Operačný program VZDELÁVANIE

Agentúra Ministerstva školstva, vedy, výskumu a športu SR pre štrukturálne fondy EÚ

Európska únia
Európsky sociálny fond

Stredná odborná škola polytechnická, Demänovská cesta 669, 031 01 Liptovský Mikuláš

Prezentácia – bezpečná komunikácia

Predmet: informatika
Ročník: druhý, štvorročný
Vytvorené dňa: 24.1.2015
Autor: Mgr. Andrej Štefaničiak

Bezpečná komunikácia prostredníctvom internetu

V internete môže prechádzajúce pakety s dátami odchytiť a zmeniť alebo prečítať ktokoľvek. Preto boli pre takúto komunikáciu vyvinuté bezpečnostné prvky v týchto oblastiach:

- integrita dát
- dôvernosť dát
- autenticita dát
- datovanie a časovanie

Najčastejšie používaným prostriedkom bezpečnej komunikácie je zabezpečené spojenie pomocou protokolu **HTTPS** (S = security).

Možnosti zabezpečenia komunikácie v prostredí internetu:

- symetrická a asymetrická kryptografia
- bezpečnostné certifikáty a certifikačná autorita
- elektronický podpis
- heslo

Symetrická a asymetrická kryptografia

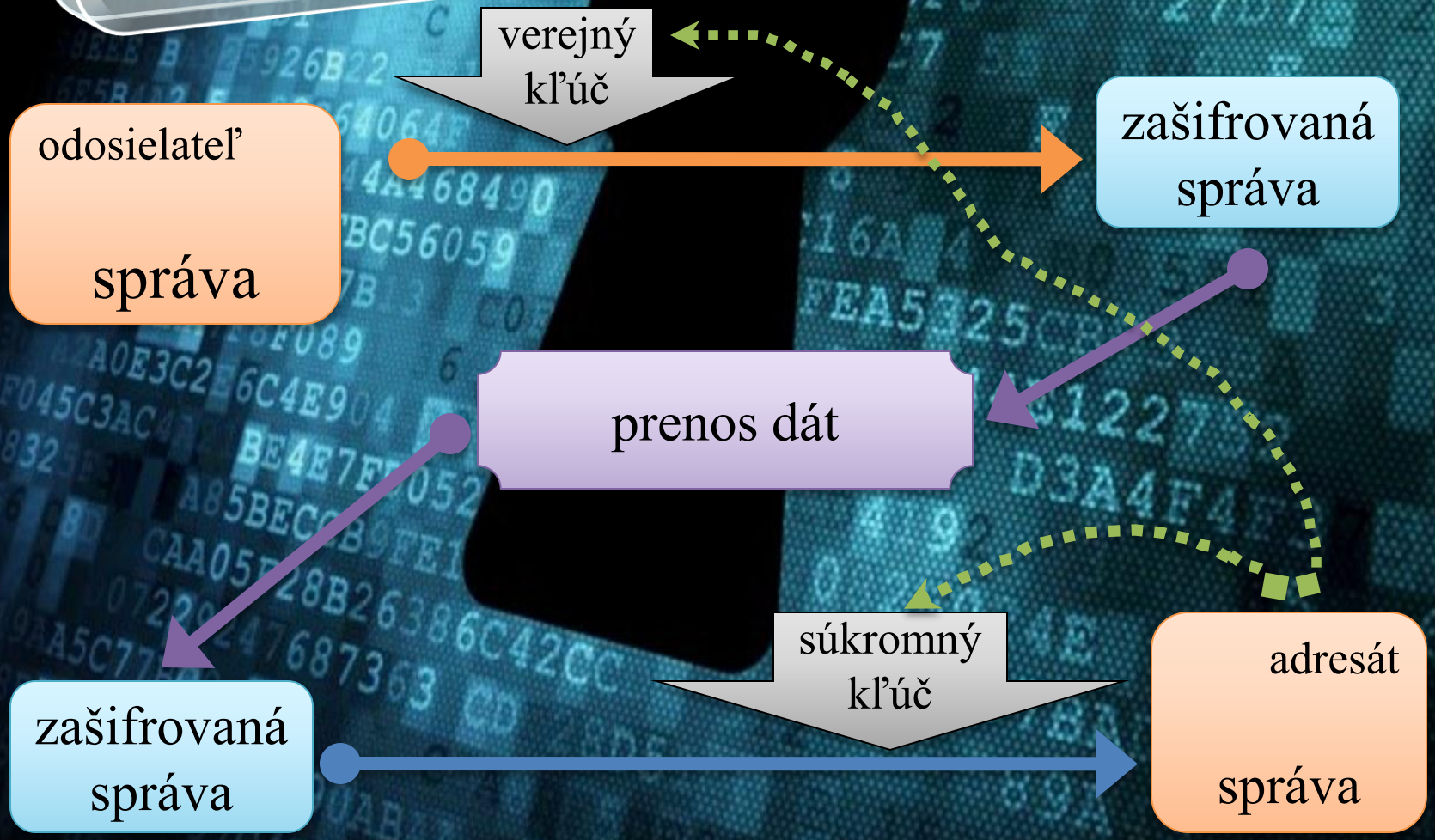
Kryptografia je veda zaoberajúca sa šifrovaním. Bezpečnosť šifry závisí na použitom algoritme dĺžke použitého kľúča či kľúčov.

