freeware **HyperCrypt 1.0**

Uživatelská příručka

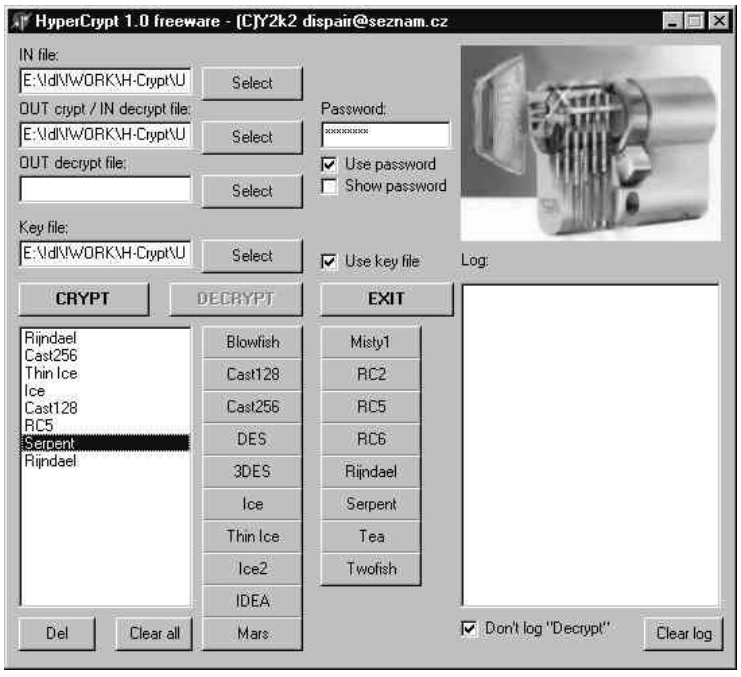
Obsah

Obsah …… 2
Úvod …… 3
Obsluha programu …… 3
Instalace a spuštění …… 3
Šifrování …… 3
Odšifrování …… 4
Konec programu …… 5
Požadavky na běh programu …… 5
Licenční podmínky …… 5
Závěr …… 5

Úvod

Asi většina uživatelů výpočetní techniky se jistě setkala s problémem, jak ochránit data před neoprávněnou manipulací. Neoprávněnou manipulací může být třeba odcizení dat (z média či během přenosu), nechtěná úprava dat, nebo „obyčejné“ špehování. K vašim datům se může dostat nejen osoba, ale i též zlomyslný počítačový program. Aby se předešlo těmto problémům, používá se šifrování. Šifrování ocení snad všechny osoby používající sdílený počítač (škola/práce). Existují různé druhy šifer lišící se zabezpečením, které jsou vhodné k použití nejen proti zvědavým kamarádům-vidlákům, ale i proti tajným agentům a policii (z toho důvodu bylo v USA zakázáno vyvážet silné šifry a známý šifrovací program *PGP* musel být vyvezen ilegálně). Podstatný rozdíl je mezi šiframi symetrickými a asymetrickými. Symetrické šifrování prování zašifrování i odšifrování pomocí jednoho a toho samého klíče nebo hesla, kdežto asymetrické umožňuje zašifrovat data veřejným klíčem a odšifrování je možné provést jen soukromým (tajným) klíčem. Obojí šifrování má své výhody i nevýhody. Program **HyperCrypt** používá šifrování symetrické.
Každá šifra má určitou délku klíče a určitý algoritmus. S vhodnou délkou klíče jsou dobré šifry rozluštitelné bez znalosti klíče za dobu, která mnohařádově překoná délku lidského života a tak jsou dostatečně odolné vůči prolomení při současné technologii. Protože každý algoritmus má své výhody, používá program **HyperCrypt** současně až 18 druhů šifer. Jedná se o ty nejlepší současné symetrické šifry, samozřejmostí je podpora standardu *AES* (šifra *Rindjael*), též jsou použity ostatní šifry, které kandidovaly ve výběrovém řízení na *AES* a další nové i starší šifry (*DES*, *Tripple DES*, *IDEA*, *CAST*…). Pokud se nějaká z šifer zdá někomu málo bezpečná, prostě použije jinou z nabídky, popřípadě více jiných. Program **HyperCrypt** umožňuje libovolné zřetězení šifer za sebou (i opakované), kromě generovaného klíče může pracovat i s heslem, které se neukládá do žádného souboru a kromě šifrování provede i zabezpečení souboru pro detekci změny v datech (hashovací funkce *SHA-1*).
Program je snadno a intuitivně ovladatelný.

