Kryptografie, elektronický podpis

Ing. Miloslav Hub, Ph.D.

27. listopadu 2007

Kryptologie

- **Kryptologie** – věda o šifrování, dělí se:
  - **Kryptografie** – nauka o metodách utajování smyslu zpráv převodem do podoby, která je čitelná jen se speciální znalostí.
  - **Kryptoanalýza** – nauka o luštění zašifrovaných zpráv.
- Kryptologie není steganografie, hashování, ani kódování.

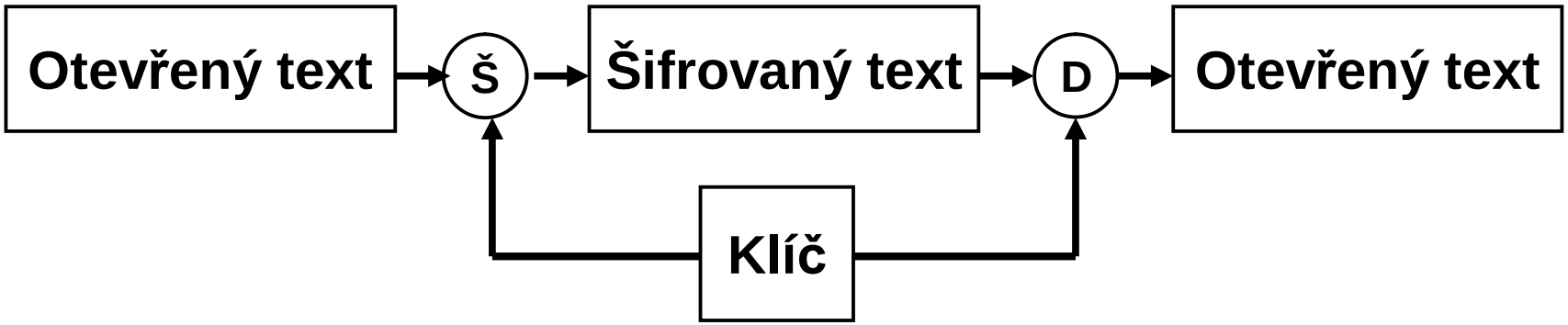
Cíle kryptografie

- Mezi základní cíle kryptografie patří:
  - Důvěrnost
  - Integrita
  - Autentizace
  - Nepopiratelnost

Rozdělení šifrovacích algoritmů

- Substituční x transpoziční
- Proudové x blokové
- Symetrické x asymetrické

Symetrické šifry



- Pro šifrování í dešifrování používán stejný klíč.
- Problém s distribucí a správy klíče.
- Rychlejší, než asymetrické algoritmy.
- Např. AES, DES, IDEA, Triple DES, Skipjack, Caesarova šifra, Vernamova šifra, Vigenerova šifra,…

Substituční šifry

- Každý znak otevřeného textu se nahrazuje jiným znakem šifrovaného textu.
- Aby příjemce získal otevřený text, musí na zašifrovaný text použít inverzní substituci.
- Možnost prolomení frekvenční kryptoanalýzou.

Druhy substitučních šifer

- V klasické kryptografii existují čtyři typy substitučních šifer:
  - **Monoalfabetická šifra** (jednoduchá substituční šifra) - každý znak otevřeného textu se nahradí příslušným znakem šifrovaného textu.
  - **Homofonní substituční šifra** - jeden znak otevřeného textu může byt nahrazen jedním z několika možných znaků šifrovaného textu. Znak „A“ by mohl být nahrazen např. 5, 10, 13 nebo 25.
  - **Polygramová substituční šifra** - šifrování probíhá mezi skupinami znaků. Skupina „AA“ může být nahrazená skupinou „JH“, „AB“ skupinou „DK“ atd.
  - **Polyalfabetická substituční šifra** - skládá se z několika jednoduchých šifer, které se postupně pro jednotlivé znaky otevřeného textu střídají.

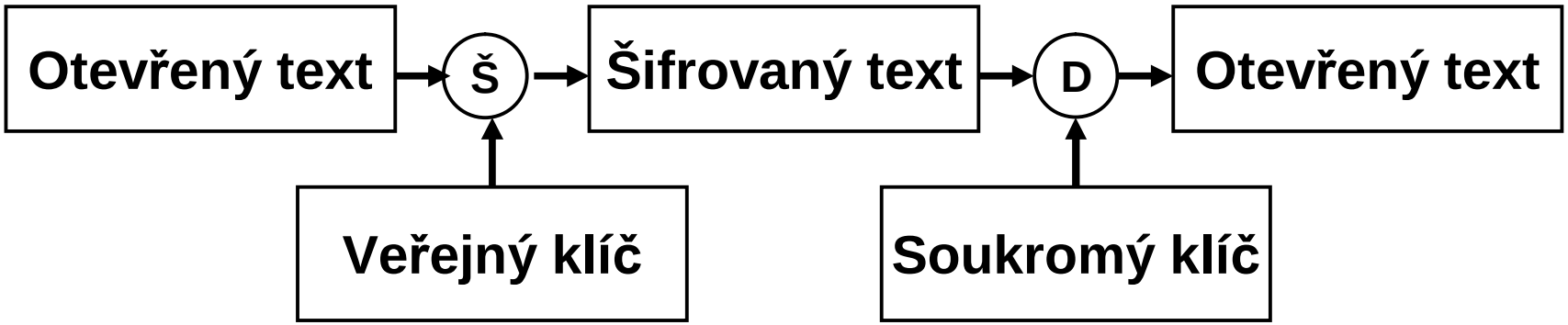
Vernamova šifra

- Jediná skutečně neprolomitelní šifra:
  - Náhodně vygenerovaný klíč
  - Klíč použit pouze jednou
  - Klíč stejně dlouhý jako šifrovaná zpráva

