego rozpakowanie. Posłuży do tego następujące polecenie wydane z konsoli systemowej, którego działanie przedstawia rysunek 14.5.

```
tar -zxvf PGPcmdlr_6.5.8.Lnx_Fw.rpm.tar.gz
```

Po rozpakowaniu archiwum do konkretnego katalogu pojawi się w nim pakiet *rpm* oraz pliki tekstowe zawierające opis wszystkich nowości wprowadzonych w konkretnej wersji programu. Kolejną czynnością, jaką należy wykonać, jest instalacja pakietu; operację tę można wykonać zarówno w środowisku graficznym, jak i konsoli systemowej. Tutaj przedstawiono instalację pakietu w konsoli systemowej, a to z tego względu, iż po skończonej instalacji przeprowadzona zostanie w niej konfiguracja programu.

Pełnym poleceniem inicjalizującym proces instalacji pakietu w naszym przypadku jest:

```
rpm -ivh PGPcmdlr_6.5.8.Lnx_Fw.rpm
```



Rysunek 14.5. *Rozpakowywanie pakietu rpm programu PGP*

Po zainstalowaniu pakietu wydajemy w konsoli kolejne polecenie, którego zadaniem będzie utworzenie pary kluczy:

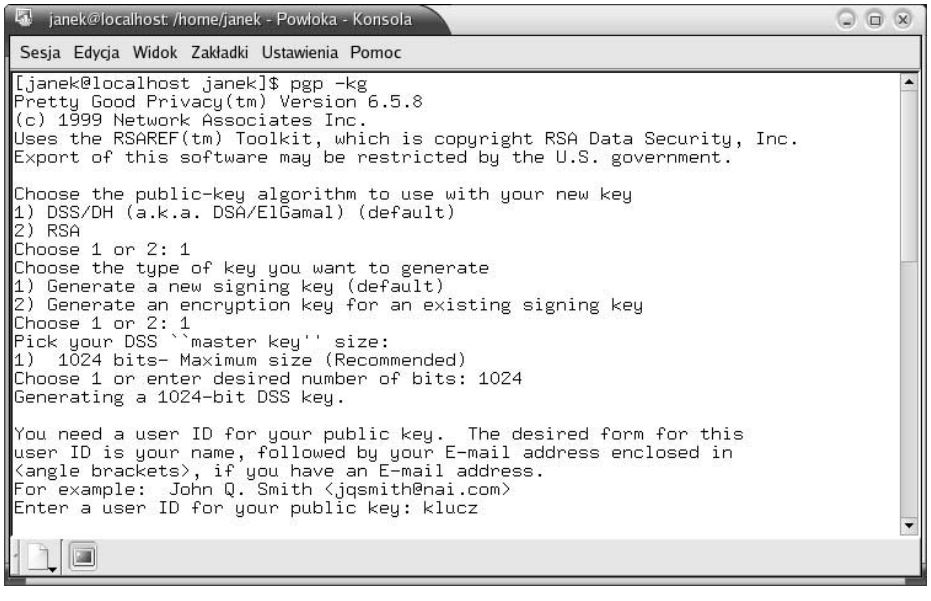
```
pgp -kg
```

Spowoduje to wyświetlanie przez program kolejnych komunikatów odnoszących się do tworzonych kluczy.

1. *Choose the public key algorithm to use with your new key* — dotyczy algorytmu szyfrowania wykorzystywanego przez nowo tworzony publiczny klucz. Należy w tym miejscu zaznaczyć opcję domyślną, a mianowicie — *DDS/DH*.
2. *Choose the type of key you want to generate* — należy wybrać pierwszą opcję, czyli tworzenie nowego klucza służącego w przyszłości do podpisywania.
3. *Pick your DSS "master key"size* — należy wpisać długość naszego klucza zgodnie z zaleceniami: *1024* i potwierdzić to klawiszem *Enter*.
4. *Enter the validity period of your signing key in days from 10-950* — w tym miejscu należy wpisać, jak długo ma być ważny nowo tworzony klucz; wpisujemy wartość 0, która spowoduje, że klucz ten nie będzie miał takiego ograniczenia.
5. *Enter pass phrase* — program poprosi nas o wpisanie hasła, a następnie powtórzenie go. Wpisywane hasło powinno być zgodne z tym, o czym była mowa już wcześniej podczas omawiania odpowiednich haseł systemowych, czyli powinno posiadać odpowiednią liczbę znaków i co najmniej jeden znak alfanumeryczny.
6. *Do you also require an encryption key?* — zostaliśmy zapytani, czy potrzebny jest nam również klucz szyfrujący; odpowiadamy, że tak — klawisz *Y* — i naciskamy klawisz *Enter*.