Používa sa:

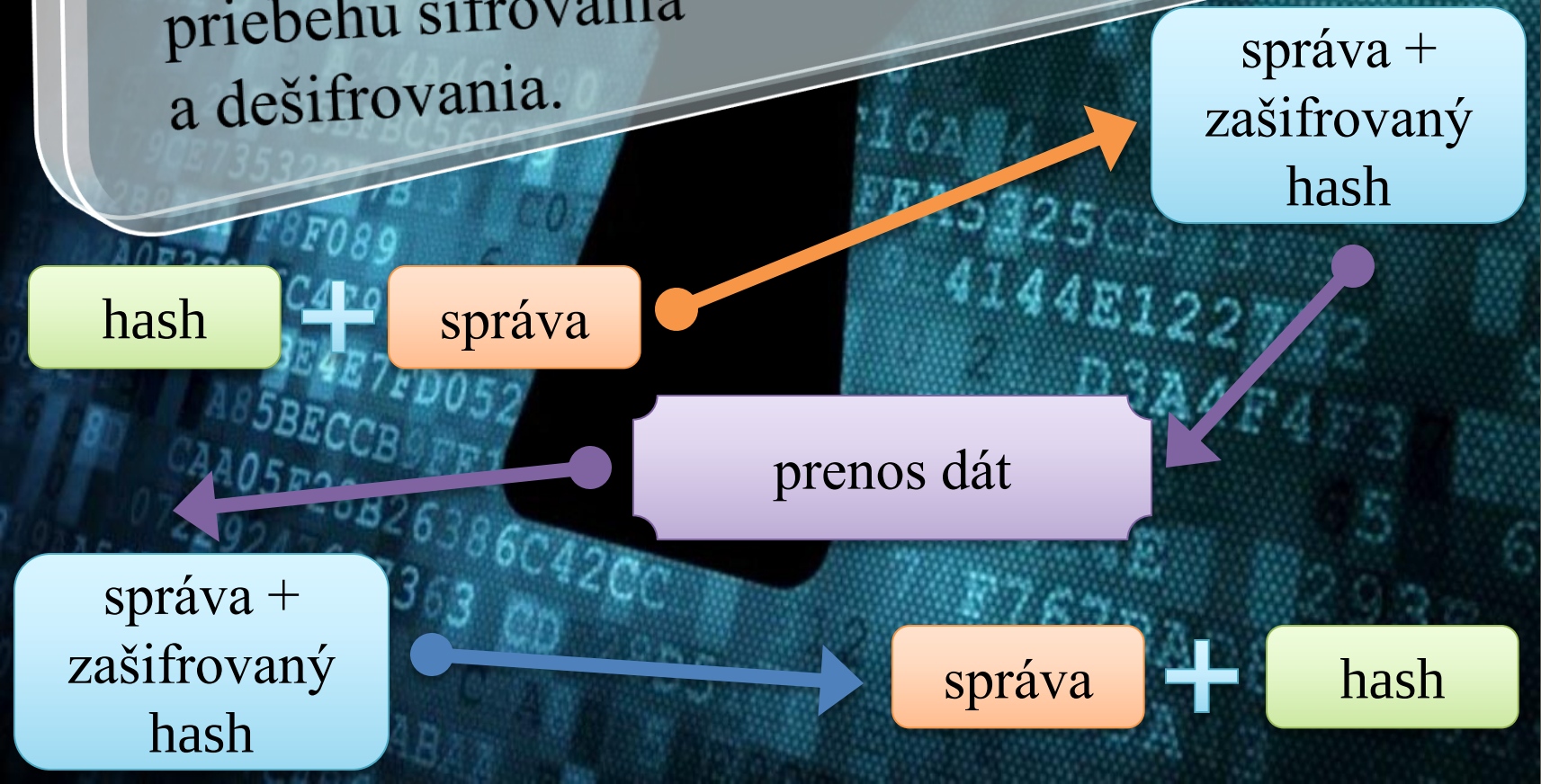
- symetrická kryptografia
- asymetrická kryptografia
- hash dokumentu

