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

PROGRAMOVÉ VYBAVENIE POČÍTAČOV

Ochrana informácií v počítačových sieťach, kódovanie

3. ročník

Šifrovacie algoritmy, použitie šifrovacích algoritmov v sieťach

(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

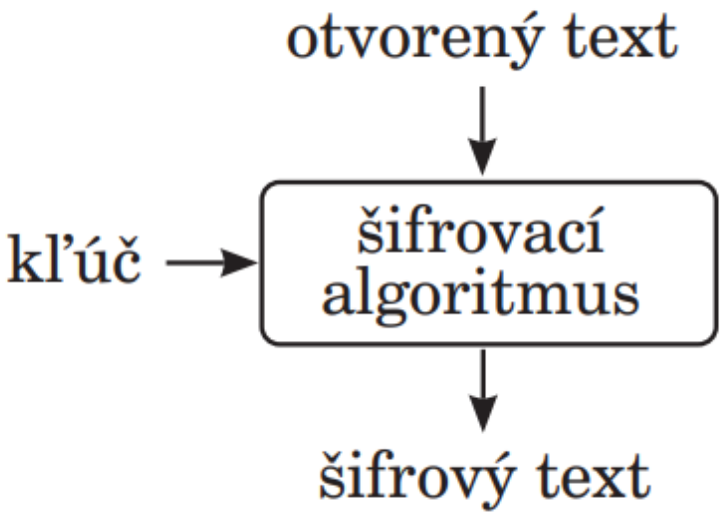
1 ŠIFROVACIE ALGORITMY

Šifrovanie si kladie za cieľ transformovať vstupné dáta do podoby, v ktorej sú pre potenciálneho útočníka nezrozumiteľné, a nie je schopný rekonštruovať ich pôvodný tvar.

ZAPAMÄTAJTE SI!

Šifrovanie prebieha aplikáciou množstva matematických operácií na spracúvané dáta. Táto množina operácií sa všeobecne nazýva algoritmus.

V minulosti sa používali rôzne druhy algoritmov, ako napr. proprietárny algoritmus, pri ktorom sa utajoval princíp algoritmu. V modernej kryptografii sa používajú algoritmy závislé na kľúči (obr. 1.1).



Obr. 1.1 Šifrovanie

Proces inverznej transformácie, keď zo šifrového textu dostaneme opäť pôvodný otvorený text, sa nazýva dešifrovanie a je realizovaný dešifrovacím algoritmom (funkciou).

1.1 Algoritmy asymetrického šifrovania

Pri asymetrickom šifrovaní sa používajú dva matematické vzťahy. Jeden vzťah na šifrovanie, druhý vzťah na dešifrovanie.

Medzi najznámejšie algoritmy asymetrickej kryptografie patria:

- Diffie – Hellmanov algoritmus,
- algoritmus RSA,
- ElGamalov algoritmus,
- DSA,
- šifrovanie na základe eliptických kriviek.

1. **Diffie – Hellmanov algoritmus:**
   - prvý asymetrický algoritmus,
   - navrhovateľmi sú Whitfield Diffie a Martin Hellman,
   - najčastejšie sa používa v hybridnom šifrovaní pre výmenu tajných kľúčov symetrickej kryptografie,
   - využíva sa na šifrovanie aj na podpisovanie,
   - vychádza z toho, že účastníci A a B si vymieňajú tajný kľúč pomocou verejných správ.

2. **ELGamalov algoritmus:**
   - vychádza z algoritmu Diffie – Hellman,
   - postavený na princípe riešenia diskrétneho logaritmu,
   - využíva sa na šifrovanie aj na podpisovanie.

3. **Algoritmus digitálneho podpisu:**
   - digital signature algorithm – DSA,
   - určený len na podpisovanie.

4. **Kryptografia na báze eliptických kriviek:**
   - prišli na to nezávisle na sebe dvaja vedci - Vietor Miller a Neal Koblitz,
   - umožňuje dosiahnuť rovnakú kryptografickú bezpečnosť pri menšej dĺžke kľúča,
   - medzi eliptickými krivkami a algoritmom RSA existuje určitá zhoda,
   - väčšia rýchlosť a menšie nároky na technické prostriedky.

