SOŠ agropotravinárska a technická,
Kušnierska brána 349/2, Kežmarok

PROGRAMOVÉ VYBAVENIE POČÍTAČOV

Ochrana informácií v počítačových sieťach, kódovanie

3. ročník

Šifrovanie komunikácie, princíp šifrovania

(Učebný text)

Ing. Peter Barančo

2023

NÁRODNÝ PROJEKT
„Zlepšenie stredného odborného školstva v Prešovskom samosprávnom kraji“

EURÓPSKA ÚNIA
Európsky sociálny fond
Európsky fond regionálneho rozvoja

MINISTERSTVO ŠKOLSTVA, VEDY, VÝSKUMU A ŠPORTU SLOVENSKEJ REPUBLIKY

OPERAČNÝ PROGRAM ĽUDSKÉ ZDROJE

PREŠOVSKÝ SAMOSPRÁVNY KRAJ

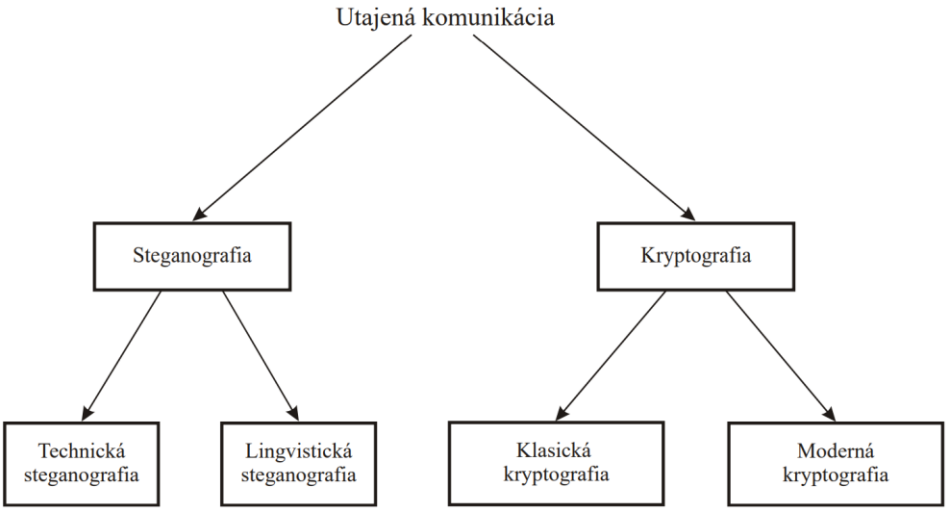
„Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu a Európskeho fondu regionálneho rozvoja v rámci operačného programu Ľudské zdroje“

OBSAH

1 ŠIFROVANIE KOMUNIKÁCIE

Z dôvodu, že správu možno zachytiť práve počas jej prenosu, sa vyvinuli metódy utajenej komunikácie (invisible communication), ktoré možno rozdeliť do dvoch skupín (obr. 1.1):

- steganografia (steganography),
- kryptografia (cryptography).



Obr. 1.1 Metódy utajenej komunikácie

Stenografia - technika ukrytia správy v správe, resp. ukrytie tajnej informácie v správe:

- technická stenografia - neviditeľné atramenty, ukrytie prenosového média, resp. extrémne zmenšenie jeho rozmerov,
- lingvistická stenografia - využíva na ukrytie tajnej správy text, resp. inú grafickú podobu (napr. notový zápis).

Kryptografia - jej cieľom je utajiť obsah správy metódami šifrovania.

- klasická kryptografia - využívala klasické šifry a postupy, ktoré zahŕňajú:
  - substitúciu - nahrádza každý symbol nezašifrovanej správy iným symbolom,
  - transpozíciu - pre usporiadanie symbolov v nezašifrovanej správe, zvoleným spôsobom.
- moderná kryptografia - spojená s rozvojom elektronickej formy komunikácie, z hľadiska realizácie šifrovania a použitých kľúčov ju možno rozdeliť na:
  - kryptografiu s tajným kľúčom (secret key cryptography),
  - kryptografiu s verejným kľúčom (public key cryptography).

