Číslo projektu	CZ.1.07/1.5.00/34.0036	**Tématický celek**	Inovace výuky ICT na BPA
Název projektu	Inovace a individualizace výuky	**Název materiálu**	Kryptografie
Číslo materiálu	VY_32_INOVACE_FIL13	**Ročník**	První
Název školy	Bezpečnostně právní akademie Brno, s.r.o., střední škola	**Datum tvorby**	31. 3. 2014
Autor	Ing. Vojtěch Filip		

Anotace

Učební materiál – co je to kryptografie, praktické aplikace kryptografie.

Metodický pokyn

Prezentaci je možné použít kdykoli, nemá striktní kontext. Osvětlí studentům, co je to kryptografie, jaké jsou její běžné aplikace. Dále se diskutují metody zabezpečení počítače, dat, internetových účtů.

Zdroje

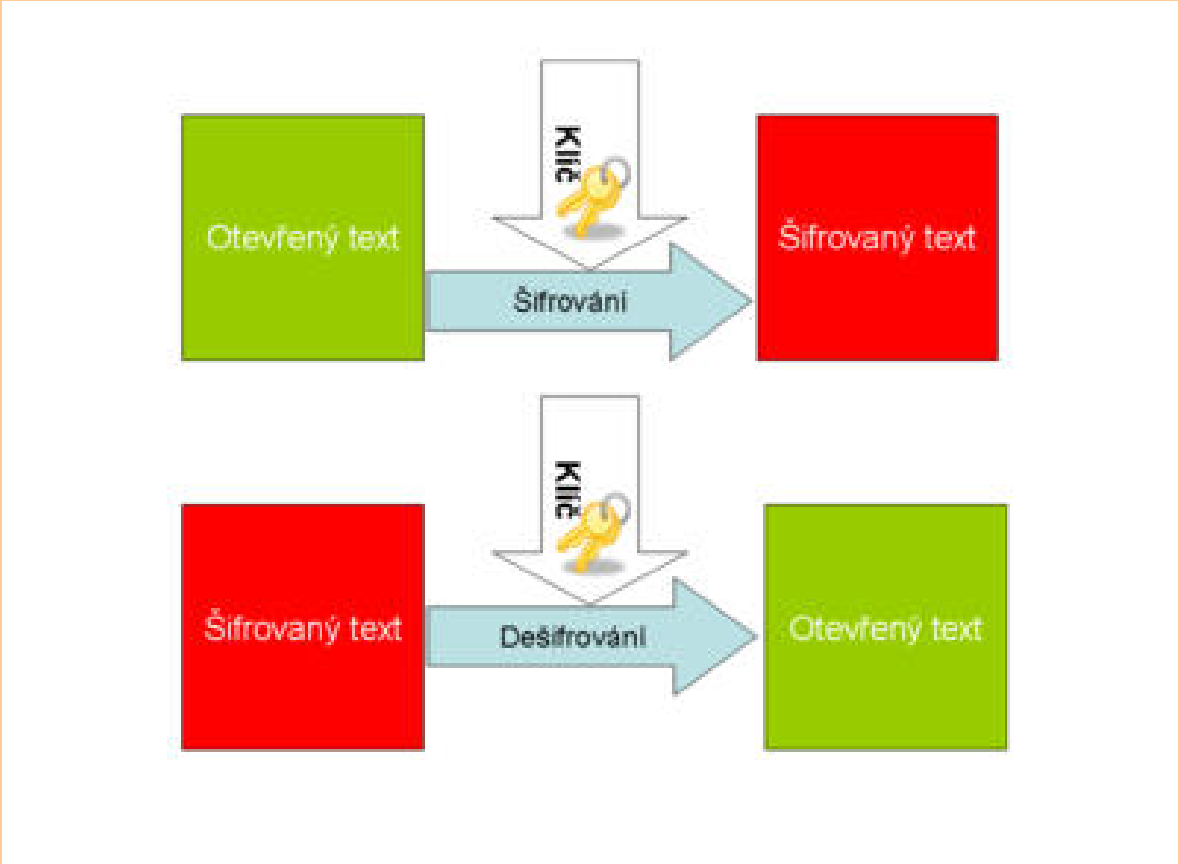
Singh, Simon. *Kniha kódů a šifer: Tajná komunikace od starého Egypta po kvantovou kryptografii.* 2. vydání v českém jazyce. Praha: Dokořán, 2009. ISBN 978-80-7363-268-7.

Šifrování dat

Motivace: cena dat je často vysoká. Jsou-li efektivně šifrovaná, prakticky je nelze zcizit.

Šifrováním dat se zabývá obor
zvaný **kryptografie**.

V praxi se bohužel šifrování
nepoužívá v dostatečné míře.



