Ochraňte svá data

Máte na disku citlivá data, která chcete ochránit před zvídavými podřízenými, kolegy, nebo dokonce před konkurencí? Pak máte jedinou možnost a tou je tato data zašifrovat. Na pomoc si můžete vzít šikovný bezplatný nástroj TrueCrypt.

Program najdete na PPK CD 15/10

TRUECRYPT

výrobce: TrueCrypt Foundation
cena: zdarma
jazyk: angličtina
rubrika na CD: Obsah CD / Šifrování souborů
více info: www.truecrypt.org

V ČLÁNKU SE DOZVÍTE:

- jak program nainstalovat
- jak se v programu orientovat
- jak vytvořit virtuální šifrovaný disk
- disk připojit a odpojit

stupeň obtížnosti: obtížnější

INSTALACE PROGRAMU

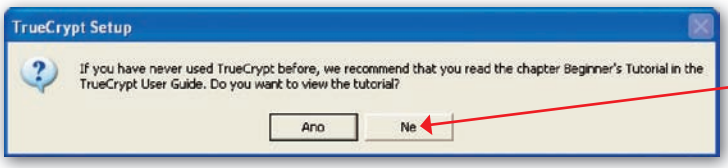
Program TrueCrypt získáte na internetových stránkách *www.truecrypt.org/downloads* nebo na CD přiloženém k tomuto vydání PPK (rubrika **Obsah CD / Šifrování souborů**). Pro úplnost dodejme, že program je k dispozici zcela zdarma, a to třeba i pro použití na firemních počítačích.

Dvojitým kliknutím na získaný balíček spusťte průvodce instalací. V prvním okně se zobrazí licenční ujednání. Potvrďte jej nejprve kliknutím na zaškrtávací políčko **I accept...** a poté kliknutím na tlačítko **Accept**. V dalším okně máte na výběr mezi běžnou instalací (**Install**) a pouhým zkopírováním programu na zvolené místo (**Extract**). Druhá volba je určena pro vytvoření přenosné (tzv. portable) verze programu na flash disku či jiném přenosném disku. Zvolte první variantu, tedy možnost **Install**.

Následuje okno s možností výběru instalační složky a s dalšími nastaveními. Zde není potřeba nic měnit, a tak jen kliknutím na tlačítko **Install** zahajte samu instalaci. O jejím úspěšném dokončení pak informuje hlášení **TrueCrypt has been successfully installed**. Po jeho potvrzení se objeví dotaz **If you have never used TrueCrypt...**, tedy zda chcete spustit průvodce pro nové uživatele. Patrně byste rádi odpověděli **ano**, ale jelikož je průvodce – na rozdíl od tohoto návodu – celý v anglickém jazyce, klikněte na tlačítko **Ne** (obr. 1).

INFO

ŠIFROVÁNÍ • Nevíte, co je to vlastně šifrování, k čemu je dobré, jak funguje a jak je spolehlivé? Přečtěte si článek „Chráníme data i soukromí“ na stranách 42 a 43 tohoto vydání PPK.



OBR. 1 Chcete spustit průvodce?

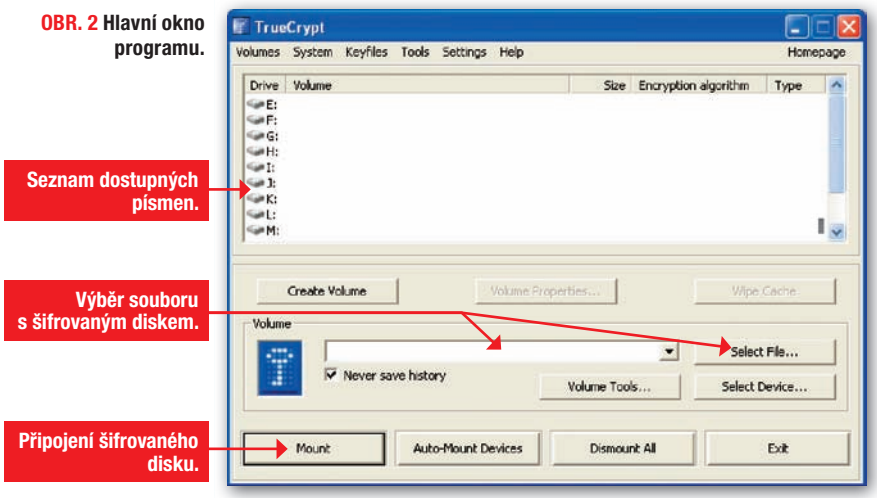
ORIENTACE V PROGRAMU

Spusťte program TrueCrypt pomocí zástupce na pracovní ploše nebo v nabídce Start. Po zobrazení hlavního okna programu můžete být lehce zmateni – ovládání programu není úplně intuitivní.