Šifrovanie (Enciphering, Encryption) je proces úpravy správy pred jej odoslaním s cieľom utajiť jej obsah. Zo zašifrovanej správy aj po jej zachytení nepovolanou osobou by sa nemal získať obsah vyslanej, resp. nezašifrovanej správy.

Keďže v súčasnosti často využívame internet na najrôznejšie činnosti, musíme počítať aj s bezpečnostnými rizikami, nakoľko väčšina trestných činov v dnešnej dobe je alebo môže byť páchaná za pomoci počítačových a informačných technológií. Na elimináciu týchto rizík sa využíva šifrovanie.

Internet využívame na rôzne činnosti:

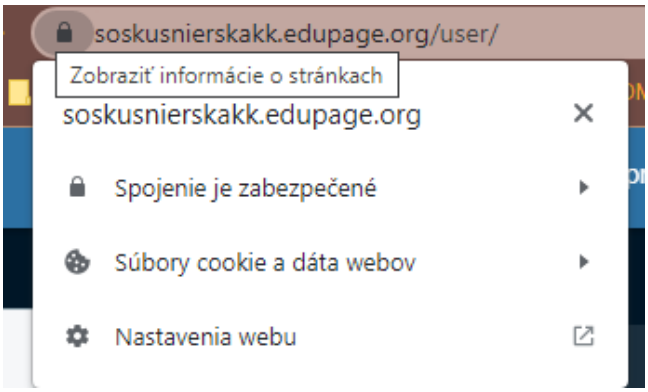
- On-line nakupovanie
- E-mailovanie
- Odosielanie dát

Väčšina stránok požaduje od užívateľov poskytnutie ich citlivých dát, ako sú kreditné karty alebo osobné informácie pri registrácii. Je dôležité, aby odosielané dáta neboli zneužité treťou stranou (neoprávnenou osobou) a bola zaručená integrita správy. Je nevyhnutné, aby prenášané dáta z bodu A do bodu B boli šifrované a bol zabránený prístup k ich modifikácii.

ZAPAMÄTAJTE SI!

Základom každej komunikácie prostredníctvom internetu by malo byť použitie šifrovanej komunikácie.

Šifrovanú komunikáciu na internete spoznáme podľa ikony zámku pred internetovou adresou (obr. 1.2). Hovoríme o tzv. SSL certifikáte, ktorý garantuje kvalitu šifrovacieho kľúča.



Obr. 1.2 Ukážka zámku

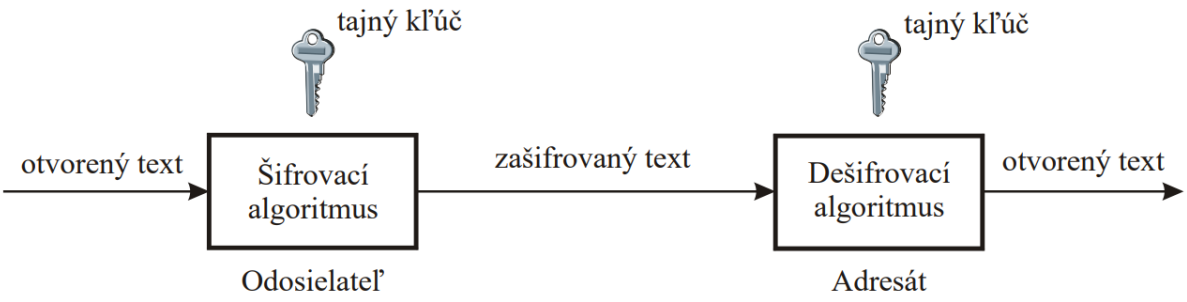
ZAPAMÄTAJTE SI!

Ak stránka nemá „zámok“, v žiadnom prípade nezadávajte na stránke vaše osobné údaje ani cez ňu neplaťte platobnou kartou. Nemáte tu totiž istotu, že sú vaše dáta zabezpečené.

2 PRINCÍP ŠIFROVANIA

Šifrovanie si kladie za cieľ transformovať vstupné dáta podoby, v ktorej sú pre potenciálneho útočníka nezrozumiteľné a nie je schopný rekonštruovať ich pôvodný tvar – zároveň však môžu oprávnene subjekty (používatelia) pôvodné dáta rekonštruovať.

