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

KRYPTOLOGIE

INFORMAČNÍ BEZPEČNOST

AUTENTIZACE + AUTORIZACE

- Identifikace v elektronickém prostředí
  - E-mailová adresa
  - Heslo k různým aplikacím – jak prolomit? => jak má vypadat?
- Ukázka nastavení soukromí na FB:
  - Jméno: ukazkyprovyuku@seznam.cz
  - Heslo: 123456kisk
- Vaše zdroje?

AUTENTIZACE

- Základ bezpečnosti všeho personalizovaného, vč. dat, činností…
- Zařízení, uživatele
- FIDIS (Future of IDentity in the Information Society) – Something you: know, have, are, (do, are assigned to)
- X autorizace
- Dvou- a třífaktorová

ZÁSADY BEZPEČNÉHO HESLA

MUSÍ BÝT:

- Aa1*
- 8/12 znaků
- Změna max. za 90 dní

NESMÍ BÝT:

- Běžné slovo
- Znakové řady
- Přednastavené
- Opakující
- Zapsáno
- Nikomu sděleno

JAK S TÍM?

- Útoky: uhodnutí, lamače
- Pomůcky: algoritmus tvorby, správce, úrovně politiky, HW doplňky
- Vyzkoušíme?

PŘÍKLADY V PRAXI

- Prostá autentizace heslem: SMTP, POP3 a IMAP protokoly pro připojování k e-mailovým serverům, ICQ pro komunikaci přes Internet
- Tokeny: platební karty, autentizační kalkulátor, USB tokeny, telefony (přihlášení na FB)
- Biometriky: přihlašování k mobilním zařízením otiskem prstu, rozpoznáním obličeje
- Grafická hesla: gesta, body na obrázku (Win8/10)

ŠIFROVÁNÍ

- E-mailů, dokumentů…, ale i přenos dat (někdy na rozhodnutí uživatele)
- Ochrana proti odposlechu, krádeži…
- Stává se povinným – e-podpis, GDPR

TERMINOLOGIE

- Kryptologie = kryptografie + kryptoanalýza
- Steganografie X šifrování X kódování
- Kódové knihy nepraktické + míchání se šifrováním (nomenklátory) – dále jen šifrování
- Jediná ukázka kódování: Navahové za 2WW
- Šifrování a dešifrování => kryptografický algoritmus
- Alice a Bob mají společné tajemství = klíč
- Symetrické + asymetrické = hybridní

AKTUÁLNÍ TRENDY

- Dřív utajování algoritmů (security through obscurity) => vždy se prozradí
- Dnes základ tajný klíč (každý může ověřit bezpečnost algoritmu) = Kerckhoffsův princip, 1883
- Naděje v kvantovém šifrování – zde složité (dále neřeším)

SYMETRICKÉ ŠIFRY

- Transpozice X substituce (monoalfabetická, homofonní, polyalfabetická… => frekvenční analýza) – dnes většinou obojí
- Nesrovnatelně rychlé proti asymetrickým
- Problémy:
  - Nutné předání a utajení klíče/algoritmu
  - S růstem komunikujících roste počet klíčů/slabin
- Aktuální (normované):
  - DES – norma ANSI a ISO, už nevyhovující (krátký klíč), substituce i transpozice, bloková šifra, míchání těsta
  - AES – náhrada DES, podobný princip, ale delší klíč a o něco složitější algoritmus

ASYMETRICKÉ ŠIFRY

- Pár klíčů – z veřejného soukromý nezjistitelný
- Snazší správa klíčů X pomalé a nutné delší klíče
- RSA (Rivest, Shamir, Aleman)
  - Dosud neprolomeno
  - Faktorizace součinu velkých prvočísel (ne jediný, ale nejčastěji využívaný výpočetní problém)
  - Normalizován + v USA patentován (vypršelo), využívá i PGP pro šifrování symetrického klíče
- PGP v USA – ke stažení zdarma (1993) Zimmermann 3 roky vyšetřován FBI (nelegální export zbraní); obžaloba stažena => FBI se bojí!

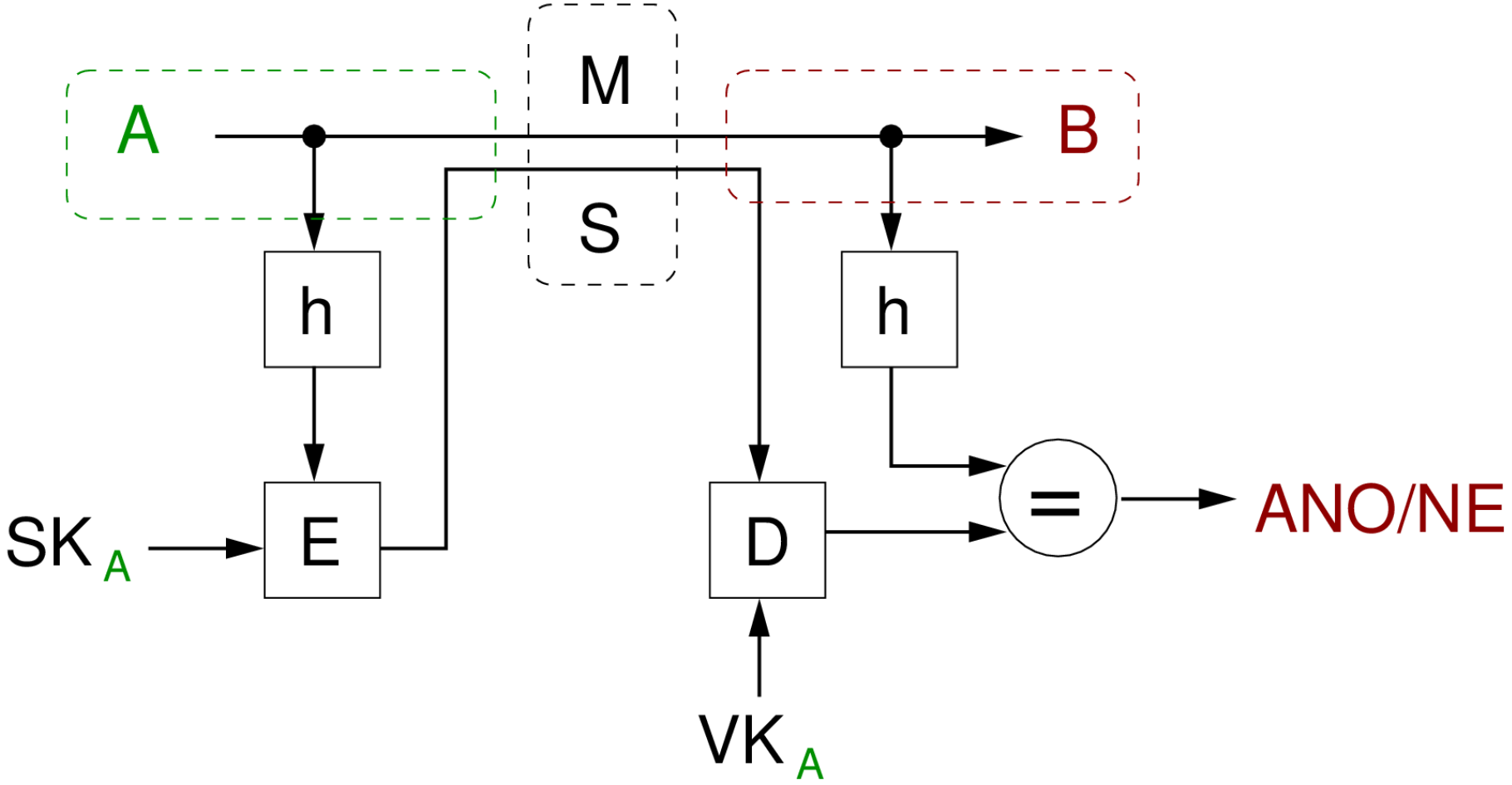
PŘÍKLADY V PRAXI

- Steganografie – zprávy skryté v obrázcích, hudbě
  - Sociální steganografie
- HTTPS – asymetrické šifrování webového přenosu, mezi transportní vrstvou (TCP/IP) a aplikační (HTTP) je SSL
- WPA2 využívá AES
- E-podpis

DIGITÁLNÍ PODPIS

- = opačný princip než asymetrické šifrování
- Zajišťuje integritu a nepopiratelnost X důvěrnost
- V mnoha zemích ekvivalent tradičnímu podpisu
- Garance veřejných klíčů CA

Digitální podpis



CO SI TO VYZKOUŠET?

- Úkoly s šifrováním => test v e-kurzu
- Technoplaneta

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