INFORMACJE TECHNICZNE

Szyfrowanie – sposób ochrony informacji przed zinterpretowaniem ich przez osoby niepowołane. Proces szyfrowania polega na przekształceniu informacji (jawnej) w inną (tzw. kryptogram lub tekst zaszyfrowany) za pomocą funkcji matematycznej oraz hasła szyfrowania (tzw. Klucza)

Deszyfrowanie - proces odwrotny do szyfrowania, polegający na tym, że kryptogram jest przekształcany z powrotem w oryginalną informację jawną za pomocą pewnej funkcji matematycznej i klucza.

Informacje dodatkowe : http://ipsec.pl/leksykon/

AES - (*Advanced Encryption Standard*, nazywany również *Rijndael***),** "iterowany szyfr blokowy", co oznacza, że blok wejściowy oraz klucz przechodzą wielokrotne RUNDY transformacji, zanim wyprodukują wynik. Po każdej rundzie, powstaje szyfr pośredni, zwany STANEM (State).

Informacje dodatkowe : http://pl.wikipedia.org/wiki/AES
http://e-handel.mm.com.pl/crypto/aes.htm

ECB - (*Electronic Code Book),* zalecana tylko dla krótkich i losowych wiadomości. Każdy blok danych wejściowych jest szyfrowany za pomocą tego samego klucza, a dane wejściowe są zapisywane w postaci bloku.

Informacje dodatkowe : http://pl.wikipedia.org/wiki/ECB
http://ipsec.pl/leksykon/ecb.php

CBC - (*Clipher Block Chaining)*, każdy blok szyfrogramu zależy od wszystkich poprzednich bloków wiadomości. Na danym bloku tekstu jawnego jest przed zaszyfrowaniem wykonywana różnica symetryczna z zaszyfrowaną wiadomością z poprzedniego bloku. Wynik tej operacji jest następnie szyfrowany za pomocą zwykłego klucza.

Informacje dodatkowe : http://pl.wikipedia.org/wiki/CBC
http://ipsec.pl/leksykon/cbc.php

CFB - *(Cipher Feedback), t*ryb użycia szyfru blokowego pozwalający na użycie go do kodowania strumieni danych. Szyfr blokowy używany jest do wygenerowania pseudolosowego ciągu danych, który następnie pełni role strumienia szyfrującego, mieszanego z danymi za pomocą pewnej funkcj.

Informacje dodatkowe : http://pl.wikipedia.org/wiki/CFB
http://ipsec.pl/leksykon/ofb.php

OFB - *(Output Feedback),* tryb użycia szyfru blokowego pozwalający na użycie go do kodowania strumieni danych. Szyfr blokowy używany jest do wygenerowania pseudolosowego ciągu danych, który następnie pełni role strumienia szyfrującego, mieszanego z danymi za pomocą pewnej funkcji
Informacje dodatkowe : http://pl.wikipedia.org/wiki/OFB
http://ipsec.pl/leksykon/ofb.php

OPIS UŻYTKOWANIA PROGRAMU

Aby zaszyfrować informację zawartą w określonym pliku należy :

0. wpisać w polu scieżkę dostępu do pliku źródłowego, w którym znajduje się informacja do zaszyfrowania lub kliknąć przycisk [Wybierz] i wtedy otwiera się okno wyszukiwania
1. wpisać w polu scieżkę dostępu do pliku docelowego, w którym ma zostać zaszyfrowana informacja lub kliknać przycisk [Wybierz] i wtedy otwiera się okno wyszukiwania
2. wprowadzić hasło, które bedzie umożliwiało odczytanie informacji
3. wybrać tryb, klikając na odpowiedni skrót (Opis trybów szyfrowania – patrz :Informacje techniczne)
4. kliknąć przycisk [Szyfruj] lub skrót klawiaturowy F2

Aby odszyfrować wcześniej zaszyfrowaną informację należy :

1. wpisać w polu scieżkę dostępu do pliku źródłowego, czyli tego, który podczas szyfrowania był plikiem docelowym lub kliknąć przycisk [Wybierz] i wtedy otwiera się okno wyszukiwania
2. wpisać w polu scieżkę dostępu do pliku docelowego, w którym ma zostać odszyfrowana informacja lub kliknać przycisk [Wybierz] i wtedy otwiera się okno wyszukiwania
3. wpisać hasło, które zostało wprowadzone przy szyfrowaniu
4. kliknąć przycisk [Deszyfruj] lub skrót klawiaturowy F3
5. tryb zostanie automatycznie włączony na ten, w którym zaszyfrowano informcję