Obr.: wikipedia.org

Př.: symetrická šifra

Šifrování ve starověku

Již staletí před naším letopočtem se používalo šifer při přenosu zpráv. Šifrování je doloženo z Arábie, Řecka nebo Říma.

Řadu šifer používal například císař Julius Caesar, což zmiňuje v *Zápiscích o válce galské*. Jeho šifry se převážně nedochovaly, avšak jedna z nich je známá dobře, dnes ji označujeme **Caesarova posunová šifra**.

A	B	C	D	E	F	G	H	I	J
X	Y	Z	A	B	C	D	E	F	G

Pro zašifrování se nahradí písmeno na prvním řádku odpovídajícím písmenem na druhém řádku, rozšifrování probíhá naopak.

Slabina: **šifrovací klíčem** je snadné uhodnout, protože se jedná pouze o posunutí řádků vůči sobě, a možných variant je jen tolik, jako písmen v abecedě. Takové šifře říkáme **slabá šifra**.

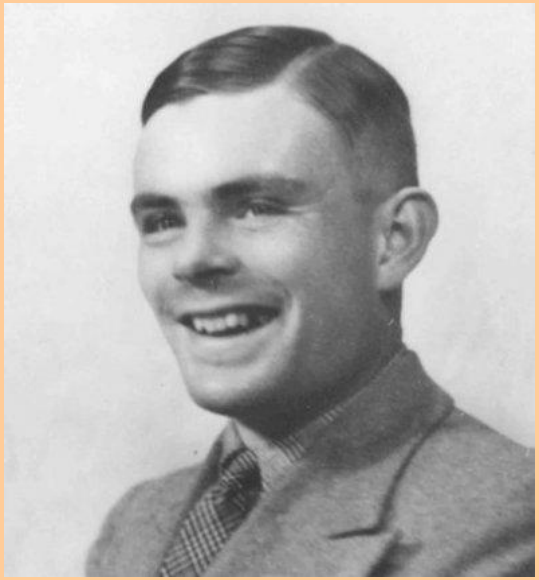
20.století - Enigma

Obr.: wikipedia.com

Mechanický šifrovací stroj pro přenos kódovaných zpráv německou armádou za II. světové války.

Pokusy o lámání šifer, které byly posléze úspěšné, probíhaly při nasazení stovek analytiků v britském **Bletchley Park**.

Pracoval zde i **Alan Turing**, otec moderní výpočetní techniky.



Ukládání hesel

Hesla se v počítači nikdy neukládají v otevřené podobě, ale ve formě takzvaného *otisku* (angl. *hash*).

Příklad:

Jméno:	petr novák	→	petr novák
Heslo:	kobliha	→	fg57Lt?bGWrt5Lhi

Podle otisku hesla je možné heslo ověřit, ne však zpětně zjistit!

Bezpečná hesla – alespoň 8 znaků, kombinace písmen a číslic, nesmí obsahovat běžná slova.

