ŠIFROVÁNÍ

Mgr. Rostislav Fojtík, PhD.
Katedra informatiky a matematiky
Obchodně podnikatelská fakulta v Karviné
Slezská univerzita

Kryptografie

- Šifrování

- Utajování zpráv

Symetrické šifrování

- Jeden klíč k šifrování i dešifrování
- Klíč musí být tajný

Caesarova šifra

- Substituční šifra
- abcdefghijklmnopqrstuvwxyz
- Klíč je posunutí o určitý počet znaků
- Například o 2 znaky, pak a = c

Caesarova šifra

- Slabá šifra - jen 25 různých klíčů
- Lze v krátkém čase prolomit “hrubou silou”
- Vyluštěte zprávu:

fdhvdurydvliudmhvbphwulfndvliud

Symetrické šifrování

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
k	w	y	j	i	b	x	l	q	a	c	z	s	v	u	m	r	t	n	d	o	h	g	p	e	f

- Počet klíčů je 26! - přibližně $4{,}03 \cdot 10^{26}$
- Vyluštěte: cvqlk
-

Kryptoanalýza

- Možnost dešifrovat zprávu i bez znalosti klíče
- Substituční šifry jsou prolomitelné pomocí frekvenční analýzy

Moderní symetrické šifry

- AES (Advanced Encryption Standard) - klíče délky např. 128 nebo 256 bitů
- Rychlé šifry (šifrování/dešifrování disku, souborů… za běhu programů)

Asymetrické šifry

- Dva klíče
  - Klíč k šifrování (veřejný)
  - Klíč k dešifrování (privátní)
- RSA, ECC, DSA

Asymetrické šifry

- Výhodou je navázání bezpečné komunikace
- Není nutné posílat nezašifrovanou zprávu
- Jsou komplikovanější než symetrické šifry
- Umožňuje podvrhnout zprávu

RSA

- Rivest, Shamir, Adleman
- Pro šifrování i digitální podepis
- Deterministicky šifrovací algoritmus

Hashovací funkce

- Úkolem je vytvoření jednoznačného otisku (hash) zprávy
- Jednosměrná funkce, z hasne nelze vyvodit zpětně původní datovou sekvenci
- Kontrola integrity - jednoznačnost hashe pro každou datovou sekvenci
- Hashovací funkce SHA

Digitální podpis

- Elektronický **x** digitální podpis
- Ověření odesílatele
- Ke zprávě se připojí otisk zprávy (hash) zašifrovaný soukromým klíčem odesílatele

Digitální podpis

- Ověření - Identita signatáře dokumentu byla ověřena veřejně důvěryhodnou CA.
- Integrita - Obsah dokumentu se od podpisu nezměnil.
- Nevypovědění - Signatář nemůže věrohodně popřít, že podepsal dokument.

Digitální podpis

- ID certifikát pro digitální podpis
- Kvalifikovaná certifikovaná autorita

…děkuji za pozornost

Mgr. Rostislav Fojtík, PhD.
Katedra informatiky a matematiky
Obchodně podnikatelská fakulta v Karviné
Slezská univerzita
fojtik@opf.slu.cz