evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERSITAS MASARYKIANA BRUNENSIS
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

ŠIFROVÁNÍ – VÝVOJ, ZÁKLADNÍ PRINCIPY A UKÁZKY

INFORMAČNÍ BEZPEČNOST

17. 4. 2013 KISK FF MU

ŠIFROVÁNÍ – OCHRANA INFORMACÍ

- Programy pro šifrování e-mailů, dokumentů…
- Šifrovaný může být i přenos dat (někdy záleží na rozhodnutí uživatele)
- Ochrana proti odposlechu, krádeži…
- Šifrování se stává povinným – e-podpis = informační politika v současné praxi

TERMINOLOGIE ODVĚTVÍ

- Steganografie – utajení pomocí ukrytí zprávy, např. hlavy otroků
- Kryptologie – „vědecká disciplína věnující se ochraně dat před neoprávněným čtením“ (Doseděl, s. 4)
  - Kryptografie – kódování a šifrování dat
  - Kryptoanalýza – analýza algoritmů (postupů) a zašifrovaných dat

TERMINOLOGIE KRYPTOLOGIE

- Šifrování (písmena) X kódování (slova)
- Kódové knihy nepraktické + míchání se šifrováním (nomenklátory) - dále jen šifrování
- Jediná ukázka kódování: Navahové za 2WW – nikdy neprolomeno
- Šifrování a dešifrování upravuje kryptografický algoritmus

TERMINOLOGIE – KLÍČE

- V literatuře pro vysvětlení: Alice a Bob mají společné tajemství = klíč
- Symetrické (1 klíč) + asymetrické (klíčový pár) = hybridní
- Hybridní řeší nevýhody obou – náhodné číslo = klíč symetrické, zašifrováno asymetricky, např. PGP

AKTUÁLNÍ TRENDY V ŠIFROVÁNÍ

- Dříve časté utajování algoritmů – security through obscurity = základ zabezpečení, ale to se vždy prozradí, proto dnes naopak (každý může ověřit bezpečnost algoritmu) = základ je tajný klíč (Kerckhoffsův princip, 1883)
- Nyní naděje v kvantovém šifrování – na naši přednášku složité (dále neřeším)

SYMETRICKÉ ŠIFRY

- Starší
- Substituce (záměna znaků) a transpozice (přehození pořadí znaků) – dnes většinou obojí
- Nesrovnatelně rychlé proti asymetrickým
- Nutné předání a utajení klíče/algoritmu = největší problém
- S růstem komunikujících nesmírně roste počet klíčů nebo rizikových míst prozrazení

SUBSTITUČNÍ ŠIFRY

- Monoalfabetické – jeden znak nahrazen za druhý, dešifrování frekvenční analýzou, např. Césarova šifra
- Homofonní – každý znak může nahradit více různých znaků
- Polygramová – náhrada skupiny znaků za jinou, např. Playfair (britské vojsko v 1WW)
- Polyalfabetická – skupina monoalfabetických postupně aplikovaná dle klíče, dešifrování složitější frekvenční analýzou, např. Vigenèrova „neprolomitelná“ šifra

DALŠÍ SYMETRICKÉ ŠIFRY

- Transpoziční – změna pořadí znaků, výhodou rozbití větších struktur, nevyužitelnost frekvenční analýzy
- Opravdu (?) nerozluštitelná šifra – délka zprávy = délka klíče
- DES (Data Encryption Standard) – norma ANSI a ISO, dnes nevyhovující (krátký klíč), využití substituce i transpozice, bloková šifra, míchání těsta
- AES (Advanced Encryption Standard, Rijndael) – náhrada DES, podobný princip, ale delší klíč a o něco složitější algoritmus

CO SI TO VYZKOUŠET?