Transpoziční šifry

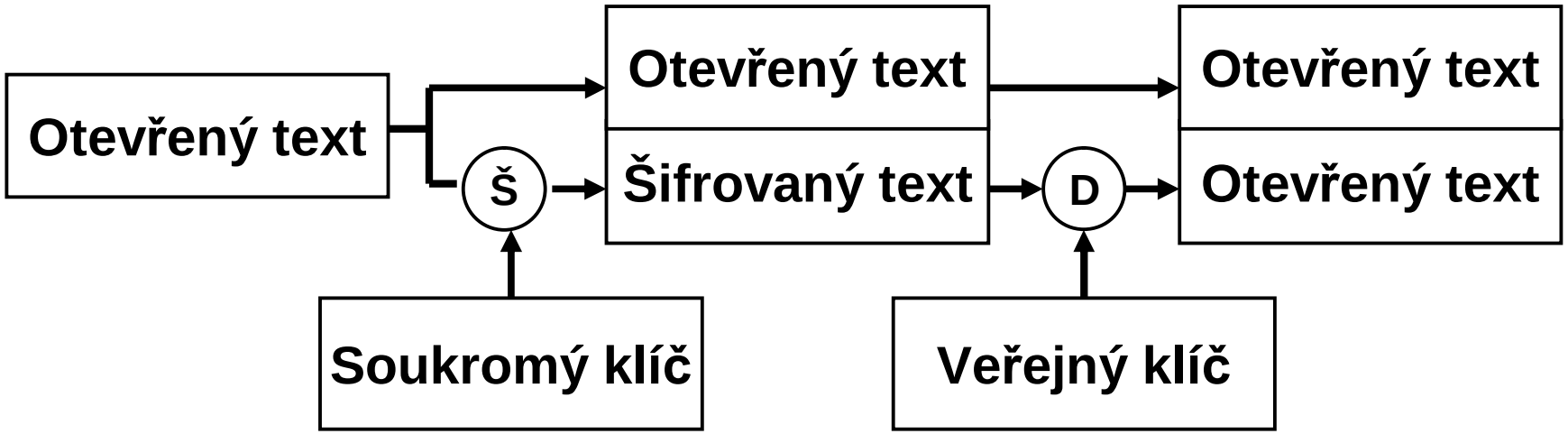
- Transpozice neboli spočívá ve změně pořadí znaků podle určitého pravidla.
- Například tak, že otevřený text je zapsán do tabulky po řádcích a šifrový text vznikne čtením sloupců téže tabulky.

Asymetrické šifry



- Pro šifrování jiný klíč (veřejný), než pro dešifrování (soukromý, tajný).
- Ze soukromého klíče lze odvodit veřejný, naopak nelze.
- Lze použít i pro elektronický podpis.
- Např. RSA, ElGamal, kryptografie nad eliptickými křivkami, Diffie-Hellman, Digital Signature Algorithm,…

Elektronický podpis - princip



- Při realizaci se nepodepisuje celá zpráva, ale z důvodu efektivity pouze hash původní zprávy.
- Hashovací algoritmus umožňuje jednosměrnou transforomaci libovolného množství dat do dat pevné délkynapř.:
  - MD5 – 128 bitů
  - SHA1 – 160 bitů

PKI (Public Key Infrastrukture)

- Prostředí, které umožňuje ochranu informačních systémů, elektronických transakcí a komunikace.
- Zahrnuje veškerý software, technologie a služby, které umožňují využití šifrování s veřejným a privátním klíčem.
- PKI zahrnuje celou řadu různých komponentů, např.
  - digitální certifikáty
  - klíče
  - asymetrická kryptografie
  - certifikační autorita
  - bezpečenostní architektura sítě
  - způsob bezpečného vydávání certifikátů
  - nástroje pro správu, obnovu a rušení certifikátů

Digitální certifikát

- Umožňuje spolehlivě identifikovat skutečného odesilatele zprávy.
- Vydává ho nějaký třetí, nezávislý subjekt. Tímto subjektem je takzvaná certifikační autorita (v zákoně 227/2000 Sb. o elektronickém podpisu se nazývá poskytovatel certifikačních služeb).
- Vydáním certifikátu certifikační autorita stvrzuje, že subjekt, kterému byl certifikát vydán, skutečně vlastní daný pár klíčů.
- Jedná se o datový soubor, uložený ve standardním, mezinárodně platném formátu. Pro certifikáty se používá mezinárodní norma X.509, která jednoznačně popisuje strukturu certifikátu.

Struktura certifikátu

- Každý certifikát musí obsahovat následující údaje:
  - Verze standardu X.509
  - Sériové číslo
  - Datum počátku a konce platnosti certifikátu
  - Identifikační údaje subjektu
  - Druh algoritmu
  - Veřejný klíč subjektu.
  - Identifikační údaje certifikační autority
  - Veřejný klíč CA
  - Podpis CA
- Další možné nepovinné položky, např. účel certifikátu apod.