Niektóre sposoby ochrony przed inwigilacją w sieci – 1

8 października 2010

Postanowiłem opublikować garść materiałów na temat sposobów ochrony przed inwigilacją w sieci. Być może dla wielu z Was nie są to żadne rewelacje, wierzę jednak, że znajdzie się przynajmniej kilka osób, którym te wiadomości będą przydatne. Tekst ten nie jest w całości mój. Zebrałem po prostu i połączyłem dostępne w sieci informacje. Starałem się w bibliografii wymienić wszystkie źródła z których korzystałem, jeżeli jednak przez przypadek coś, lub kogoś pominąłem to proszę o wyrozumiałość. Zapewniam że w takim przypadku moim celem nie było kopiowanie cudzych prac i prezentowanie ich jako swojego dorobku. Moim celem jest jedynie propagowanie wiedzy, którą uważam za przydatną dla wszystkich zaangażowanych w walkę z NWO.

SYSTEMY SZYFROWANIA DANYCH

Na temat potrzeby ochrony przesyłanych przez sieć danych nie trzeba się długo rozwodzić. Potrzeba ochrony danych osobowych i zachowania tajemnicy korespondencji jest oczywista dla każdego. Ponieważ w Internecie nie ma możliwości przesłania danych bezpośrednio od nadawcy do adresata, należy przyjąć za pewnik, że osoby niepowołane będą miały do nich dostęp. Pozostaje więc sprawić, że nieuprawniony odbiorca przeglądając przechwycone dane nic z nich nie zrozumie, a zatem należy je zaszyfrować. Istnieje wiele systemów kryptograficznych oferujących możliwość szyfrowania danych, korzystają z nich korporacje, banki i osoby prywatne. Przyjrzyjmy się najpopularniejszym z nich, na pozór wydaje się, że wszystkie są na tyle skomplikowane, że zapewniają skuteczną ochronę. Ale czy na pewno?

DES (Data Encryption Standard) opracowany w latach

siedemdziesiątych w firmie IBM, w ramach konkursu na opracowanie efektywnego kryptosystemu na potrzeby rządu Stanów Zjednoczonych. Po drobnych modyfikacjach wprowadzonych przez NSA, w 1977 roku DES został uznany przez rząd USA za oficjalny standard. Od tej pory jest szeroko wykorzystywany – głównie w świecie finansów i bankowości. Ze względu na jego „siłę" eksport do innych krajów podlega dużym ograniczeniom. Algorytm systemu DES opiera się na 56-bitowym tajnym kluczu, który wykorzystywany jest do kodowania 64-bitowych bloków danych. Operacja przebiega w kilku-kilkunastu etapach, podczas których tekst wiadomości ulega wielokrotnym przeobrażeniom. Tak jak w każdej metodzie kryptograficznej posługującej się kluczem prywatnym, klucz ten musi być znany zarówno nadawcy jak i odbiorcy. Ponieważ dla każdej wiadomości klucz wybierany jest losowo spośród 72 000 000 000 000 000 (72 kwadrylionów) możliwych, wiadomości szyfrowane przy pomocy algorytmu DES przez długi czas uchodziły za niemożliwe do złamania. W roku 1998 grupa Electronic Frontier Foundation dokonała złamania szyfru DES w przeciągu mniej niż 72 h, przy wykorzystaniu specjalnego komputera o ogromnej mocy obliczeniowej zbudowanego za kwotę około 250 tysięcy dolarów. Rok później grupa Distributed.Net, korzystając ze stworzonej w Internecie sieci rozproszonej zbudowanej ze 100 tysięcy komputerów PC dokonała tego samego zadania w 22 h i 15 minut. W 2001 roku naukowcy Michael Bond i Richard Clayton z Cambridge University przedstawili model pozwalający na złamanie DES w czasie mniej niż 10 h. Obecnie długość klucza stanowi największą wadę algorytmu.