5. Algoritmus RSA:

- v súčasnej dobe je najpoužívanejším algoritmom asymetrickej kryptografie,
- v praxi je najčastejšie používaný na šifrovanie krátkych správ, digitálny podpis, príp. na šifrovanie pri prenose kľúča,
- používa sa na zabezpečenie telekomunikačných kanálov a je aj súčasťou veľkého množstva bezpečnostných protokolov.

2 POUŽITIE ŠIFROVACÍCH ALGORITMOV V SIEŤACH

V súčasnej dobe sa asymetrická kryptografia používa v mnohých produktoch informačných a telekomunikačných firiem na celom svete. Poskytuje množstvo výhod, ako je nenáročná správa kľúčov, možnosť podpisovania atď. Asymetrické šifrovanie je pre svoju bezpečnosť a jednoduchú správu kľúčov často používané aj v elektronickom bankovníctve, obzvlášť pre zabezpečenie komunikácie banky s externými subjektmi.

2.1 Použitie asymetrického šifrovania v elektronickom bankovníctve

Existuje veľké množstvo spôsobov elektronickej komunikácie s bankou prostredníctvom rôznych služieb. Za najčastejšie používanú službu v elektronickej komunikácii medzi bankou a klientom je možné považovať internet banking.

Internet banking poskytuje klientom:

- moderný spôsob komunikácie,
- rýchly a komfortný prístup k financiám bez časového stresu a osobnej návštevy banky,
- okamžitý prehľad o finančných prostriedkoch.

Jedným z najdôležitejších kritérií pre bezpečnosť elektronického bankovníctva je bezpečnosť prenášaných dát. Hlavnými kritériami pre bezpečnosť prenášaných dát sú:

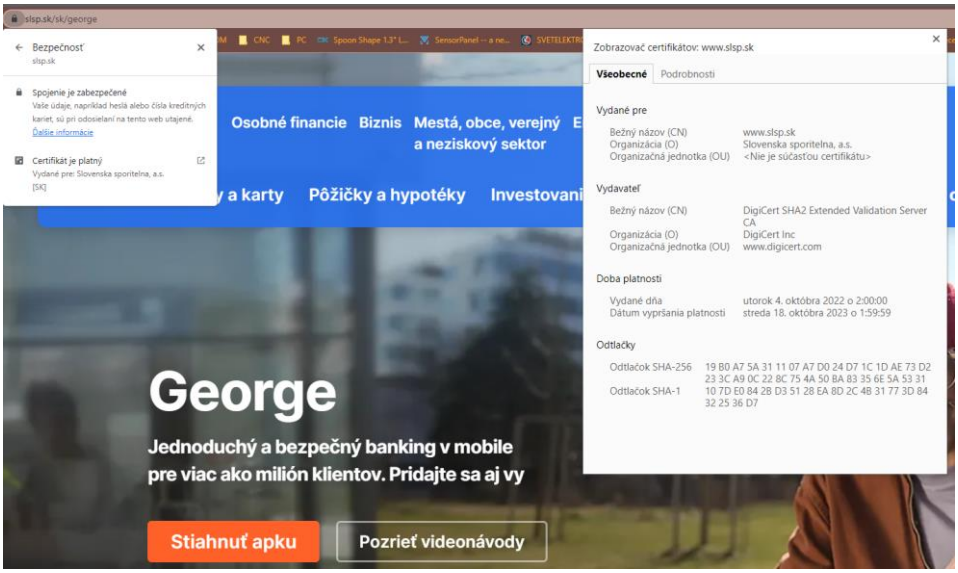
- dôvernosť,
- dostupnosť,
- neodmietnuteľnosť (nepopierateľnosť).

Na zabezpečenie komunikácie sa využívajú rôzne bezpečnostné protokoly využívajúce rozličné metódy autentifikácie a šifrovania prenášaných dát.

2.2 Zabezpečenie internetového bankovníctva

Zabezpečenie komunikácie medzi bankou a klientom sa skladá z niekoľkých častí.

