T: Szyfrowanie danych. Prywatne kanały danych.

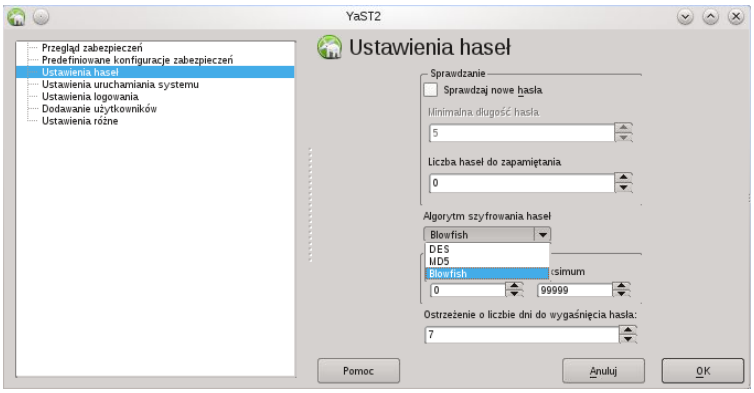
Kryptografia (krypto – ukryty, graphia – pismo) jest to nauka zajmujące się tworzeniem wiadomości w taki sposób, aby tylko upoważnione osoby mogły je odczytywać.

Szyfr (inaczej kryptograficzny algorytm szyfrujący) – jest to funkcja matematyczna wykorzystywana do szyfrowania tekstu jawnego lub jego deszyfrowania. Zazwyczaj jedna funkcja wykorzystywana jest do szyfrowania, a inna do deszyfrowania wiadomości. Wiadomość przed zaszyfrowaniem nazywana jest tekstem jawnym, zaś wiadomość zaszyfrowaną nazywamy szyfrogramem. Proces zamiany tekstu jawnego na szyfrogram nazywamy szyfrowaniem.

Zadanie1:

Odszukaj w serwisie Wikipedii wyjaśnień następujących haseł:

- DES (Data Encryption Standard),
- 3DES,
- BLOWFISH,
- IDEA,
- ARCFOUR,
- TWOFISH (SSH2).



Programy przeznaczone do szyfrowania danych, umożliwiają szyfrowanie wybranych plików lub całych dysków, niektóre pracują przy tym "w locie", co oznacza, że użytkownik mając zabezpieczone w pełni zasoby może z nich korzystać identycznie jak w przypadku zasobów niezabezpieczonych. Większość programów wykorzystuje tak silne algorytmy szyfrujące, że praktycznie nie ma możliwości, aby dane zostały odczytane przez osoby niepowołane.

DES (Data Encryption Standard) jest szyfrem blokowym z blokami o długości 64 bitów. Do szyfrowania i deszyfrowania danych wykorzystywanych jest 56 bitów klucza, który zapisany jest w postaci 64 bitowego ciągu, w którym co 8 bit jest bitem kontrolnym i może służyć do kontroli parzystości.

3DES – wykorzystujący do szyfrowania i deszyfrowania trzy klucze. Najpierw wiadomość jest szyfrowana pierwszym kluczem, następnie deszyfrowana drugim i ponownie szyfrowana trzecim kluczem. Szyfrogram uzyskany w ten sposób jest dużo bezpieczniejszy, ponieważ DES nie tworzy grupy.

Blowfish to szyfr blokowy stworzony przez Bruce'a Schneiera w 1993 roku jako szybka i bezpłatna alternatywa dla istniejących ówcześnie algorytmów. Algorytm operuje na 64-bitowych blokach i używa kluczy od 32 do 448 bitów.

Zadanie2:

Zapoznaj się z informacjami na temat IPsec publikowanymi w serwisie internetowym Wikipedii.

Zadanie3:

Zapoznaj się z zawartością następujących witryn internetowych:
http://www.elektroda.pl/rtvforum/topic1237904.html
http://www.szarp.com.pl/howto/howto/html/ssh.html
http://support.microsoft.com/kb/314076/pl

Zadanie4:

Odszukaj w serwisie internetowym Wikipedia informacje na temat sieci VPN (ang. Virtual Private Network).

Ciekawostka:

Oprogramowania kryptograficznego nie można umieszczać na serwerach w USA ze względu na tamtejsze ograniczenia eksportowe, traktujące tego typu programy jak zwykłą broń.