7. *Pick your DH key size* — wybór długości klucza szyfrującego zależy tylko i wyłącznie od użytkownika, jednak przed wybraniem którejś z opcji należy pamiętać, że im dłuższy klucz zostanie wybrany, tym dłużej trwać będzie proces szyfrowania informacji. Zaleca się wybór klucza 1024- lub 2048-bitowego.
8. *Enter validity period of your encryption key in days from 0-1095* — podobnie jak w przypadku klucza służącego do podpisywania, wybieramy wartość 0, która spowoduje, że klucz będzie zawsze ważny. Po zatwierdzeniu wyboru klawiszem *Enter* PGP poprosi użytkownika o naciskanie przypadkowych klawiszy do momentu, aż zakończy się proces generowania losowych danych.
9. *Make this the default signing key* — program zapyta, czy użytkownik chce, aby nowo utworzony klucz został domyślnym kluczem służącym do podpisywania. Należy odpowiedzieć twierdząco i potwierdzić swój wybór klawiszem *Enter*. Spowoduje to zakończenie procesu tworzenia nowych kluczy.

Część procesu tworzenia nowych kluczy przedstawia rysunek 14.6.



Rysunek 14.6. *Proces tworzenia nowych kluczy*

Pomyślne zakończenie procesu tworzenia pary nowych kluczy nie kończy jednak procesu konfiguracji programu PGP. Wydając w konsoli polecenie `pgp -kx`, można zapisać utworzony klucz publiczny w wybranym przez siebie pliku. Przykładowy klucz publiczny został zamieszczony poniżej:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 6.5.8

mQGiBEA3xhMRBADm/NWD9Jg+OgRnjzu4AVwhDQIeHSAV+Sgvil833VwT9qUxLFRK
iX+EDko2nD8F4bWy/aKVRqn9nTqHYrdb3/SvXs8E+ZICC6bRJ1DR2Yq/QItUaEDf
lQgtqvvtCpJ2T4EstUGNEppOa9As1LGCcRzoi105gzhapFVKNMjuYnCzwQCg/1UD
94ysdxmOCWVlhuKT86RYbmUD/R4GBTIVofZ4iipXt5oshROwx23i2kbD3BbxbiNw
```

```
F91aFCOL78aPgt+UlYGSZkLFoz+QgX+PyoaRdoChMifVcAP0m2l6FTlBq1GN8N9G
jGoFcgaRns1AHXI31TKl5iIQLm0HVGL69iVjDkWM3VzTfHkiUmJk7xeLEChIlsvx
0tLZA/sFS7W/tSjulbdv+nCaaEYn15WknFjzpjsaErzGZ+YVbRr0rfArw+R5JjNS
YZK5as9DHiy/PyAFJYoDJjxPLNbEhizpC/T8nq7RmxhGj/aCarFk7FzzMEm+Ctyp
aWXGGHfKMUEzt7GW/wOT8/ujxfh0xd5nK/HFVFpEq1cHvamE9bQeSmFuIEtvd2Fs
c2tpIDxqYW5la0Bsb2NhbGhvc3Q+iQBOBBARAgAOBQJAN8YTBAsDAQICGQEACgkQ
xNZkyvPJRYe9OQCghxMz2k45eta9vGbgGH4RP13a8IgAn1hEtDZqC4dpUmYQ2Nj/
vZIEG4zluQENBEA3xhYQBADMlboCyFaazb+PeCmz00eLLRy7g4lUqxF3zy32nyLa
wNQWDH8/5Y1cAbHMWKsQrR54z9kwtZniTuXQ7FzJr7fulleWkBoWOoHUW3xOOmjV
pGSo7FTG0mxTqBo58/WnT78CGzSgG2wbPxbG2agFAehXS9UOyvHFx2xIxct2v+p8
XwACAgP/bSCZg10zIw3f8AQH+8WSzJbFYcXCHyx7MWCIAGkVyf6I4L/34rbg++LG
IWnUYsZAjTN+tyj0QjYCm+EhORnzRlicewOMY/rcM7rwdexIUZ4reYO4EirMig0c
xbklbIotjDJ6dkBfjs6xmiK78uaXGZMhQoU0dtauS4Xm9yOGDzmJAEYEGBECAAYF
AkA3xhYACgkQxNZkyvPJRYcYhgCfV3MH/j3n7uUMnmzwVMDIjNJwdKoAnAvSw7H7
Zkjhc4H/0vz1/6rLKBPR
=a08t
-----END PGP PUBLIC KEY BLOCK-----
```

Zarządzanie programem PGP odbywa się tylko i wyłącznie z poziomu konsoli systemowej, dlatego też warto zapoznać się z dostępnymi parametrami polecenia.

Składnia polecenia przedstawia się następująco:

```
pgp -opcje
```

Ważniejsze dostępne opcje to:

- `-e nazwa_pliku` — deszyfruje zaszyfrowany plik określony przez parametr `nazwa_pliku` przy użyciu klucza publicznego.
- `-kg` — generuje parę kluczy użytkownika — klucz prywatny oraz klucz publiczny.
- `-o nazwa_pliku` — deszyfruje zaszyfrowany plik lub sprawdza poprawność podpisu.
- `-s nazwa_pliku` — podpisuje wybrany plik i jednocześnie go szyfruje przy użyciu klucza użytkownika.
- `-h` — wyświetla wszystkie dostępne parametry wraz z krótkim opisem.

SSL

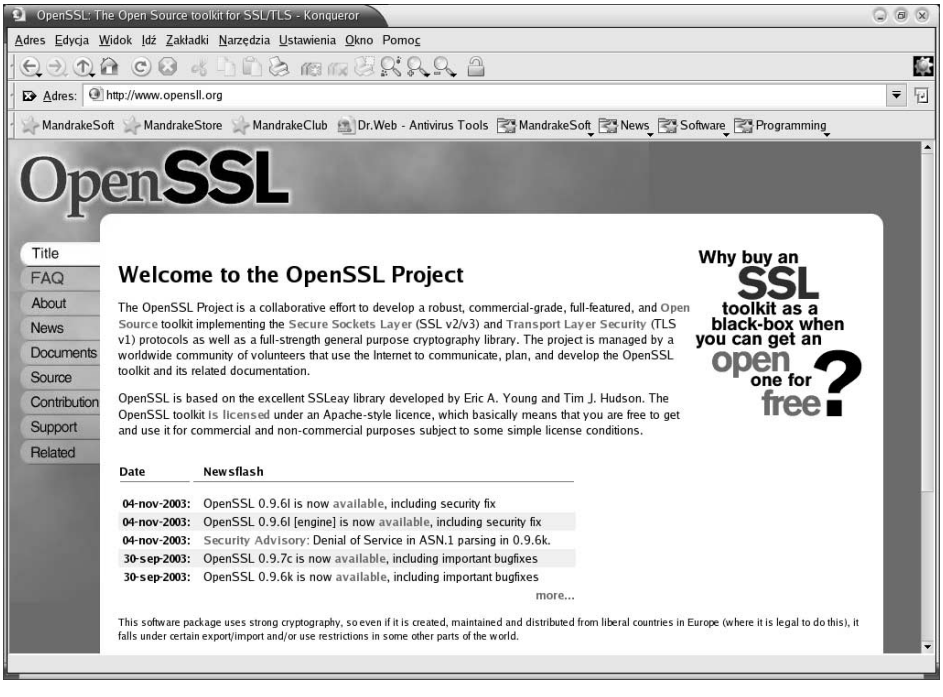
Protokół *SSL* (*Secure Socket Layer*) może posłużyć jako kolejny sposób na zaszyfrowanie transmisji, w której przesyłane są dane użytkownika oraz jego hasła. Protokół ten wykorzystuje się do tworzenia bezpiecznych stron internetowych, które spotkać można robiąc na przykład zakupy internetowe. SSL zostało stworzone po to, aby na bieżąco szyfrować wszystkie dane, po ustanowieniu sesji pomiędzy klientem a serwerem wykorzystuje parę kluczy prywatnych oraz publicznych.

Dużą zaletą protokołu SSL jest jego otwartość i rozszerzalność, czyli brak przywiązania do tylko jednego konkretnego algorytmu szyfrowania informacji. Sprawia to, że podczas połączenia ze stroną internetową protokół pozwala na wybór najbardziej odpowiedniego algorytmu. Klient SSL łącząc się z konkretnym serwerem może przedstawić mu całą listę obsługiwanych algorytmów, na przykład DES, 3DES, natomiast rolą serwera będzie wybór jednego z nich obsługiwanego również przez serwer.

Strona, na której można znaleźć dodatkowe informacje o protokole SSL, znajduje się pod adresem:

www.openssl.org.

Strona pokazana została na rysunku 14.7.



Rysunek 14.7. *Strona główna projektu OpenSSL*

Protokół SSL oraz inne protokoły szyfrujące korzystają z dwóch rodzajów szyfrowania: szyfrowania symetrycznego (z jednym kluczem szyfrująco-deszyfrującym) oraz asymetrycznego (z kluczem prywatnym oraz publicznym). Szyfrowanie asymetryczne wykorzystywane jest do uwierzytelniania stron internetowych oraz do bezpiecznej wymiany klucza symetrycznego, który jest niezbędny do zaszyfrowania strumienia danych.