AES (Advanced Encryption Standard), nazywany również Rijndael. AES wykonuje 10 (klucz 128 bitów), 12 (klucz 192 bity) lub 14 (klucz 256 bitów) rund szyfrujących substitution-permutation. Składają się one z substytucji wstępnej, permutacji macierzowej (mieszanie wierszy, mieszanie kolumn) i modyfikacji za pomocą klucza. Funkcja substytucyjna ma bardzo oryginalną konstrukcję, która uodparnia ten algorytm na znane ataki kryptoanalizy różnicowej i liniowej. Wiadomo że system

DES został złamany za pomocą kryptoanalizy różnicowej około 20 lat temu. W 2006 opublikowana została praca, w której twierdzi się, że AES nie jest w pełni odporny na atak XSL, ale oszacowanie ilości koniecznych obliczeń obarczone jest dużą niepewnością, w związku z tym oceny, na ile skuteczny jest ten atak, są różne. W 2009 opublikowany zostały dwa nowe ataki z użyciem kluczy pokrewnych (key related attack) redukujące złożoność AES-256 do 2119. W grudniu 2009 opublikowano atak na niektóre sprzętowe implementacje AES umożliwiający odtworzenie klucza ze złożonością 232 przez zastosowanie różnicowej analizy błędów (differential fault analysis).

GPG lub GnuPG (GNU Privacy Guard – Strażnik Prywatności GNU) - wolny zamiennik oprogramowania kryptograficznego PGP. Udostępniony na licencji GPL, pierwotnie rozwijany przez Wernera Kocha. Projekt jest wspierany przez rząd niemiecki. GPG spełnia standard OpenPGP. Obecne wersje PGP (oraz Filecrypt firmy Veridis) mogą współpracować z systemami spełniającymi założenia standardu OpenPGP (takimi jak GPG). Jak jednak często się zdarza w takich sytuacjach, nie wszystkie funkcje nowszego oprogramowania są wspierane przez starsze. Użytkownicy muszą rozumieć te niezgodności i potrafić je obejść. GPG jest stabilnym oprogramowaniem nadającym się do codziennych zastosowań. Często jest zawarte w niekomercyjnych systemach operacyjnych, jak FreeBSD, OpenBSD czy NetBSD, oraz w prawie wszystkich dystrybucjach systemu GNU/Linux. Mimo że podstawowy program GPG działa z linii poleceń, istnieją rozmaite nakładki, udostępniające interfejs graficzny. Na przykład GnuPG zostało zintegrowane z KMail i Evolution – klientami poczty środowisk KDE i GNOME. Wtyczka enigmail pozwala na zastosowanie GPG w Mozilli. Ponieważ mechanizm wtyczek nie jest częścią GPG, ani nie jest specyfikowany w OpenPGP, a twórcy GPG i OpenPGP nie brali udziału w jego tworzeniu, to istnieje możliwość, że użycie enigmail może powodować utratę poziomu bezpieczeństwa zapewnianego przez GPG. Podobne zastrzeżenia dotyczą PGP. GPG szyfruje wiadomości używając asymetrycznych par kluczy generowanych dla

poszczególnych użytkowników. Klucze publiczne mogą być wymieniane na różne sposoby, na przykład przez serwery kluczy w internecie. Należy je wymieniać uważnie, aby uniknąć podszycia się na skutek utraty jednoznacznej zależności między kluczem, a jego właścicielem. Do wiadomości można dołączyć podpis kryptograficzny w celu umożliwienia weryfikacji jej integralności oraz tożsamości nadawcy. Ponieważ GPG można dowolnie rozprowadzać, nie może ono używać opatentowanych lub w inny sposób ograniczonych algorytmów lub oprogramowania. To dotyczy algorytmu IDEA obecnego w PGP niemal od początku. Zamiast tego używane są inne, nieopatentowane algorytmy, takie jak 3DES. Można używać algorytm IDEA przy użyciu darmowej wtyczki, należy jednak wziąć pod uwagę potencjalne efekty opisane wcześniej. Współcześnie wszystkie te programy przechodzą na uważany za znacznie silniejszy (i pozbawiony problemów patentowych) algorytm AES. GPG może być również skompilowane na platformach takich jak Mac OS X i Microsoft Windows. Dla Mac OS X istnieje wolna wersja MacGPG używająca interfejsu OS X i macierzysty klas. Kompilacja oryginalnego GPG na inne systemy nie jest trywialna, ale niektóre kompilatory radzą sobie z tym zadaniem. GPG jest programem do szyfrowania hybrydowego, gdyż używa kombinacji tradycyjnych szyfrów symetrycznych (szybszych) i kryptografii klucza publicznego (łatwa i bezpieczna wymiana kluczy – na przykład przez użycie klucza publicznego odbiorcy do zaszyfrowania klucza sesji używanego tylko raz). Ten tryb pracy jest częścią OpenPGP i był zawarty w PGP od jego pierwszej wersji.