Princíp konvenčného šifrovania je znázornený na obr. 2.1.



Obr. 2.1 Model konvenčného šifrovania

Symetrické šifrovanie zahrňuje päť zložiek. Sú to:

- otvorený text,
- šifrovací algoritmus,
- tajný kľúč,
- zašifrovaný text,
- dešifrovací algoritmus.

Otvorený text je správa, resp. dáta, ktoré predstavujú vstup kryptografického systému, resp. sú to vstupné dáta pre šifrovací algoritmus.

Šifrovací algoritmus je algoritmus, ktorý realizuje šifrovanie, t. j. transformáciu otvoreného textu na zašifrovaný text s využitím kryptografických techník, napr. substitúcie a permutácie.

Tajný kľúč je tiež vstupom kryptografického systému, a nezávisí od otvoreného textu. Tajný kľúč určuje konkrétny tvar transformácie otvoreného textu na zašifrovaný text.

Zašifrovaný text predstavuje výstup šifrovacieho algoritmu. Je jednoznačne určený otvoreným textom a tajným kľúčom. Pre daný otvorený text dva rôzne tajné kľúče produkujú dva rôzne zašifrované texty.

Dešifrovací algoritmus realizuje proces získania otvoreného textu z prijatého zašifrovaného textu s využitím rovnakého tajného kľúča, ktorý bol použitý pri šifrovaní.

2.1 Základné techniky šifrovania informácií

2.1.1 Symetrické šifrovanie

Šifrovací algoritmus využívajúci jeden a ten istý kľúč na šifrovanie a dešifrovanie (obr. 2.2).

V texte správy sa použije tajný kľúč, aby sa obsah zmenil určitým spôsobom.

Útočník bez kľúča nie je schopný zo zašifrovaných údajov získať ich pôvodnú podobu napriek tomu, že pozná šifrovací algoritmus.

Výhody:

- bezpečnosť,
- rýchlosť,
- štandardy, rozsiahle výskumné zázemie.

Nevýhody:

- distribúcia kľúča,
- nie je možné zabezpečiť nepopierateľnosť.

Obr. 2.2 Princíp symetrického šifrovania

Najznámejším a najpoužívanejším symetrickým šifrovacím algoritmom je v AES (Advanced Encryption Standard):

- AES-128,
- AES-192,
- AES-256.

Názov AES-n označuje variant s dĺžkou kľúča n bitov. Dĺžka kľúča je dôležitým parametrom pre bezpečnosť šifrovacieho algoritmu – ovplyvňuje počet potenciálnych kľúčov, ktoré musí útočník vyskúšať v prípade, že sa rozhodne prezrieť priestor všetkých kľúčov.

Kľúče s dĺžkou 128 bitov (teda 2128 potenciálnych kľúčov) možno považovať za dostatočne bezpečné (ak nie sú slabiny v samotnom šifrovacom algoritme alebo v spôsobe generovania).

ZAPAMÄTAJTE SI!

2^{128} = 340 triliónov potenciálnych kľúčov

2.1.2 Asymetrické šifrovanie

Asymetrické šifrovanie používa pri výmene informácií dva kľúče, verejný kľúč a súkromný kľúč (obr. 2.3). Verejný je k dispozícii každému, kto sa snaží odoslať nejakú správu. Druhý, súkromný kľúč, je uchovaný v tajnosti. Každá správa (text, binárne súbory alebo dokumenty), ktorá je zašifrovaná

pomocou verejného kľúča, sa môže dešifrovať iba s použitím rovnakého algoritmu, ale zároveň s použitím zodpovedajúceho súkromného kľúča.

ZAPAMÄTAJTE SI!

Dešifrovací kľúč nie je možné efektívne vypočítať zo šifrovacieho kľúča.

Výhody:

- najvyššia bezpečnosť,
- spĺňa podmienky integrity a nepopierateľnosti,
- štandardy, rozsiahle výskumné zázemie,
- vznikajúce legislatívne zázemie (elektronický podpis) využívajúce tento algoritmus.