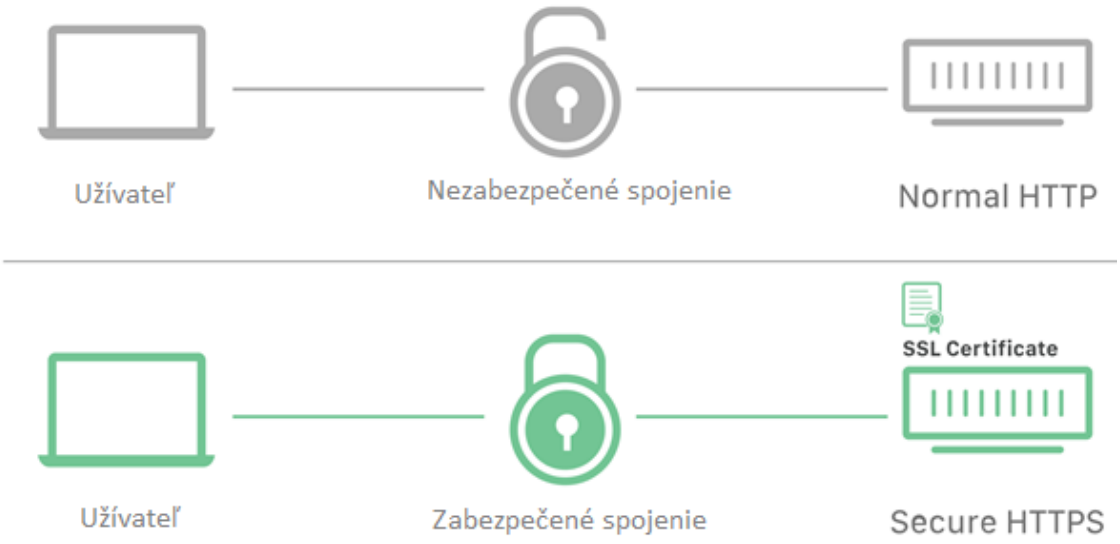
Prvá časť spočíva v overení pravosti internetovej stránky banky. Každá internetová stránka banky obsahuje certifikát (obr. 2.1), vydaný certifikačnou autoritou a klient si ho môže kedykoľvek skontrolovať.



Obr. 2.1 Overenie bezpečnosti internet bankingu Slovenskej sporiteľne – George.sk

Druhá časť je samotná komunikácia medzi bankou a klientom, ktorá je zabezpečená pomocou SSL (Secure Socket Layer) vrstvy. SSL bol prvým kryptografickým protokolom svojho druhu. Pod jeho skratkou sa skrýva jednoduché spojenie Secure Sockets Layer. V marci roku 1995 bol SSL uvedený dovtedy populárneho prehliadača Netscape Navigator 1.1.

Pomocou vrstvy SSL sa často zabezpečuje aplikačný protokol HTTP. Zabezpečený protokol HTTP sa označuje skratkou HTTPS (obr. 2.2), ktorá sa zobrazí po prihlásení na zabezpečenú webovú stránku, avšak SSL dokáže podporovať aj iné protokoly, napríklad FTP, POP3, SMTP atď. SSL podporuje veľké množstvo šifier modernej kryptografie ako napr. RSA, DES, 3DES alebo SHA-1.



Obr. 2.2 HTTP vs HTTPS

TLS (Transport Layer Security) bol prvý krát predstavený v roku 1999 ako zdokonalená pôvodná SSL verzia 3.0. Jeho autormi sú americkí inženieri Christopher Allen a Tim Dierks.

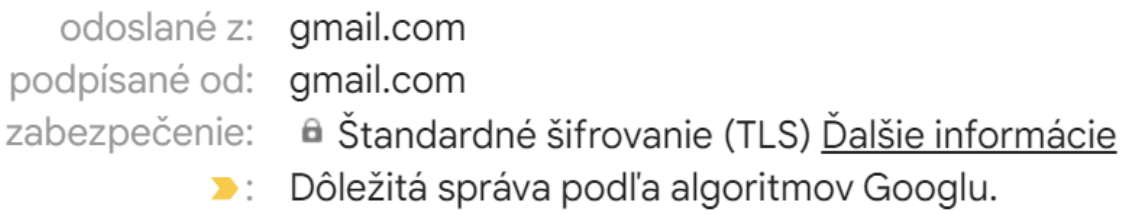
Rozdiely medzi TLS a SSL 3.0 nie sú dramatické, ale sú dostatočne významné, aby vylučovali schopnosť vzájomne spolupracovať.

ZAPAMÄTAJTE SI!

Protokol TLS umožňuje sieťovú komunikáciu medzi aplikáciami tak, aby bolo zabránené odposluchu či falšovaniu preposielaných dát.

TLS je najpoužívanejší štandard pre zabezpečenie komunikácie medzi dvomi či viac zariadeniami naprieč internetom. Garantuje dôveryhodnosť a integritu prenášaných informácií. Najväčšie uplatnenie TLS nachádza v zabezpečovaní relácií medzi webovým prehliadačom a webovým serverom. Využíva sa takmer všade, od VPN po video chat.