PGP (Pretty Good Privacy całkiem niezła prywatność). Projekt PGP został zapoczątkowany w 1991 przez Philipa Zimmermanna i rozwijany przy pomocy społeczności programistów z całego świata. Wydarzenie to stało się pewnym przełomem – po raz pierwszy zwykły obywatel dostał do ręki narzędzie chroniące prywatność, wobec którego pozostawały bezradne nawet najlepiej wyposażone służby specjalne. Program PGP działał na platformach Unix, DOS i wielu innych, będąc dostępnym całkowicie za darmo, wraz z kodem źródłowym. Od 1994 roku

program był dostępny w polskiej wersji językowej. Począwszy od 2002 roku oprócz wersji bezpłatnej korporacja PGP oferuje również wersje komercyjne, które zawierają między innymi możliwość tworzenia zaszyfrowanych folderów, szyfrowanie całych dysków, automatyczną integrację z programami pocztowymi. Korporacja PGP oferuje to oprogramowanie dla Windows 2000/XP/Vista oraz Mac OS X. Ponieważ korporacja PGP zaprzestała rozwijania wersji dla systemów uniksowych, społeczność internetowa po określeniu standardu w postaci OpenPGP utworzyła równoważną algorytmicznie z oryginalnym PGP jego niezależną implementację pod nazwą GNU Privacy Guard (GPG). PGP pozwala szyfrować i deszyfrować przesyłane wiadomości, podpisywać je cyfrowo, weryfikować autentyczność nadawcy (pod warunkiem, że ten także korzysta z PGP) i zarządzać kluczami. Weryfikacja kluczy opiera się o sieć zaufania (web of trust). Program w wersji komercyjnej oprócz szyfrowania korespondencji elektronicznej pozwala na tworzenie wirtualnych zaszyfrowanych dysków (Virtual Disk), tworzenie zaszyfrowanych archiwów (PGP Zip) oraz w najnowszej wersji pozwala zaszyfrować folder lub całą fizyczną zawartość dysku twardego (PGP Whole Disk). Pozwala również w sposób bezpieczny usuwać zawartość plików z dysków. Wersja ta udostępnia również możliwość przechowywania klucza prywatnego na zewnętrznym kluczu sprzętowym, co pozwala na zwiększenie bezpieczeństwa. Dla większych jednolitych środowisk firma PGP Corp. udostępnia systemy centralnego zarządzania polityką bezpieczeństwa – PGP Universal. Kryptolodzy z czeskiej firmy Decros ogłosili odkrycie poważnego błędu w programie PGP, umożliwiającego – przy spełnieniu specyficznych warunków – ujawnienie klucza prywatnego użytkownika tego programu, a właściwie jego części służącej do podpisywania wiadomości. Wykryty przez czeskich kryptologów błąd umożliwia poznanie klucza bez konieczności łamania samych szyfrów go zabezpieczających. Atak bazuje na fakcie, iż program nie sprawdza integralności pliku z kluczem, tzn. tego, czy klucz nie został przez kogoś zmodyfikowany. Użytkownikowi należy najpierw podstawić w miejsce jego oryginalnego klucza klucz odpowiednio spreparowany, a

następnie przechwycić wiadomość, którą użytkownik podpisał korzystając z fałszywego klucza (i wreszcie podmienić z powrotem fałszywy klucz na prawdziwy, aby zaatakowany użytkownik się nie zorientował). Na podstawie przechwyconej wiadomości można odpowiednim programem w ciągu kilkunastu sekund obliczyć prawdziwy klucz. Właśnie metoda owej modyfikacji klucza oraz wyliczenia prawdziwego klucza na podstawie wiadomości podpisanej fałszywym stanowi rzeczywiste odkrycie czeskich kryptologów.

RSA nazwa pochodzi od pierwszych liter nazwisk jego twórców Rona Rivesta, Adi Shamira oraz Leonarda Adlemana. Jeden z pierwszych i obecnie jeden z najpopularniejszych asymetrycznych algorytmów kryptograficznych, zaprojektowany w 1977 przez. Pierwszy, który można stosować zarówno do szyfrowania jak i do podpisów cyfrowych. Bezpieczeństwo szyfrowania opiera się na trudności faktoryzacji dużych liczb pierwszych. Pierwszą udaną faktoryzację RSA zakończono 2 grudnia 1999 roku w ramach konkursu The RSA Factoring Challenge. Dotychczas największym kluczem RSA jaki rozłożono na czynniki pierwsze jest klucz 768-bitowy. Liczby pierwsze zostały znalezione 12 grudnia 2009 a informacje o przeprowadzonej faktoryzacji opublikowano 7 stycznia 2010 roku. Wykorzystano do tego klaster komputerów; czas zużyty na obliczenia był o 2 rzędy wielkości krótszy od prognozowanego. Potencjalnym zagrożeniem dla RSA jest skonstruowanie komputera kwantowego.