Pri **symetrickej kryptografii** sa používa jeden algoritmus a kľúč, ktorými sa správa zašifruje aj dešifruje.

Pri **asymetrickej kryptografii** sa používa algoritmus a dva kľúče. Verejným sa šifruje a súkromným dešifruje.



Hash je odtlačok dokumentu, ktorý predstavuje textový reťazec. Hash sa vypočíta pri odoslaní aj prijatí správy. Ak boli oba výsledky správne, tak posielaná správa nebola pozmenená. Výhodou je zrýchlenie priebehu šifrovania a dešifrovania.



Šifrovaná komunikácia má jeden problém, ktorý sa snaží odstrániť inštitút **certifikačnej autority**. Jej úlohou je odovzdať overené **bezpečnostné certifikáty**. Certifikát je súbor s údajmi o určitej osobe (firme), ktorý je elektronicky podpísaný.

Čo potrebujeme k **elektronickému podpisu**:

- súkromný kľúč
- program (algoritmus) na vytvorenie el. podpisu

Ako podpísať dokument?

1) odosielateľ zadá do programu umiestnenie dokumentu a heslo pre sprístupnenie súkromného kľúča
2) program vygeneruje podpis, ktorý sa uloží do nového súboru (dokument s podpisom = 2 súbory na odoslanie)
3) adresát overí podpis tak, že do programu zadá umiestnenie dokumentu a súboru s podpisom
4) program si načíta údaje zo súboru s podpisom a porovná ich s overovaným dokumentom

Silné **heslo** obsahuje aspoň 6 znakov, nedáva žiadny zmysel, obsahuje veľké a malé písmená, čísla a iné znaky (@, ?...).

Ako sa môže k heslu dostať niekto iný?

- sociotechnickými prostriedkami
- využitím neopatrnosti užívateľa
- škodlivým kódom

Pri využití programových prostriedkov na zistenie hesla sa používajú tieto metódy:

- útok hrubou silou
- slovníkový útok
- podobné alebo zhodné heslá

Otázky na záver:

1) Čo to bola Enigma?
2) Pre komunikáciu prostredníctvom internetu boli vyvinuté bezpečnostné prvky. V akých oblastiach?
3) Čím sa zaoberá kryptografia?
4) Pri asymetrickom šifrovaní sa používajú dva kľúče. Aké sú to a kto je ich vlastníkom?
5) Čo je to hash dokumentu?
6) Povedzte príklad silného a pritom zapamätateľného hesla.
7) Čo je to bezpečnostný certifikát a kto ho vydáva?

KONIEC
Esc