- Úkoly s šifrováním
- Technoplaneta

ASYMETRICKÉ ŠIFRY

- Pár klíčů (soukromý a veřejný) – jedním šifrovat, druhým dešifrovat, z veřejného soukromý nezjistitelný
- Snazší správa klíčů (počet klíčů = 2x počet uživatelů) X pomalé a nutné delší klíče
- RSA (Rivest, Shamir, Aleman)
  - Dosud neprolomeno
  - Faktorizace velkých prvočísel
  - (Složité) stanovení pravidel pro tvorbu klíčů
  - Normalizován + v USA patentován (vypršelo)

KLÍČE ASYMETRICKÉ ŠIFRY

- Základem výpočetně náročné problémy, které jsou s jistou znalostí snadno řešitelné; dnes nejběžnější:
  - Faktorizace součinu velkých prvočísel (RSA – tím se šifruje i symetrický klíč v PGP, aby to bylo rychlé)
  - Problém výpočtu diskrétního logaritmu
  - Problematika eliptických křivek

DIGITÁLNÍ PODPIS

- = opačný princip než asymetrické šifrování
- Zajišťuje integritu (nezměněnost) a nepopiratelnost (autor je podepsán) X šifrování důvěrnost dat
- Již dle zákona mnoha zemí (i ČR) ekvivalentní tradičnímu podpisu (nutné splnění daných podmínek)
- Integrita – kontrolní součty
  - Matematickými funkcemi vznikne krátký digitální otisk (hash) identifikující zprávu (jedinečný + zpětné zjištění téměř neproveditelné)
  - Odesilatel zašifruje a přiloží, příjemce sám spočítá, dešifruje a srovná
  - Nejpoužívanější hashovací funkce: MD4, MD5 a SHA-1

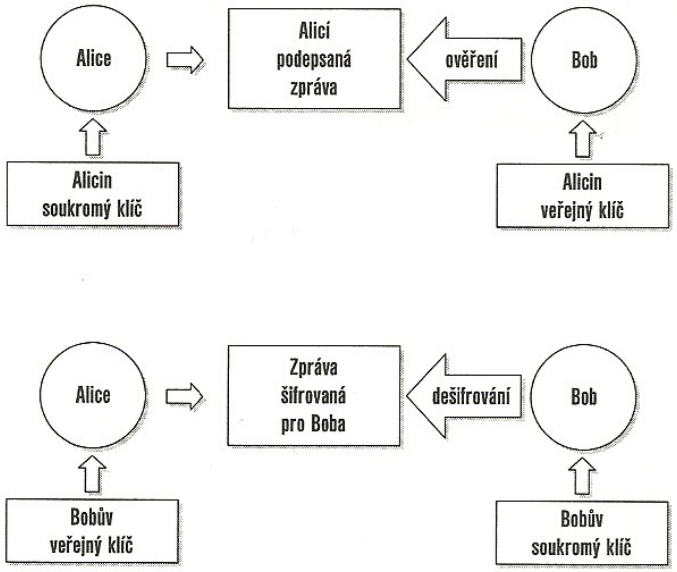
CERTIFIKOVANÝ KLÍČ

Obsah certifikátu veřejného klíče	
Položka	**Popis**
ID certifikátu	Jednoznačné sériové číslo
Datum vydání	Kdy byl certifikát vydán
Platnost do	Časové omezení platnosti
Omezení certifikátu	Účel, pro který lze certifikát použít (např. podepisování)
ID certifikační autority	Kdo certifikát vydal
Algoritmy CA	Jaké algoritmy používá pro podepisování certifikační autorita
Veřejný klíč CA	Nemusí být součástí certifikátu
ID vlastníka	Rodné číslo či IČO
Veřejný klíč vlastníka	Vlastní certifikovaný klíč
Podpis	Předchozí data jsou podepsána soukromým klíčem CA