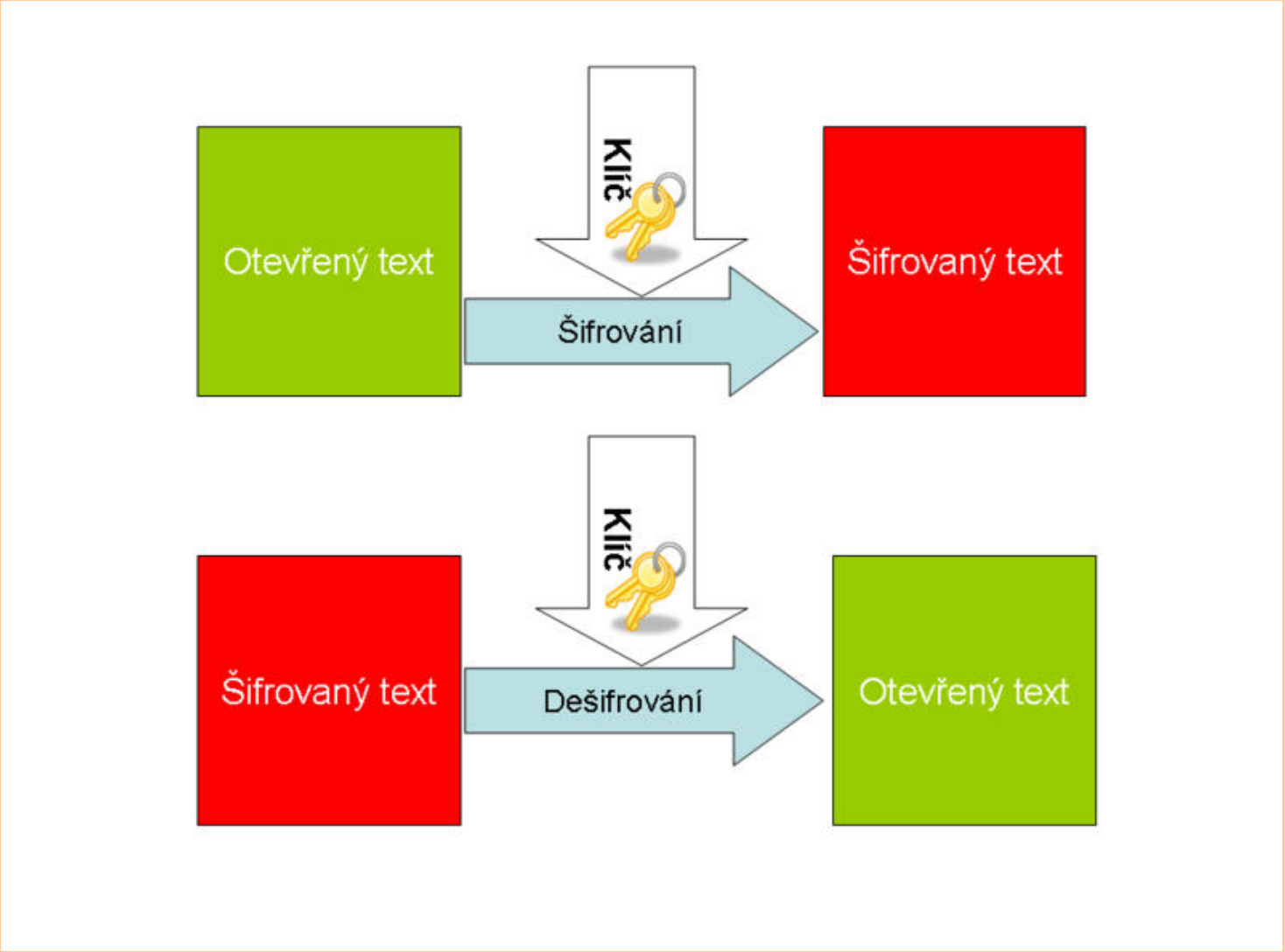
Jednoduché šifrování

Pomocí tzv.
symetrické šifry.

Kdo zná klíč,
může data
zašifrovat
i rozšifrovat.

Příklady využití

- šifrovaný disk
- GSM hovor
- Wi-Fi



Zdroj: wikipedia.org

Šifrování komunikace

- přenos dat v sítích WiFi (WEP, WPA, WPA2)
- šifrování e-mailů (SSL/TLS, PGP)
- mobilní hovory (GSM, UMTS)
- placené televizní vysílání (je zapotřebí dekódovací karta)
- archiv se soubory šifrovaný heslem (např. programem 7-Zip)
- šifrování obsahu WWW (https://)
    - Facebook
    - gmail.com, email.cz, …
    - elektronické bankovnictví
- dálková správa informačních technologií – SSH
- aktualizace Windows Update

Obecně lze říci, že veškerá komunikace obsahující citlivé údaje by měla být chráněna proti odposlechu šifrováním.

Digitální podpis

Osvědčuje pravost určitého elektronického dokumentu.

Majitel vlastní takzvaný ***privátní klíč***. Tento klíč umožňuje dokument podepsat.