PROGRAM TRUECRYPT

TrueCrypt jest niewątpliwie jedną z najlepszych aplikacji służących zabezpieczaniu swoich danych przed odczytaniem przez niepowołane osoby. Program chroni dane szyfrując je za pomocą jednego z trzech dostępnych algorytmów (AES, Serpent oraz Twofish) lub nawet ich sekwencji. Warto zauważyć, że algorytmy te są w chwili obecnej uważane za silne, co oznacza, że nie znaleziono jak dotąd żadnej innej metody na złamanie któregokolwiek z nich, jak tylko odnalezienie prawidłowego

hasła (czy to metodą brute force, czy słownikową). Co istotne, program jest całkowicie darmowy. W tym przypadku nie jest tak, jak w wielu innych sytuacjach, w których ocenia się program nieco „ulgowo” tylko dlatego, że jest bezpłatny – TrueCrypt może śmiało konkurować na równych warunkach z innymi, komercyjnymi aplikacjami do ochrony danych.

Aplikacja umożliwia tworzenie zaszyfrowanych plików o praktycznie dowolnym rozmiarze (ograniczonym rzecz jasna do pojemności nośnika na których są zapisane), jak i szyfrowanie całych partycji. Ostatnia, długo oczekiwana piąta wersja, umożliwia także szyfrowanie partycji systemowej.

Program dostępny jest w wersjach napisanych pod Windowsa, Linuxa, a od piątej wersji, również Macintosha. Podstawowe jego funkcje (tworzenie zaszyfrowanych woluminów, szyfrowanie partycji oraz, rzecz jasna, ich obsługa) dostępne są we wszystkich wersjach, jednak największą funkcjonalność ma wersja dla systemów Windows, której dotyczy ten artykuł.

Dokładny opis stosowania programu znajdziecie tutaj: http://dyski.cdrinfo.pl/artykuly/truecrypt5/index.php

W przypadku wszystkich opisanych systemów brak jest informacji wskazujących jednoznacznie na ich niezawodność. Z dużą dozą prawdopodobieństwa można założyć, że Echelon potrafi złamać wszystkie systemy. Za takimi wnioskami przemawia zaakceptowanie owych systemów przez NSA lub brak zakazu ich stosowania, co równa się akceptacji. Dla własnego bezpieczeństwa należy więc założyć, że skuteczny sposób szyfrowania danych nie istnieje. A zatem wszystko co przesyłamy przez sieć może być odczytane przez osoby niepowołane. W tej sytuacji każdy użytkownik Internetu powinien samodzielnie rozważyć, czy na pewno chce zaryzykować upublicznienie swoich danych osobowych lub ujawnienie treści prowadzonej korespondencji. Oczywiście programy szyfrujące są przydatne jako ochrona przed różnego rodzaju hackerami lub innymi użytkownikami naszego komputera, jednakże należy mieć

świadomość że ich złamanie jest możliwe.

Ponadto istnieje ryzyko, że użycie programów szyfrujących przez przeciętną osobę może przyciągnąć uwagę systemu. No bo skoro zwykły Kowalski zadaje sobie trud by szyfrować swoją pocztę i dokumenty to logicznie rzecz biorąc znaczy to, że coś ukrywa, a skoro ukrywa to różnego rodzaju służby mogą uznać, że warto zbadać sprawę bliżej.

Mamy więc do czynienia z sytuacją, w której dysponujemy narzędziami pozwalającymi na skuteczną ochronę naszych danych przed zwykłymi użytkownikami sieci włączając w to większość przestępców komputerowych, jednak dla psów gończych systemu nasze dane nadal są dostępne jak na dłoni.

Przeanalizujmy zatem konsekwencje tego stanu rzeczy, przyjmując następujące założenia:

Po pierwsze – w naszej korespondencji lub dokumentach które przesyłamy przez sieć znajdują się treści za które system może nas pociągnąć do odpowiedzialności karnej. Po drugie – wiemy, że system te dane przechwyci. A zatem zostaniemy zatrzymani i ukarani? Nie koniecznie. Pamiętajmy, że warunkiem ukarania jest fizyczne zatrzymanie autora podejrzanej korespondencji, a to z kolei nie będzie możliwe jeżeli system nie połączy korespondencji z osobą, czyli nie namierzy nadawcy po numerze IP, lub nadawca nie popełni nieostrożności w wyniku której sam udostępni swoje dane.