Typowa sesja za pomocą protokołu SSL przebiega w następujący sposób:

1. Nawiązanie przez klienta połączenia z serwerem.
2. Wymiana informacji o obsługiwanych szyfrach i certyfikatach tożsamości.
3. Uzgodnienie wspólnego zbioru obsługiwanych algorytmów.
4. Potwierdzenie tożsamości serwera przez klienta na podstawie otrzymanych od niego informacji (działa to również w drugą stronę, czyli do uwierzytelnienia klienta przez serwer).

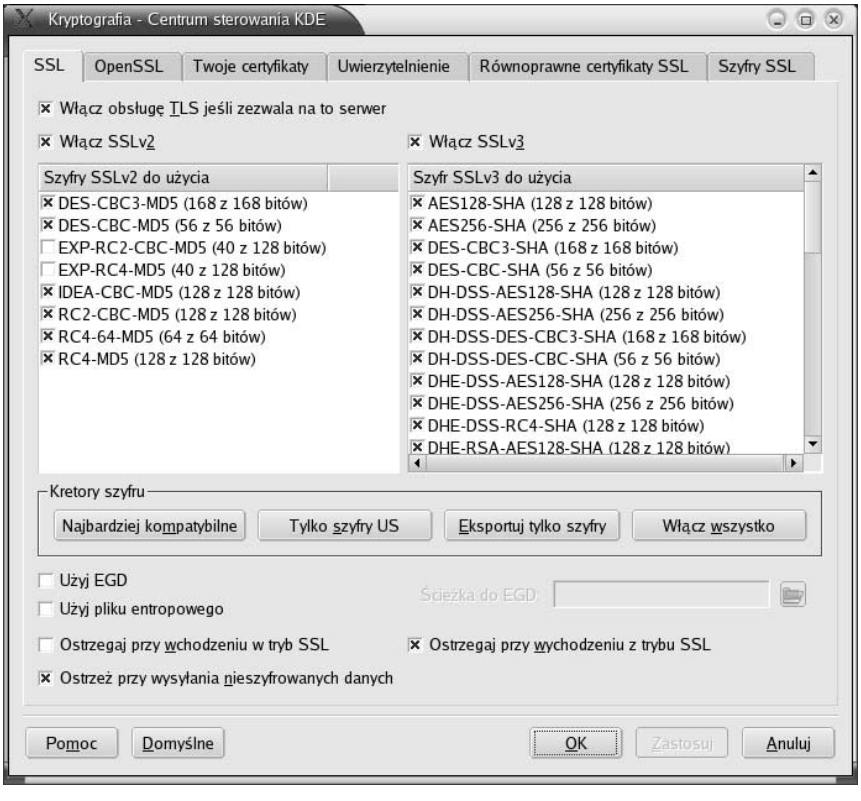
5. Wymiana kluczy sesyjnych (*session keys*), które zostały wygenerowane w sposób losowy.

6. Rozpoczęcie transmisji całkowicie szyfrowanej za pomocą wygenerowanych wcześniej kluczy.

System operacyjny Mandrake Linux pozwala na bardzo szybką konfigurację metod szyfrowania w trybie graficznym. Aby uruchomić program służący do tego celu, należy rozwinąć menu systemowe w sposób podany poniżej i wybrać odpowiednią aplikację — *Kryptografia*:

System/Konfiguracja/KDE/Bezpieczeństwo/Kryptografia.

Po wykonaniu tej czynności zostanie otwarte nowe okno widoczne na rysunku 14.8, w którym użytkownik będzie miał możliwość konfiguracji metod szyfrowania według własnych potrzeb.



Rysunek 14.8. *Konfiguracja metod szyfrowania w środowisku graficznym*

Okno to zostało podzielone na sześć tematycznych zakładek:

- *SSL* —pozwala między innymi na określenie szyfrów wykorzystywanych przez SSL, za jej pomocą można również skorzystać z kreatora szyfru, który pozwoli na włączenie wszystkich szyfrów lub tylko tych najbardziej zgodnych.
- *OpenSSL* — za pomocą tej zakładki użytkownik ma możliwość zmiany ścieżki dostępu do bibliotek OpenSSL.
- *Twoje certyfikaty* —umożliwia użytkownikowi import istniejących i wybranych przez siebie certyfikatów.
- *Uwierzytelnienie* — jeżeli użytkownik chce dokonać zmian w obsłudze certyfikatów, to posłuży mu do tego celu właśnie ta zakładka.
- *Równoprawne certyfikaty SSL* — pozwala na określenie uprawnień oraz ważności certyfikatów.
- *Szyfry SSL* — za pomocą tej zakładki można usuwać istniejące oraz importować nowe szyfry SSL.