Největší část okna zabírá výpis písmen jednotek, která jsou programu TrueCrypt k dispozici (jde o výpis těch písmen, která nejsou obsazena žádným diskem, flash diskem, mechanikou, čtečkou paměťových karet atd.). Následuje trojice tlačítek, z nichž nejdůležitější a také aktuálně jediné přístupné je **Create Volume** (vytvořit šifrovanou jednotku).

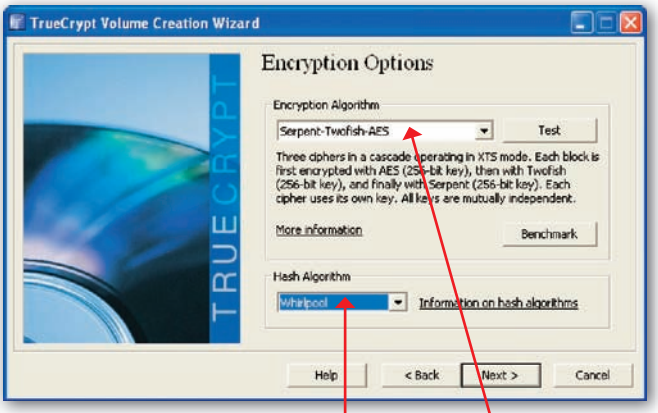
Následuje část **Volume**, sloužící k připojení existující šifrované jednotky. Zde je nejdůležitějším tlačítkem **Select file** – slouží k výběru souboru se šifrovanou jednotkou. Zcela dole naleznete sadu čtyř tlačítek, z nichž brzy použijete to první, tedy tlačítko **Mount**, sloužící k připojení šifrované jednotky do systému (obr. 2). Ostatní tlačítka mají také svůj význam, ale v dnešním návodu se seznámíte s nejjednodušším postupem pro vytvoření šifrovaného disku. Nicméně to jsme trochu předběhli...

OBR. 2 Hlavní okno programu.



VYTVOŘENÍ VIRTUÁLNÍHO ŠIFROVANÉHO DISKU

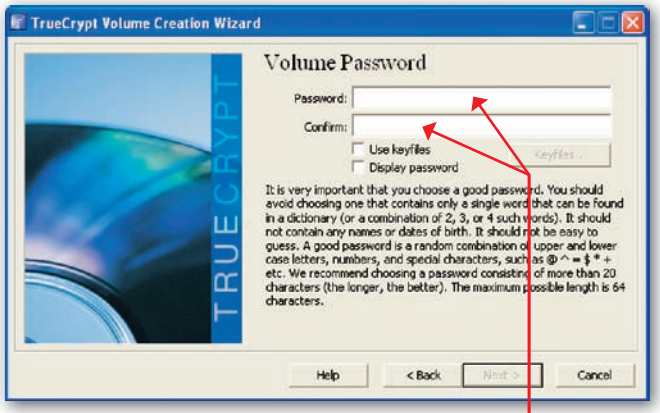
Klikněte na tlačítko **Create Volume**, a spustí se poměrně složitý průvodce. V prvním okně máte na výběr, zda chcete vytvořit virtuální šifrovaný disk ve formě souboru na disku (**Create an encrypted file container**), nebo zda



OBR. 3 Parametry šifrování.

Hashovací funkce.

Šifrovací algoritmus.



OBR. 4 Zadání hesla pro přístup k šifrovanému disku.

Heslo by mělo mít nejméně 20 znaků.

chcete zašifrovat celý současný disk (ať již systémový, či jen datový). Nyní zvolte první možnost, dalším se budeme věnovat v některém z příštích vydání PPK. Pokračujte kliknutím na tlačítko **Next**.

V druhém okně si vyberte mezi vytvořením standardní jednotky a jednotky skryté. Významem skryté jednotky se dnes taktéž nebudeme zabývat, zvolte tedy možnost **Standard TrueCrypt Volume**. V následujícím okně určete umístění souboru se šifrovaným diskem (**Select file**). Tento soubor můžete umístit vskutku kamkoliv, pouze je potřeba, aby na vybraném disku byl dostatek volného místa (podle toho, kolik dat chcete zašifrovat). Jakmile jste s umístěním spokojeni, zadejte ještě název souboru. Ten může být jakýkoliv, a dokonce pro zvýšení bezpečnosti může mít i jakoukoliv koncovku. Zkušenější uživatelé tak můžou šifrovaný disk zamaskovat jako jiný soubor. Nechcete-li mít problémy s jeho pozdějším nalezením, doporučujeme zvolit standardní koncovku souboru ***.tc** (zkratka od TrueCrypt).

