Kapitola: Zobrazení dat v počítači

Cvičení 11 – Šifrování a elektronický podpis

Témata: zabezpečení informací proti neoprávněnému čtení, bezpečná komunikace elektronickými médii, prokazování identity odesílatele, bezpečnostní rizika, kryptologie.

Co máme znát

Textový souborový formát, pojem konverze, odesílání a přijímání e-mailu, práce s přílohami k e-mailu, ovládání libovolného textového editoru.

Seznam pojmů

Kryptologie, symetrická a asymetrická šifra, veřejný a soukromý klíč, elektronický podpis, otevřený text, šifrový text, certifikační autorita.

Ověřte, že rozumíte vstupním pojmům a vztahům odpověďmi na tyto otázky:

- Co je to textový formát souboru?
- Co znamená konverze souborového formátu?
- Lze pomocí archivačních nástrojů (ZIP) zabezpečit soubory proti neoprávněnému čtení a modifikaci?
- Jakým způsobem lze zamezit neoprávněné osobě ve čtení elektronické pošty?
- Je běžná elektronická pošta zasílána šifrovaně?
- Jaké typy šifrovacích metod můžeme používat?
- Jaké jsou výhody a nevýhody jednotlivých metod?
- Co ovlivňuje bezpečnost zašifrované zprávy?
- Proč se používá šifrování s veřejným a soukromým klíčem?
- Kde získám veřejný klíč osoby, se kterou chci komunikovat šifrovaně?
- Co je a jaké funkce má certifikační autorita?

Materiál

Programy: Program MS Word (verze 2003), program WinPT, editor PSPad, program KGpg, příkaz more.

Úkoly

1. MS WORD
   (a) Spusťte si program MS Word a prostudujte si v nabídce Nástroje v položce Možnosti kartu Zabezpečení.
   (b) Jakým způsobem lze zabezpečit dokument pořízený v MS Word?
   (c) Jaké šifrovací algoritmy lze v MS Wordu použít?
   (d) Napište ve Wordu krátkou zprávu a zašifrujte ji pomocí hesla, na kterém se domluvíte s kolegou ve dvojici.
   (e) Zašlete e-mailem kolegovi zašifrovaný dokument.
   (f) Dešifrujte domluveným heslem přijatý dokument.
2. GENEROVÁNÍ KLÍČŮ

(a) Spusťte si program WinPT (v Linuxu KGpg) a vygenerujte si pár klíčů – soukromý a veřejný. Prozkoumejte jaké možnosti lze nastavit pro generování klíčů.

3. VÝMĚNA VEŘEJNÝCH KLÍČŮ

   (a) Exportujte svůj veřejný klíč do souboru a zašlete kolegovi ve dvojici e-mailem jako přílohu.
   (b) Získejte z e-mailové přílohy kolegův klíč a naimportujte jej.
   (c) Po importu se podívejte, jaké vlastnosti importovaný klíč má a nastavte jeho důvěryhodnost.

4. ASYMETRICKÉ ŠIFROVÁNÍ

   (a) Vytvořte si jednoduchý textový soubor se zprávou pro kolegu ve dvojici.
   (b) Zašifrujte soubor kolegovým veřejným klíčem.
   (c) Odešlete zašifrovaný soubor e-mailem kolegovi.
   (d) Získejte zašifrovaný soubor od kolegy stejnou cestou.
   (e) Soubor dešifrujte s pomocí vlastního soukromého klíče.

5. PODPIS + ŠIFROVÁNÍ

   (a) Vytvořte si soubor ve Wordu se zprávou pro kolegu ve dvojici.
   (b) Podepište soubor svým soukromým klíčem.
   (c) Zašifrujte podepsaný soubor kolegovým veřejným klíčem.
   (d) Odešlete zašifrovaný soubor s podpisem e-mailem kolegovi.
   (e) Získejte zašifrovaný soubor od kolegy stejnou cestou.
   (f) Soubor dešifrujte s pomocí vlastního soukromého klíče.
   (g) Ověřte zda soubor pochází skutečně od vašeho kolegy.

6. SYMETRICKÉ ŠIFROVÁNÍ

   (a) Vymyslete si vlastní symetrický klíč (heslo) pro šifrování zpráv a napište ho na kus papíru.
   (b) Vytvořte si jednoduchý textový soubor se zprávou pro kolegu ve dvojici.
   (c) Zašifrujte soubor vymyšleným heslem, odešlete jej e-mailem a klíč sdělte kolegovi.
   (d) Pomocí kolegova hesla dešifrujte přijatou zprávu.

Související odkazy

- http://www.gnupg.org
- http://www.simonsingh.net
- http://www.crypto-world.info