Nevýhody:

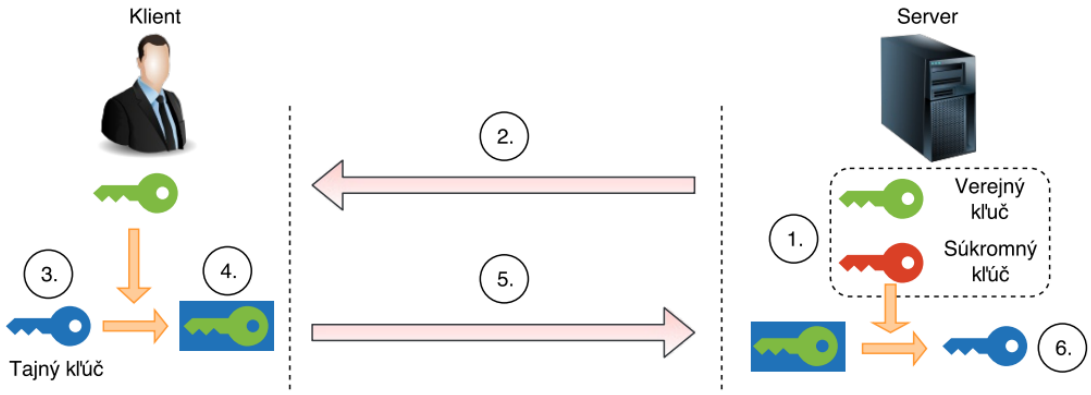
- relatívna zložitosť pochopenia a používania,
- pomalosť.

Obr. 2.3 Princíp asymetrického šifrovania

2.1.3 Hybridné šifrovanie

Hybridný kryptosystém je optimálny spôsob, ako zlepšiť výkonnosť a efektivitu výmeny informácií. Je to kombinácia symetrického a asymetrického šifrovania. V podstate ide o to, že pre veľmi dlhé správy je väčšina práce v šifrovaní a dešifrovaní vykonaná efektívnejšou schémou symetrických kľúčov, zatiaľ čo neefektívna schéma asymetrického šifrovania sa používa iba na šifrovanie a

dešifrovanie krátkej kľúčovej hodnoty. Všetky praktické implementácie kryptografie s asymetrickým šifrovaním používajú dnes hybridný kryptosystém. Na obr. 2.4 je znázornená architektúra hybridnej komunikácie.



Obr. 2.4 Efektívna ochrana pomocou hybridného kryptosystému

POSTUP

1) Server na začiatku komunikácie vytvorí verejný a súkromný kľúč.
2) Vytvorený verejný kľúč je zdieľaný s užívateľom. Súkromný kľúč si server ponecháva v utajení.
3) Užívateľ si vygeneruje svoj vlastný tajný kľúč.
4) Pomocou verejného kľúča zašifruje svoj tajný.
5) Zašifrovaný tajný kľúč následne odošle na server.
6) Server pomocou súkromného kľúča dešifruje správu a získa tak užívateľov tajný kľúč. Po ukončení procesu obe strany vlastnia unikátny tajný kľúč a komunikácia môže začať.

OTÁZKY

1. Vysvetlite rozdiel medzi stenografiou a kryptografiou.
2. Vysvetlite, čo znamená šifrovanie end-to-end.
3. Vysvetlite princíp šifrovania.
4. Čím sa líši symetrické šifrovanie od asymetrického?
5. Aký kryptosystém vznikne kombináciou symetrického a asymetrického šifrovania?

ZDROJE

Doseděl, T. (2004). *Počítačová bezpečnost a ochrana dat.* Praha: Grada.

Levický, D. (2005). *Kryptografia v informačnej bezpečnosti.* Košice: Elfa.

Ochodková, E. (2003). *Kryptografie a počítačová bezpečnosť.* Ostrava: Technická univerzita Ostrava.

Přybil, J. (2004). *Informační bezpečnost a utajování zpráv.* Praha: ČVUT Praha.

Rjaško, M. (31. 5 2023). *Kryptológia - Úvod do informačnej bezpečnosti.* Dostupné na Internete: http://www.dcs.fmph.uniba.sk/~rjasko/uib/crypto_2018.pdf

Stanek, M. (2004). *Základy kryptológie.* Bratislava: FMFI UK.