Dále (**Next**) se dostanete k výběru parametrů šifrování. Zde je třeba určit především způsob šifrování (**Encryption Algorithm**), tedy šifrovací funkci, odborně řečeno šifrovací algoritmus. Hashovací funkci (**Hash Algorithm**) lze vždy ponechat standardní – bez hlubokého kryptografického vzdělání jen těžko pochopíte rozdíl. Na obrázku 3 je zvolena možnost **Serpent-Twofish-AES**, což lze laicky vysvětlit jako trojnásobné zašifrování. Každý soubor je nejprve zašifrován funkcí AES, poté funkcí Twofish a nakonec ještě funkcí Serpent.

Co se způsobu šifrování týče, vždy musíte zvolit, zda u daného šifrovaného disku preferujete rychlost, anebo bezpečí. Jinými slovy, čím silnější ochranu zvolíte, tím pomalejší bude práce s výsledným diskem. (V případě malého virtuálního disku to může být zanebatelné, ale při šifrování celé systémové jednotky může být start a provoz systému prodloužen na několikanásobek!) O tom, jak rychlá je která volba, se můžete přesvědčit po kliknutí na tlačítko **Benchmark** (v nově otevřeném okně spustíte stejnojmenným tlačítkem test rychlosti).

V dalším (**Next**) okně určujete velikost šifrovaného disku. O maximální možné velikosti (o zbývajícím volném místě na zvoleném fyzickém disku) informuje věta **Free space on disc...is...**. Zadejte tedy velikost budoucího šifrovaného disku a nezapomeňte zvolit správné jednotky, tedy buď **MB** (megabajty), nebo **GB** (gigabajty) – pro připomenutí: 1 GB je 1 000 MB.

Následuje zadání hesla pro přístup k šifrovanému disku (obr. 4). Heslo by mělo být nejméně dvacetimístné, jinak vás program upozorní, zda opravdu chcete použít „krátké“ heslo. V následujícím kroku (**Next**) již naformátujte svůj nový šifrovaný disk kliknutím na tlačítko **Format**. V posledním (**Next**) okně s nadpisem **Volume Created** ukončete průvodce kliknutím na tlačítko **Exit**.

INFO

TIPY PRO TVORBU HESLA

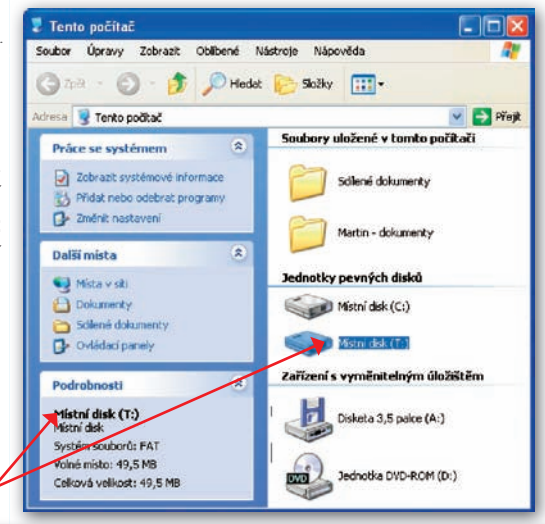
• Heslo by nemělo být uhodnutelné (12345, vaše jméno, jméno vašeho psa, datum narození potomka, běžná slova jako „ahoj“ aj.) a mělo by obsahovat malá i velká písmena, číslice i speciální znaky, jako je třeba pomlčka nebo tečka. Tím zajistíte, že nebude prolomitelné, neboť vyzkoušení všech možných kombinací přesahuje možnosti i toho nejvýkonnějšího počítače. (Mimochodem: U dvacetimístného hesla je počet variant s použitím výše zmíněných rad až neuvěřitelný – toto číslo má řádově 38 nul. Vyzkoušení byť i jen poloviny přípustných kombinací by pak ani vysoce výkonný vědecký počítač nezvládl rychleji než za desítky tisíc let…)

PŘIPOJENÍ A ODPOJENÍ DISKU

Šifrovaný disk je před jeho použitím třeba připojit do systému. V hlavním okně programu TrueCrypt (viz obr. 2) klikněte na písmeno, které chcete disku přiřadit, klikněte na tlačítko **Select File** a vyberte soubor, který jste nedávno vytvořili. Nakonec klikněte na tlačítko **Mount** a zadejte heslo pro přístup k šifrovanému disku.

Po úspěšném připojení se šifrovaný disk objeví jako další disk systému. Můžete s ním běžně pracovat, nahrávat na na něj / z něj soubory, mazat je a upravovat (obr. 5). Po ukončení práce klikněte znovu na tlačítko **Mount**, to je však nyní opatřeno popiskem **Dismount** (Odpojit). Tím dojde k odpojení zvolené jednotky a k vašim datům se nikdo nedostane.

Martin Taneček,
martin@tanecek.eu



OBR. 5 Přístup k šifrovanému disku.

Váš šifrovaný disk.