Mnoho poskytovateľov e-mailových služieb nešifruje prenos údajov správ. Ak prostredníctvom týchto poskytovateľov odosielate alebo prijímate e-maily, vaše správy si môžu prečítať internetoví sliediči rovnako, ako by prečítali vašu pohľadnicu v pošte. Stále viac poskytovateľov e-mailových služieb sa to snaží zmeniť šifrovaním správ prijímaných a odosielaných pomocou protokolu Transport Layer Security (TLS) (obr. 2.3). Všeobecne sa používanie šifrovania prenosu údajov časom rozširuje, pretože čoraz viac poskytovateľov ho začína podporovať a udržiavať.



Obr. 2.3 Štandardné šifrovanie pomocou protokolu TLS

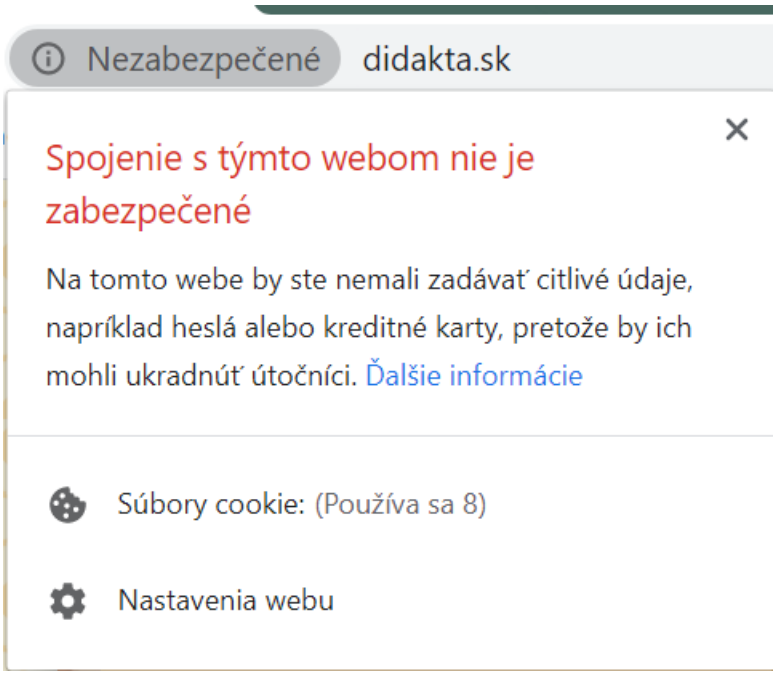
2.3 Nezabezpečený alebo Nebezpečný

Na takýchto stránkach sa neodporúča zadávať súkromné ani osobné informácie. Ak je to možné, web nepoužívajte (obr. 2.4).

Nezabezpečený: postupujte opatrne. Web má závažný problém so zaistením súkromného pripojenia. Cudzie osoby môžu vidieť informácie, ktoré odošlete či dostanete prostredníctvom tohto webu.

Môže sa zobraziť hlásenie „Prihlásenie nie je zabezpečené“ alebo „Platba nie je zabezpečená“.

Nebezpečný: tomuto webu sa vyhnite. Ak dostanete červené upozornenie vypĺňajúce celú obrazovku, web bol službou **Bezpečné prehliadanie** nahlásený ako nebezpečný. Používaním tohto webu vystavíte svoje súkromné informácie riziku.



Obr. 2.4 Nezabezpečená stránka

ZAPAMÄTAJTE SI!

Bezpečné prehliadanie je služba zostavená bezpečnostným tímom spoločnosti Google určená na identifikáciu nebezpečných webových stránok na internete a upozorňovanie používateľov a vlastníkov webových stránok na potenciálne hrozby.

OTÁZKY

1. Čo je dešifrovanie?
2. Popíšte asymetrické šifrovanie a jeho výhody.
3. Charakterizujte TLS protokol.
4. Na akých web stránkach by sme nemali zadávať „citlivé“ informácie a prečo?

ZDROJE

Dobda, L. (2001). *Ochrana dat v informačních systémech.* Praha: Grada.

Grošek, O., & Porubský, Š. (1992). *Šifrovanie : algoritmy, metódy, prax.* Praha: Grada.

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

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