Obsluha programu



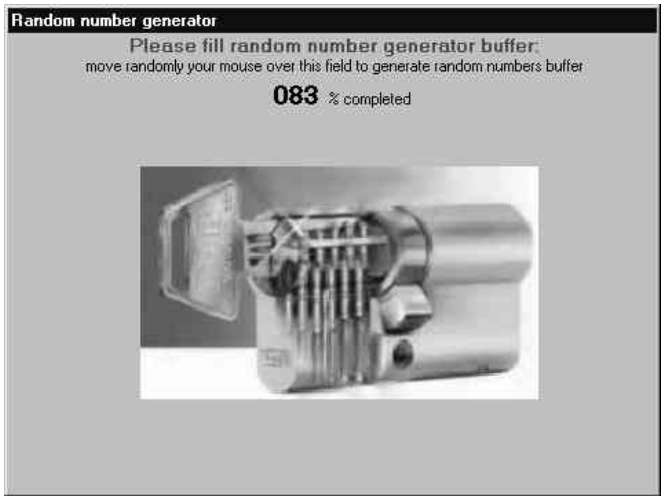
Instalace a spuštění:
Program pracuje ihned po spuštění bez nutnosti instalace a konfigurace *(u některých programů, dokonce i komerčních, bývá problém je vůbec nainstalovat nebo spustit ☺)*.

Šifrování:
Nejprve je nutné zvolit soubor, který chceme zašifrovat. Můžeme jej buď ručně napsat do řádky „IN file“, nebo najít na disku pomocí tlačítka „Select“ vedle řádky s názvem vstupního souboru. Pokud soubor hledáme na disku, jsou automaticky po jeho zvolení vyplněny položky „OUT crypt“ a „Key file“ sloužící ke specifikaci výstupního souboru a souboru pro uložení tajného klíče. Pokud vám tyto nabídnuté názvy nevyhovují, zvolte je ručně jejich vepsáním do příslušných řádek nebo výběrem pomocí tlačítek „Select“.

Program nabízí šifrování ve čtyřech režimech:
1) pomocí vygenerovaného klíče a bez hesla
2) pomocí vygenerovaného klíče + heslo
3) bez klíče jen s heslem
4) bez klíče i hesla

Čtvrtý způsob (začnu odzadu) je vhodný snad jen pro jednorázové použití, aby nebyl například přímo pomocí textového editoru vidět text. Data nejsou chráněna ani klíčem ani heslem a lze je rozluštit kdykoli, pokud útočník zná použitý algoritmus.

Třetí způsob je zabezpečen podle toho, jak vhodné je heslo. Pokud útočník zná algoritmus a heslo je velmi jednoduché (například „aaa“), může též dojít k prolomení šifry. Pokud je heslo zvoleno vhodně, je při současné technologii nemožné rozluštit šifrovaná data a to bez ohledu na zvolenou šifru.
Šifrování bez klíče je vhodné například tam, kde není možné bezpečně doručit uložený klíč od odesílatele k příjemci. Pokud je to možné, doporučuji použít první nebo druhý způsob šifrování – pomocí vygenerovaného klíče uloženého na disk. Druhý způsob zajišťuje ochranu dat i poté, došlo-li k prozrazení tajného klíče útočníkovi (např. jej odcizil z disku), avšak v tom případě se na šifrovaná data vztahuje to samé, co ke třetí metodě práce s programem. Klíč je vygenerován pro každou šifru náhodně v plném rozsahu (považuji za zbytečnost šifrovat kratším klíčem než maximálním možným, ačkoli to algoritmy šifer umožňují, protože při dnešním výkonu počítačů to neznamená prakticky žádné zpomalení, ale jen maximální možnou bezpečnost dat – přecejen už jsou pryč doby 386tek, kdy by rozdíl mezi 40 a 56 bity znamenal ušetření čtvrt hodiny času při šifrování dat ☺). Protože pseudonáhodné generátory používané v programovacích jazycích nejsou pro účely šifrování použitelné, je pro vygenerování klíčů třeba zásah uživatele. Podobně jako u programu *PGP* se náhodná



čísla generují podle pohybu myši po ploše programu. Čím chaotičtěji bude uživatel pohybovat myší, tím lépe. Nicméně náhodná čísla jsou generována podle více kritérií (souřadnice myši, rychlost pohybu myši, aktuální datum a čas s přesností na milisekundy), takže i nesmělé popotahování myšičky v rohu splní svůj účel. Generování klíče probíhá na začátku šifrování a v případě, že dojde buffer s náhodnými čísly, je uživatel požádán o vygenerování nového. Při generování většího množství klíčů může zabrat generování více bufferů poměrně dost času (i několik minut hýbání myšičkou ☺).

