e-Nigma

Przeznaczenie:

Program e-Nigma przeznaczony jest do ochrony treści plików (w szczególności dokumentów niejawnych przed dostępem osób trzecich). Ochrona zrealizowana jest poprzez szyfrowanie zawartości pliku kluczem 128 bitowym algorytmu RC4, produkowanym z hasła wprowadzonego przez użytkownika. Praktycznie nieznajomość hasła przy kluczu 128 bitowym nie pozwala poznać treści uprzednio zaszyfrowanego pliku.
RC4 jest szeroko stosowanym algorytmem szyfrowania z kluczem symetrycznym opracowanym przez firmę RSA Data Security Inc. Algorytm ten wykorzystuje jeden klucz do szyfrowania i deszyfrowania informacji i wymaga względnie niewielkiego narzutu obliczeniowego.

Wymagania:

Platforma Microsoft Windows 95/98, Windows NT i pochodne wyższe (Windows 2000, XP, Vista). Internet Explorer 5.5 lub wyższy z siłą szyfrowania 128 bitową lub wyższą.

Funkcjonalność:

Program e-Nigma wkomponowany jest w powłokę Eksploratora Windows oraz programu pocztowego. Ustawienie kursora myszy na dowolny plik i kliknięcie prawym przyciskiem myszy powoduje wyświetlenie menu kontekstowego z poleceniem: Szyfruj dla plików z rozszerzeniem innym niż “.enigma” lub Rozszyfruj – dla plików z rozszerzeniem “.enigma”. Wszystkie składniki oprogramowania instalowane są na C:\Enigma.

Opis działania:

Użykownik wybiera plik do zaszyfrowania lub rozszyfrowania. Wpisuje hasło z potwierdzeniem. Hasło jest haszowane algorytmem MD5. Następnie z otrzymanego hasza generowany jest klucz symetryczny o długości: 128 bitów lub 40 bitów – ustawiane przez użytkownika. Na koniec treść pliku jest szyfrowana kromkami za pomocą algorytmu RC4 kluczem symetrycznym.
Wynikowy plik jest tego samego rozmiaru co źródłowy.
Źródłowy plik po udanym szyfrowaniu jest skasowany – patrz kasowanie pliku źródłowego.
Aby przywrócić treść pliku zaszyfrowanego konieczna jest znajomość hasła którego użyto do szyfrowania. Nieznajomość hasła – uniemożliwia odtworzenie treści pliku.
Hasła nie są przechowywane w systemie.

Moc szyfrowania

Ważną sprawą dla bezpieczeństwa zaszyfrowanych informacji jest długość używanych kluczy (np. 128 bitów). Im klucze są dłuższe, tym trudniej jest informacje odszyfrować. Powszechnie uważa się, że:

1. dla kluczy asymetrycznych: 512 - to zbyt mało, 768 - stosunkowo bezpiecznie,

1024 - silne bezpieczeństwo.

2. dla kluczy symetrycznych: 40 - to zbyt mało, 56 - stosunkowo bezpiecznie, 128 - silne bezpieczeństwo.

Łamanie kluczy metodą brute force (sprawdzanie po kolei możliwych kluczy).

1. Złamanie klucza 40 bitowego zajęło 3 godziny sieci komputerów.
2. Złamanie klucza 56 bitowego (w algorytmie RC5) zajęło 250 dni w ramach jednego z projektów distributed.net. Eksperyment został przeprowadzony przez sieć komputerów, których moc obliczeniowa była równoważna 26 tysięcom komputerów klasy Pentium 200.
3. Złamanie klucza 128 bitowego zajęłoby 1 bilion x 1 bilion lat (za pomocą pojedynczego superkomputera).

Aktualizacje oprogramowania:

Aktualizacje dostępne są z menu Aktualizacje,
lub z lokalizacji: http://www.e-msoft.com

Dane techniczne:

Algorytm szyfrowania: RC4.
Długość klucza: 128 bitów.
Usuwanie oryginalnego pliku: jednokrotne zamazywanie treści jawnej.
Ograniczenie długości pliku: brak ograniczenia.

Znaki towarowe: