Advanced Encryption Package 2005 Professional

Šifrant, k vašim službám – ochraňte své soukromí před zvědavými pohledy (CD)

KAREL ŠREDL

Vítám vás u dalšího dílu Rychlokurzu. A co tu dnes pro vás máme? Osobního profesionálního šifranta jménem Advanced Encryption Package 2005 Professional. Protože název programu je velmi dlouhý (byť možná vznešený), budeme v dalším textu užívat pouze zkratku z prvních písmen – AEP2005. Program umožní udržet obsah vašich souborů v tajnosti a zajistí, aby to, co chcete utajit, utajeno zůstalo.

Instalace

Po spuštění instalačního souboru budete vyzváni k výběru jazyka instalace. Mezi angličtinou, němčinou, japonštinou a ruštinou sice budete marně hledat češtinu, ale nebojte se, k dokončení instalace budete potřebovat jediné slovo *[Next>]*. Klikáním na toto tlačítko projdete všemi kroky až k závěrečnému *[Finish]* – Hotovo.

Spuštění

Jak bývá zvykem, instalátor vytvoří v nabídce *[START] > Programy* adresář „Advanced Encryption Package...". Po spuštění aplikace se ocitnete v hlavním okně, které obsahuje vše důležité. V levé části (shora) se nachází stromová struktura souborů a adresářů, pod ní vstupní filtr, určení výstupního adresáře a okno se záznamy akcí (Logging). V pravé části jsou pak shora tlačítka s dostupnými akcemi, pod nimi volby k aktuálně zvolené akci a nakonec velké tlačítko *[START]*.

KROK 1: OZNAČENÍ SOUBORŮ

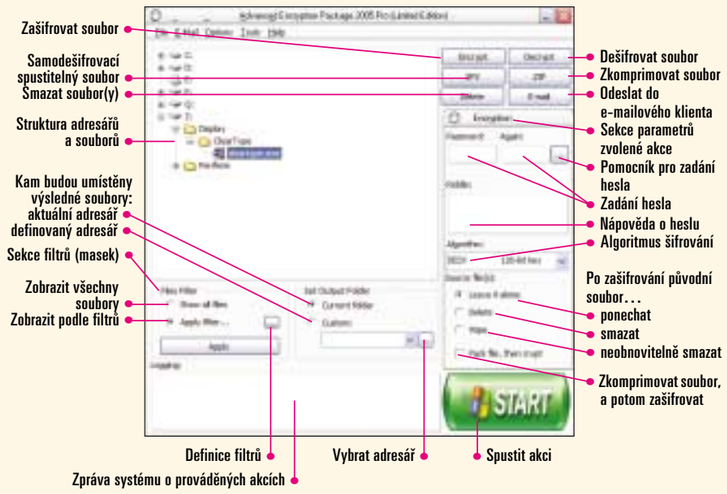
První krok je vždy stejný – musíme označit soubory, s nimiž budeme pracovat. K tomu slouží velké okno v levé části, kde vidíme stromovou strukturu adresářů a souborů. Tam najdeme požadovaný soubor či soubory. Ty pak označíme buď jednotlivě (držte CTRL a kliknutím soubory označte), nebo klikněte na první požadovaný soubor, stiskněte a držte SHIFT a klikněte na soubor poslední. Označí se všechny soubory ležící mezi nimi.

S výběrem souborů souvisí sekce označená *[Files Filter]*. Za normálních okolností je zvýrazněná volba *Show all files*, což znamená, že se ve stromové struktuře zobrazí soubory všech typů. Pokud vás ovšem zajímají pouze wordovské dokumenty, můžete nastavit takzvaný filtr. Klikněte na tlačítko *[...]* vedle volby *Apply filter...* Objeví se dialogové okénko s dvěma vstupními poli. Jedno, označené *Show*, slouží pro definování toho, co zobrazit chceme, druhé *Hide* naopak toho, co chceme skrýt. Pokud naše zadání zní zobrazit pouze soubory s příponou DOC a šablony DOT, zapíšeme do masky v poli *Show* hodnotu **.doc; *.dot*. Klikněte na *[OK]* a poté na tlačítko *[Apply]*. Ve stromové struktuře by nyní měly zůstat pouze soubory odpovídající naší masce (tedy soubory DOC a DOT). Filtry nám takto mohou zjednodušit práci.

KROK 2: AKCE

Máme označené soubory a nyní je potřeba určit, co s nimi. Přesuneme se pohledem na pravou stranu okna a pojedeme pěkně shora dolů. Nejprve kliknutím na tlačítko vybereme akci, poté pod ní vyplníme parametry a nakonec kliknutím na *[START]* akci spustíme. Pojďme se na jednotlivé možnosti podívat podrobněji:

- **ENCRYPT (Zašifruj)** – základní akce, kterou bychom od podobného programu čekali. Vezme daný soubor, zašifruje ho zadaným heslem a uloží s příponou AEP do adresáře určeného v sekci [Set Output Folder]. Parametry akce jsou:
  - **Password, Again** – do těchto polí zapište heslo, s nímž budete chtít soubor zašifrovat.
  - **Riddle** – velice zajímavé políčko. Zde lze zapsat text, který by vám měl připomenout, jaké heslo jste použili (pro případ, že ho zapomenete, nebo používáte hesel více). K této nápovědě se dostanete i bez znalosti hesla, stačí kliknout na zašifrovaný soubor pravým tlačítkem a zvolit *Get Riddle*. Má tedy sloužit jen jako „nařknutí", rozhodně tam nepište „Heslo je 3. měsíc v roce".
  - **Algorithm** – volba šifrovacího algoritmu.
  - **Source file(s)** – zde stanovíte, co se má provést se zdrojovými soubory po zašifrování. Možnosti jsou *Leave it alone* (nechat je být), *Delete* (smazat) nebo *Wipe* (neobnovitelně smazat).
  - **Pack File, then Crypt** – říká, že soubor bude nejprve zkomprimován a teprve potom zašifrován. Obecně to znamená, že výsledný soubor bude menší než zdrojový (při pouhém zašifrování se naopak soubor zvětší).
- **SFX (Spustitelný archiv)** – tato akce je velmi podobná akci ENCRYPT (vlastně je s ní téměř identická). Výsledkem však není soubor s příponou AEP, ale spustitelný soubor EXE. Tuto možnost využijete, pokud budete předávat zašifrované soubory někomu, kdo program AEP2005 nemá. Parametry jsou identické s akcí ENCRYPT, jen přibylo jedno políčko:
  - **SFX Comment** – neboli text, který se objeví po spuštění souboru s archivem. Měl by obsahovat stručný popis toho, co se v archivu nachází.
- **DECRYPT (Dešifruj)** – opačná akce k zašifrování. Na základě hesla získáte ze zašifrovaného souboru opět soubor původní. Parametry jsou jen dva:
  - **Password** – sem zapište heslo.
  - **Source file(s)** – zde určíte, co se má provést se zašifrovaným souborem po dešifrování. Buď *Leave it alone* (nechat ho být), nebo *Delete* (smazat).
- **ZIP (Komprimuj)** – tato funkce vám nabídne možnost klasického komprimování a dekomprimování souborů metodou ZIP.
  - **Add to ZIP** – komprimuje označené soubory do souboru ZIP (po stisku *[START]* budete vyzváni k zadání jména).
  - **Unzip** – dekomprimuje označený soubor do adresáře nastaveného v sekci *[Set Output Folder]*.



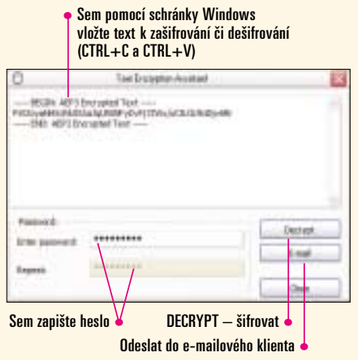
- **What to do with source files** – opět určíte, co dělat po dokončení akce se zdrojovými soubory (*Leave it alone*, *Delete* a *Wipe*).
- **DELETE (Smaž)** – tato funkce slouží ke smazání souborů. Jestliže si říkáte, že k tomu stačí tlačítko *[Delete]* v Průzkumníku, tak ano – stačí. Avšak každý druhý freeware na internetu umí takto smazané soubory obnovit. Proto existují postupy, jak soubor smazat tak, aby obnovitelný nebyl (tzv. *Wipe* – čti vajp). Program AEP2005 nabízí oba způsoby:
  - **Delete** – klasické obnovitelné smazání (rychlý způsob).
  - **Wipe** – bezpečné neobnovitelné smazání (pomalý způsob).
- **E-MAIL** – odešle označené soubory do klienta elektronické pošty.

Tímto jsme probrali základní služby, které nám program AEP poskytuje. Všechny jsou také dostupné z kontextové nabídky po kliknutí pravým tlačítkem myši např. v Průzkumníku Windows. Zbývá však ještě několik doplňkových služeb – což ovšem neznamená, že nejsou zajímavé. Jsou to takové ty pověstné třešničky na dortu.

Šifrování textu

Poměrně zajímavou možností je šifrování prostého textu. Pokud chcete např. odeslat e-mail nebo ICQ tak, aby nikdo nemohl zprávu jen tak přečíst (jen adresát, který má náš program AEP2005 a zná heslo), pak postupujte následovně. Napište zprávu do e-mailového klienta nebo do okna ICQ. Označte jí a stiskem *CTRL+X* text přesuňte do schránky Windows. Nyní spusťte AEP2005 a v menu zvolte *E-mail > Text Encryption Tool*. Do hlavního vstupního pole vložte text stisknutím *CTRL+V* a do sekce *[Password]* zapište 2× heslo. Stiskněte *[ENCRYPT]* a uvidíte, že zadaný text se změnil na změť nečitelných znaků uvozených hlavičkou ----- *BEGIN: AEP3 Encrypted Text* -----. Nyní celý text označte (*CTRL+A*) a vložte opět do schránky (*CTRL+C*). V e-mailovém klientovi (nebo v ICQ) pak zašifrovaný text jednoduše vložíte stiskem *CTRL+V* a odešlete.

Adresát na druhé straně podle hlavičky pozná, že se jedná o text zašifrovaný právě naším programem, spustí AEP a přejde do *E-mail > Text Encryption Tool*. Přes schránku (*CTRL+C* a *CTRL+V*) překopíruje šifrovaný text do políčka pro text, stiskne *[DECRYPT]* a text je opět čitelný.



Generátor hesel

Máte problém rychle vymyslet bezpečné heslo? Spusťte generátor hesel z menu *Tools > Password generator*. V dialogovém okně nastavte znaky, které mé heslo obsahovat a jeho délku. Pak stiskněte tlačítko *[Generate]* a v poli *Password:* se vám jedno takové objeví.

Čistka počítače

Dalším užitečným nástrojem je funkce pro vyčištění informací, které po vás zůstanou při používání např. Internet Exploreru. Seznam navštívených adres, stažené soubory, to vše může prozradit něco z vašeho soukromí. Proto je potřeba vše smazat. Jak na to? V menu zvolte *Tools > Clear Computer History* a v dialogu zaškrtejte informace, které chcete pročistit. Nakonec stiskněte tlačítko *[Clear]*, a je to.

Nastavení

Ačkoli je to nezvyklé, nastavení programu jsem nechal až nakonec. Vlastně není potřeba nic nastavovat – a pokud přece, pak se pojďme rychle podívat na ty nejzajímavější volby:

Options > Change Skin – volba pro změnu vzhledu. Vyberete ze seznamu soubor s definicí vzhledu a stiskněte *[Otevřít]*. Budete upozorněni, že se změna stylu projeví až při příštím spuštění a program bude ukončen. Příště už bude AEP vypadat jinak.

Hlavní nastavovací volby jsou dostupné přes menu *Options > Options*, my si zde popíšeme jen ty nejzajímavější:

- **FILES**
  - **Show system and hidden files** – v seznamu souborů budou zobrazovány i ty označené jako skryté či systémové.
  - **Save used passwords to a file** – uloží seznam hesel použitých při šifrování do jednoho zašifrovaného souboru. Takto nezapomenete, jaké heslo jste kde použili. Do pole *File* zapište jméno souboru (nebo ho kliknutím na tlačítko *[...]* vyhledejte), pod něj do pole *Password* zapište heslo, jímž bude soubor zašifrován. Do pole *Again* zadejte totéž heslo pro kontrolu ještě jednou.
- **INTERFACE**
  - **Ask password to start AEP** – při každém spuštění aplikace budete dotázáni na heslo (pole *Password* a *Again*).
- **SECURE DELETION** – v této sekci jsou volby pro nastavení bezpečného mazání souborů. Doporučuji nic neměnit!
- **LANGUAGE** – volba jazyka.
- **SOUND**
  - **Play sound after long operation** – po dokončení dlouhotrvajících operací přehraje zvuk. Vy můžete nastavit, o jaký zvuk se bude jednat (soubor WAV) a co považujete za dlouhotrvající operaci (implicitně 10 s).

Závěr

Šifrování a bezpečnost dat jsou v dnešní společnosti velmi důležité. Advanced Encryption Package 2005 Professional umožňuje vybudovat si na vlastním počítači jistou úroveň zabezpečení a soukromí. Pokud potřebujete hlavně šifrovat jednotlivé soubory či text, pak je AEP ta správná volba. Navíc obsahuje jako bonus několik dalších šikovných nástrojů. 5 0152/OK ❑