SIEĆ TOR

Zgodnie z zasadą, w myśl której każda akcja musi zrodzić reakcję, ograniczanie wolności wypowiedzi w Internecie, czyli cenzura prewencyjna oraz zamach na nasze dobra osobiste czyli inwigilacja doprowadziły do powstania metody obrony przed tymi działaniami. Metodą taką jest sieć TOR, która gwarantuje anonimowość uniemożliwiając namierzenia naszego IP. A zatem jeżeli zastosujemy się do podstawowych zasad ostrożności zalecanych przez twórców TOR-a i mamy minimum zdrowego

rozsądku system nie zdoła nas namierzyć, ani zablokować naszej korespondencji.

Tor (ang. The Onion Router) jest wirtualną siecią komputerową implementującą trasowanie cebulowe drugiej generacji, zapobiegającą analizie ruchu sieciowego i w konsekwencji zapewniającą użytkownikom prawie anonimowy dostęp do zasobów Internetu. Roger Dingledine, Nick Mathewson i Paul Syverson przedstawili pracę „Tor: The Second-Generation Onion Router" na 13. sympozjum bezpieczeństwa stowarzyszenia USENIX w piątek, 13 sierpnia 2004 r. Podobnie jak sieci Freenet, GNUnet czy MUTE, Tor może być wykorzystywany w celu ominięcia mechanizmów filtrowania treści, cenzury i innych ograniczeń komunikacyjnych.

Tor wykorzystuje kryptografię, wielowarstwowo szyfrując przesyłane komunikaty (stąd określenie „trasowanie cebulowe"), zapewniając w ten sposób doskonałą poufność przesyłania pomiędzyruterami. Użytkownik musi mieć uruchomiony na swoim komputerze serwer pośredniczący sieci Tor. Oprogramowanie łączące się z Internetem może korzystać z Tora poprzez interfejs SOCKS. Wewnątrz sieci Tor ruch jest przekazywany pomiędzy ruterami, a oprogramowanie okresowo ustanawia wirtualny obwód poprzez sieć Tor, osiągając w końcu wyjściowy węzeł, z którego niezaszyfrowany pakiet jest przekazywany do miejsca jego przeznaczenia. Z punktu widzenia docelowego komputera, ruch wydaje się pochodzić z wyjściowego węzła sieci Tor.

Tor nie oferuje całkowitej anonimowości i przy założeniu dostępu do odpowiednio dużych środków technicznych możliwe jest wytropienie danego użytkownika tej sieci[3]. Tor nie może i nie próbuje chronić przed monitorowaniem ruchu na granicach sieci, tzn. pakietów wchodzących i opuszczających sieć.[4] Na przykład rząd Stanów Zjednoczonych ma możliwość monitorowania dowolnego szerokopasmowego połączenia z Internetem dzięki urządzeniom wprowadzonym na podstawie Communications Assistance for Law Enforcement Act (CALEA) i dlatego może

kontrolować oba punkty końcowe połączeń Tora wykonywanych w obrębie USA. O ile Tor chroni przed analizą ruchu, nie może zapobiec potwierdzeniu komunikacji.

Tor, początkowo sponsorowany przez laboratoria badawcze Marynarki Wojennej Stanów Zjednoczonych, pod koniec 2004 r. stał się projektem firmowanym przez Electronic Frontier Foundation (EFF), która wspierała go finansowo aż do listopada 2005 r. Obecnie rozwojem oprogramowania Tor zajmuje się Tor Project – organizacja non-profit o charakterze badawczo-edukacyjnym, z siedzibą w Stanach Zjednoczonych, otrzymująca wsparcie finansowe z różnych źródeł.

UWAGI TWÓRCÓW TORA

„Chcesz, żeby Tor naprawdę działał?

…to prosimy nie poprzestawaj tylko na instalacji. Musisz zmienić część swoich zwyczajów i przekonfigurować swoje oprogramowanie! Tor sam z siebie NIE jest wszystkim, czego ci trzeba, by zachować anonimowość. Jest kilka poważnych pułapek, na które trzeba uważać:

Tor chroni tylko te aplikacje internetowe, które są skonfigurowane, by swoje dane wysyłać przez Tora – Tor nie anonimizuje magicznie całego ruchu w sieci tylko dlatego, że jest zainstalowany. Polecamy przeglądarkę Firefox z rozszerzeniem Torbutton.