Použití klíče se zapíná zaškrtávací položkou „Use key file“ a použití hesla „Use password“. Heslo je třeba zadat do řádku „Password“. Heslo je implicitně skryto za hvězdičkami, ale je možné jej zobrazit zaškrtnutím položky „Show password“.
Před šifrováním je ještě nutné nastavit použité šifry. Implicitně je zadána šifra ***AES*** (*Rindjael*), do seznamu (vlevo dole) je však možné osmnácti tlačítky libovolně přidávat a vsunovat následující šifry:
Blowfish, Cast128, Cast256, DES, Tripple DES, Ice, Thin Ice, Ice2, IDEA, Mars, Misty1, RC2, RC5, RC6, Rindjael, Serpent, Tea a Twofish
Výběr je značný a s použitím více šifer značně vzrůstá již tak spolehlivá bezpečnost. Bez znalosti klíče je totiž kromě klíče (popř. hesla) nutná ještě znalost toho, jaké šifry byly vůbec použity a v jakém pořadí. Tyto informace se však neukládají do šifrovaného souboru, ale do klíče a tak se při pokusu o prolomení šifry „není čeho chytit“. Šifry je možné ze seznamu odebírat jednotlivě (po označení odebírané šifry) tlačítkem „Del“, popřípadě lze provést smazání celého seznamu tlačítkem „Clear all“.
Šifrování uživatel provede tlačítkem „Crypt“, jakmile jsou všechny údaje uživatelem zadány (tlačítko „Crypt“ odšedne), v případě použití klíčů je uživatel požádán o naplnění bufferů náhodných čísel (viz popis šifrování s klíčem).
Průběh šifrování je uživateli vypsán do okénka „Log“, které je možné v případě nepřehledného zaplnění smazat tlačítkem „Clear log“.
Ukázka zašifrovaného souboru se nachází v adresáři s programem včetně klíče. Soubor s klíčem je sice v této ukázce delší, než samotný šifrovaný soubor (zkomprimovaný cca 16Kb), ale jeho délka by zůstala stejná i pro několika Gb dlouhý soubor.

Odšifrování:
Pro odšifrování je třeba zadat vstupní soubor „IN decrypt file“ (pozor: je shodný s „OUT crypt file“), výstupní soubor „OUT decrypt file“, zaškrtnout použití klíčů a hesla a popř. jméno souboru s klíčem „Key file“. Soubor s klíčem a výstupní soubor je doplněn automaticky při zvolení vstupního souboru, ale je možné je změnit ručně.
Pokud není použit klíč, je nutné ještě ručně zadat do seznamu použité šifry ve správném pořadí, které je stejné jako při šifrování.
Pozor: program úmyslně pro vyšší bezpečnost nekontroluje, zda byly použity správné algoritmy, správné heslo a správná metoda dešifrování !!! Při použití klíče je pouze zkontrolována integrita samotného klíče a zašifrovaného souboru (pro případ poškození zašifrovaných dat např. chybou na disku), ale výstupní data nejsou jakkoli kontrolována a uživatel si je musí buď překontrolovat sám (obrázek lze zobrazit, text lze číst…) nebo

musí šifrovat archívy, které jsou samy chráněny před změnami dat. Pokud ale nebyla nahlášena chyba klíče a chyba šifrovaných dat a zároveň bylo použito správné heslo, správná metoda dešifrování a správné algoritmy, je dešifrovaný soubor také v pořádku. Pokud jsou v pořádku klíč i šifrovaný soubor, ale byla zvolena špatná metoda (např. nebylo zadáno heslo) a nebo bylo špatně heslo, výsledný soubor je celý nesmyslný.
Tento způsob zabezpečení velice ztěžuje pokusy o prolomení šifry, protože útočník nemá možnost ověřit, zda jsou data dešifrována správně (kontrolní hash je jen pro šifrovaný soubor a pro klíč a navíc je uložen v klíči a nikoli v šifrovaném souboru). Bez znalosti klíče je tedy nemožné při pokusu o prolomení šifry poznat, zda byl klíč zadán špatně (zkoušení všech klíčů může zabrat i miliardy let při současné technologii pro jeden algoritmus) a nebo zda byla data dešifrována správně, ale následuje další algoritmus ze seznamu (ale který ? ☺).
Při dešifrování je též možno vypisovat aktuální algoritmus, ale implicitně je to zakázáno, aby nemohl potenciální útočník koukající přes rameno (nebo odchytávající obrazovku) poznat, jaká šifra je použita.

Konec programu:
Program se ukončuje tlačítkem „Exit“ nebo standardním zavíracím křížkem.

Požadavky pro běh programu:
Program **HyperCrypt** nemá žádné zvláštní požadavky pro spuštění a používání. Lze jej provozovat na všech 32bit operačních systémech Windows (**Win95, Win98, WinME, WinNT, Win2000, WinXP**). Program nic neukládá do registrů ani kamkoli jinam, lze jej používat ihned po spuštění bez nutnosti instalace a odinstalovat pouhým smazáním. Program pracuje optimální rychlostí, která je srovnatelná s běžnými komprimačními programy, používat jej lze i na starších počítačích (testováno P75MHz). Rychlost klesá v závislosti na počtu použitých algoritmů (pochopitelně ☺).

Licenční podmínky:
Program **HyperCrypt** zle volně šířit a zdarma používat za dodržení licenčních podmínek *ZOA*, ale přes to, že je program zdarma, nebudou odmítnuty žádné případné peněžité ani věcné dary ☺

Závěr
Program plně vyhovuje nedávno schválenému standardu *AES*, ale díky implementování starších prověřených šifer může program použít i ten, kdo nedůvěřuje neprověřeným novinkám.
Program **HyperCrypt** považuji za natolik bezpečný, že jej používám i pro svoje data ☺ :-) I při použití jednoho z bohatého výběru a dobrého utajení klíče a hesla je v současné době nemožné v běžných podmínkách prolomit šifrovaná data. Pokud se dokonce použijí všechny nabízené šifry a to v libovolném pořadí a několikrát, může se cítit bezpečně třeba i galaktický gigaterorista ☺ :-)