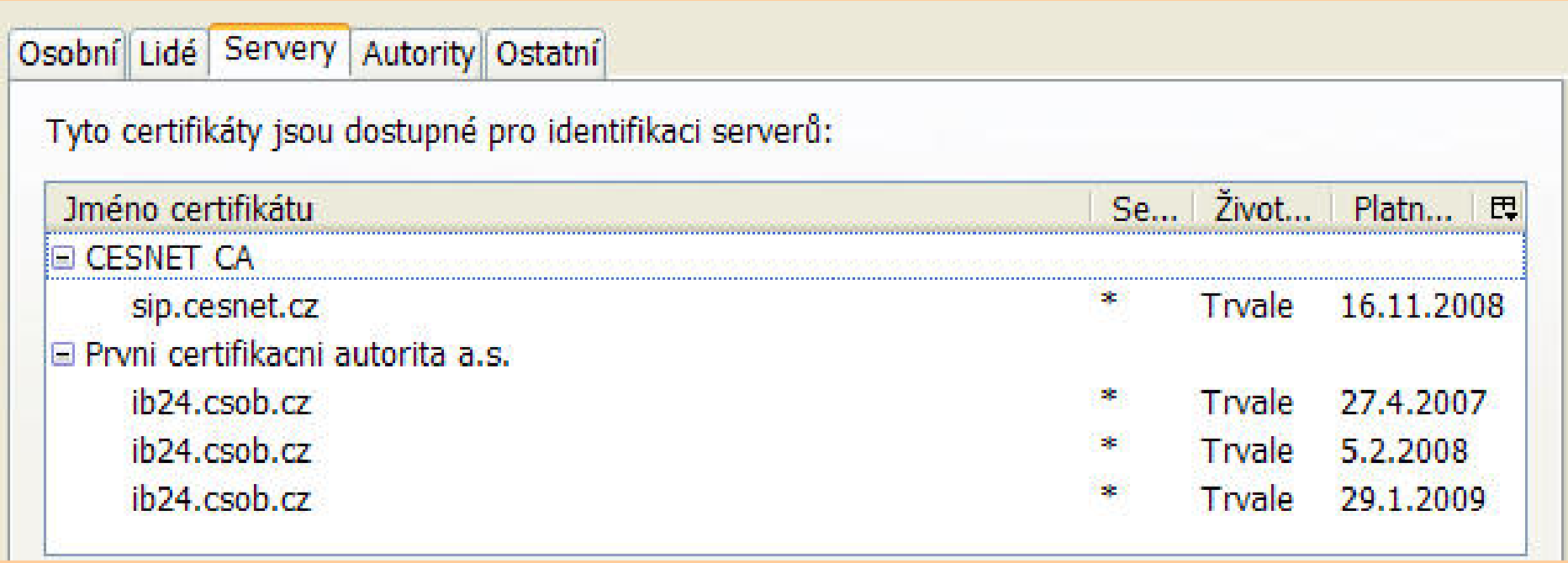
Ostatní mají k dispozici ***veřejný klíč – certifikát***. Nemohou dokument podepsat, ale mohou ověřit jeho pravost.

Obecně se podpis využívá například pro:

- sestavení spojení elektronické komunikace
- podpis libovolného dokumentu
- autorizaci bankovní transakce
- ...

Certifikáty

Např. Mozilla Firefox obsahuje řadu certifikátů. Nástroje – Možnosti – Rozšířené – Certifikáty.



Certifikát obsahuje například vydavatele, držitele, účel, platnost, ...

Tento certifikát byl ověřen pro následující použití:

Certifikát SSL serveru

Vydáno pro

Obecné jméno (CN)	ib24.csob.cz
Organizace (O)	CSOB a.s.
Jednotka organizace (OU)	Elektronicke bankovnictvi
Sériové číslo	11:F8:1F

Vydal

Obecné jméno (CN)	I.CA - Standard root certificate
Organizace (O)	Prvni certifikacni autorita a.s.
Jednotka organizace (OU)	<není součástí certifikátu>

Platnost

Vydáno dne	30.1.2008
Platný do	29.1.2009

Otisky

Otisk SHA1	12:23:1D:A9:2D:4C:50:7B:39:41:A3:C3:33:91:76:F3:6C:8A:D4:5D
Otisk MD5	5E:9B:28:E6:0D:61:28:48:AA:98:B2:BF:04:52:EF:58

Elektronické bankovnictví

- banka vydá certifikát pro zabezpečené připojení (https://)
- klient má jistotu že komunikuje s bankou – platnost dat je ověřena pomocí certifikátu
- klient je dále identifikován jménem a heslem
- pro zadání transakcí je navíc vždy požadováno doplňkové potvrzení – elektronický podpis klienta, potvrzující SMS, apod.

Bitcoin - BTC

- kryptografická měna, či spíše komodita
- sofistikované algoritmy umožňují vygenerovat jen omezený počet čísel (mincí), a tyto převádět mezi klienty sítě
- algoritmy používají komplexní kryptografii – symetrickou šifru, digitální podpisy, hashovací funkce
- Bitcoin by mohl být zruinován novým objevem v kryptografii

Budoucnost šifrování

Většina šifrovacích algoritmů je založena na matematické **domněnce**, že rozklad velkého čísla na prvočísla je i pro počítač extrémně složitý.

90 = 5 x 3 x 3 x 2 *jednoduché!*

37589137 = ??? *složité!*

Rozklad na prvočísla se zatím nepodařilo efektivně vyřešit žádným algoritmem. Naděje je vkládána do tzv. **kvantových počítačů**. Než o naději se ale jedná spíše o hrozbu, protože moderní civilizace je na šifrování závislá.

Závěr

- nikomu neříkej svá hesla a PINy
- používej různá hesla, zejména pro služby pochybného charakteru
- používej zabezpečené spojení, používej ověřené certifikáty
- od všech služeb chráněných heslem se při opuštění počítače odhlašuj

Cvičení

1. Jak staré jsou šifry?

2. Kde se používají šifry v současnosti?

3. K čemu slouží certifikát?

---

více než 200 let – komunikace, maily, bankovnictví, … – k ověření pravosti elektronického dokumentu