Torbutton blokuje wtyczki przeglądarki takie jak Java, Flash, ActiveX, RealPlayer, Quicktime, wtyczka Adobe PDF, i inne: mogą one zostać zmanipulowane, by zdradzić twój adres IP. Znaczy to na przykład, że Youtube jest zablokowane. Jeśli naprawdę potrzebujesz Youtube, możesz przekonfigurować Torbuttona, by na to zezwolić; ale zdaj sobie sprawę z tego, że otwierasz się na potencjalny atak. Ponadto, rozszerzenia takie jak Google toolbar wyszukują więcej informacji o stronach, które wpisujesz: mogą pomijać Tora lub wysyłać prywatne informacje. Niektórzy ludzie wolą używać dwóch

przeglądarek (jednej dla Tora, drugiej do niebezpiecznego przeglądania sieci).

Strzeż się ciasteczek: jeśli kiedykolwiek zdarzy ci się przeglądać sieć bez Tora, a jakaś strona przyśle ci ciasteczko, to ciasteczko to może identyfikować cię nawet wtedy, gdy ponownie zaczniesz używać Tora. Torbutton stara się bezpiecznie zajmować się ciasteczkami. Rozszerzenie CookieCuller może pomóc w ochronie ciasteczek, których nie chcesz stracić.

Tor anonimizuje źródło przesyłanych informacji i szyfruje wszystko między Tobą i siecią Tora oraz wewnątrz sieci Tora, ale nie może szyfrować danych między siecią Tora a punktem docelowym. Jeśli wysyłasz prywatne informacje, powinieneś wkładać w ich ochronę tyle wysiłku, ile normalnie byś wkładał w normalnym, strasznym Internecie – używaj HTTPS lub innego protokołu uwierzytelniania i szyfrowania na całej drodze nadawca-odbiorca.

Tor, powstrzymując ludzi atakujących twoją sieć lokalną od poznania lub wpływu na punkt docelowy wysyłanych informacji, otwiera nowe ryzyka: złośliwe lub źle skonfigurowane węzły wyjściowe Tora mogą wysłać cię na złą stronę lub nawet wysłać ci aplety Java wyglądające jak pochodzące z zaufanych domen. Bądź ostrożny/a przy otwieraniu dokumentów lub aplikacji pobranych przez Tora, chyba że sprawdziłeś/aś ich integralność.”

BĄDŹ OSTROŻNY

Na koniec kilka uwag dotyczących najczęściej popełnianych nieostrożności, które powodują, że nawet TOR jest bezradny.

1. Wysyłanie wiadomości z konta pocztowego założonego na własne, prawdziwe nazwisko. Jeżeli założymy darmowe konto poczty elektronicznej na jakiś pseudonim, to przy rejestracji będziemy zmuszeni podać dane osobowe które, jeżeli będą prawdziwe, wystarczą aż nadto aby nas namierzyć. W takim

przypadku wysyłanie wiadomości z takiego konta pocztowego jest równoznaczne z podpisaniem się imieniem, nazwiskiem i adresem.

2. Posiadanie założonego na prawdziwe nazwisko konta na portalach społecznościowych typu Nasza Klasa, Facebook i tym podobne.

3. Podawanie na różnego rodzaju stronach Internetowych swoich danych osobowych.

4. Stosowanie TOR-a w sposób niezgodny z jego przeznaczeniem, czyli sprzeczny z zaleceniami autorów.

Opracowanie: Cartafirus
Źródło: New World Order

BIBLIOGRAFIA

1. http://www.ws-webstyle.com/pl/netopedia/bezpieczenstwo_hacking/des_data_encryption_standard

2. http://pl.wikipedia.org/wiki/Advanced_Encryption_Standard

3. http://pl.wikipedia.org/wiki/RSA_(kryptografia)

4. http://blog.konieczny.be/2005/05/25/kryptografia-aes-zlamany/

5. http://www.zgapa.pl/zgapedia/AES.html

6. http://pl.wikipedia.org/wiki/Tor_(sieć_anonimowa)#Ukryte_us.C5.82ugi

7. http://www.torproject.org/index.html.pl

8. http://dyski.cdrinfo.pl/artykuly/truecrypt5/index.php