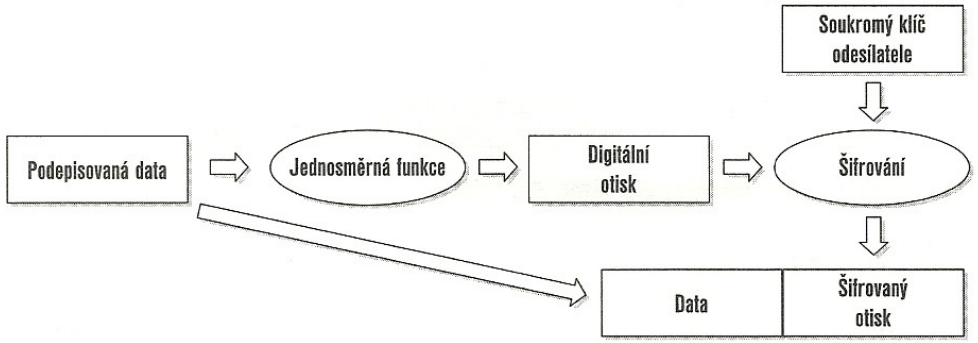
Tabulka 5.1: Obsah certifikátu

- Nepopiratelnost podpisu zajištěna soukromým klíčem (zná jen oprávněná osoba), ten jedinečný a zpětně nezjistitelný, a kvalifikovaným certifikátem (vytváří autorita, nutné ověřovat platnost)
- Obsah certifikátu veřejného klíče libovolný, ale existují i normy, např. ITU X.509
- 4 třídy certifikátů (čím vyšší, tím víc požadavků), pro komunikaci se státní správou min. úroveň 3

DIGITÁLNÍ PODPIS A ŠIFROVÁNÍ



Obrázek 2.10: Šifrování versus podepisování



Obrázek 5.2: Schéma vytváření digitálního podpisu

DIGITÁLNÍ PODPIS – FINÁLE

- Finálně:
  - odesilatel: hash – zašifrování svým soukromým – možné přiložit certifikát a zprávu zašifrovat – odeslání
  - příjemce: možné dešifrování – možné ověření certifikátu – výpočet hashe – dešifrování hashe veřejným klíčem odesilatele – porovnání hodnot hashe
- Český zákon 227/2000 Sb. + prováděcí vyhláška 366/2001 Sb.
- PGP a zákon USA – po umístění PGP na internet zdarma ke stažení v r. 1993 Zimmermann 3 roky předmětem vyšetřování velké porody a pronásledován FBI (nelegální export zbraní); dosud se řeší (bezpečnost X soukromí), i obžaloba Zimmermanna byla po podpoře veřejnosti a odborníků a rozšíření PGP (reklama – FBI se bojí!) stažena

OMEZIT MOŽNOSTI ŠIFROVÁNÍ?

„Je to špatná politika - nekriticky zakázat technologii jen proto, že někteří zločinci ji mohou používat ke svému prospěchu. Například každý občan Spojených států může volně koupit **pár rukavic**, přestože je může **lupič** použít k vyplenění domu bez zanechání otisků. **Kryptografie** je technologií **ochrany dat stejně** jako rukavice jsou technologií ochrany rukou. Kryptografie chrání data před hackery, průmyslovou špionáží a podvodníky, zatímco rukavice chrání ruce před pořezáním, odřeninami, horkem, chladem a infekcí. Kryptografie **může zmařit FBI** odposlech, rukavice jí mohou překazit analýzu otisků prstů. Jak kryptografie, tak rukavice jsou **směšně laciné a široce dostupné**. Dobrý kryptografický software můžete stáhnout z internetu za cenu nižší, než je cena kvalitního páru rukavic.“ (Ron Rivest IN Singh, s. 289)

POUŽITÁ LITERATURA

- BERLOQUIN, Pierre. *Skryté kódy a velkolepé projekty: tajné jazyky od starověku po současnost*. Vyd. 1. Praha: Knižní klub, 2011, 375 s. Universum (Knižní klub). ISBN 978-80-242-2847-1.
- DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.
- ERICKSON, Jon. *Hacking umění exploitace*. Vyd. 1. Brno: Zoner Press, 2005, 263 s. ISBN 80-868-1521-8.
- SINGH, Simon. *Kniha kódů a šifer: Tajná komunikace od starého Egypta po kvantovou kryptografii*. 1. vyd. Praha: Argo, 2003, 382 s. ISBN 80-720-3499-5.
- THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005, 338 s. ISBN 80-251-0417-6.

Děkuji za pozornost.

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