Úvod do kryptografie, digitální podpis

PV080

Vašek Matyáš

Ochrana komunikace/dat

- Fyzická ochrana
  - místnosti
  - kabely
  - diskety
  - ...
- Kryptografie – umění ochránit význam (informační hodnotu) dat i „na dálku“.
- Steganografie

Kde kryptografie pomáhá

- Důvěrnost dat
- Integrita dat
- Autenticita dat (integrita a ověření původu)
- Nepopiratelnost
- Autentizace a autorizace uživatelů/strojů
  - Dostupnost
  - Prokazatelná zodpovědnost
  - Řízení přístupu

...

Tři dimenze kryptografie

- Druhy použitých operací
  - Substituce
  - Permutace
  - …
- Druh a parametry klíčů
  - Symetrické = konvenční = sdílené
  - Asymetrické = veřejné & soukromé
  - Bez klíčů (hašovací funkce, RND)
- Způsob zpracování dat
  - Po blocích
  - V souvislém proudu

Co je hašování (hashování)

- “Otisk dat”
  - Malý a “jedinečný” reprezentant jakkoliv velkých dat

… It will be a blustery day above Scotland with gales and showery rain in the north-east. Elsewhere in Scotland the showers will be more scattered at first with a few sunny spells, but outbreaks of rain

- 01:A0:7D:2B:76:52:67:05
- EC:43:6F:B3:68:CE:20:E7
- Hašovací funkce
  - rychlost výpoštu, *jednosměrnost*
  - *bezkoliznost* – *slabá* (pro daný vstup) a *silná* (nalezení libovolné dvojice vstupů)
  - problémy funkcí MD5 (128 bit), SHA-0 a -1(160 bit)
  - dočasně doporučeny delší varianty SHA a výběr SHA-3

Co jsou klíče?

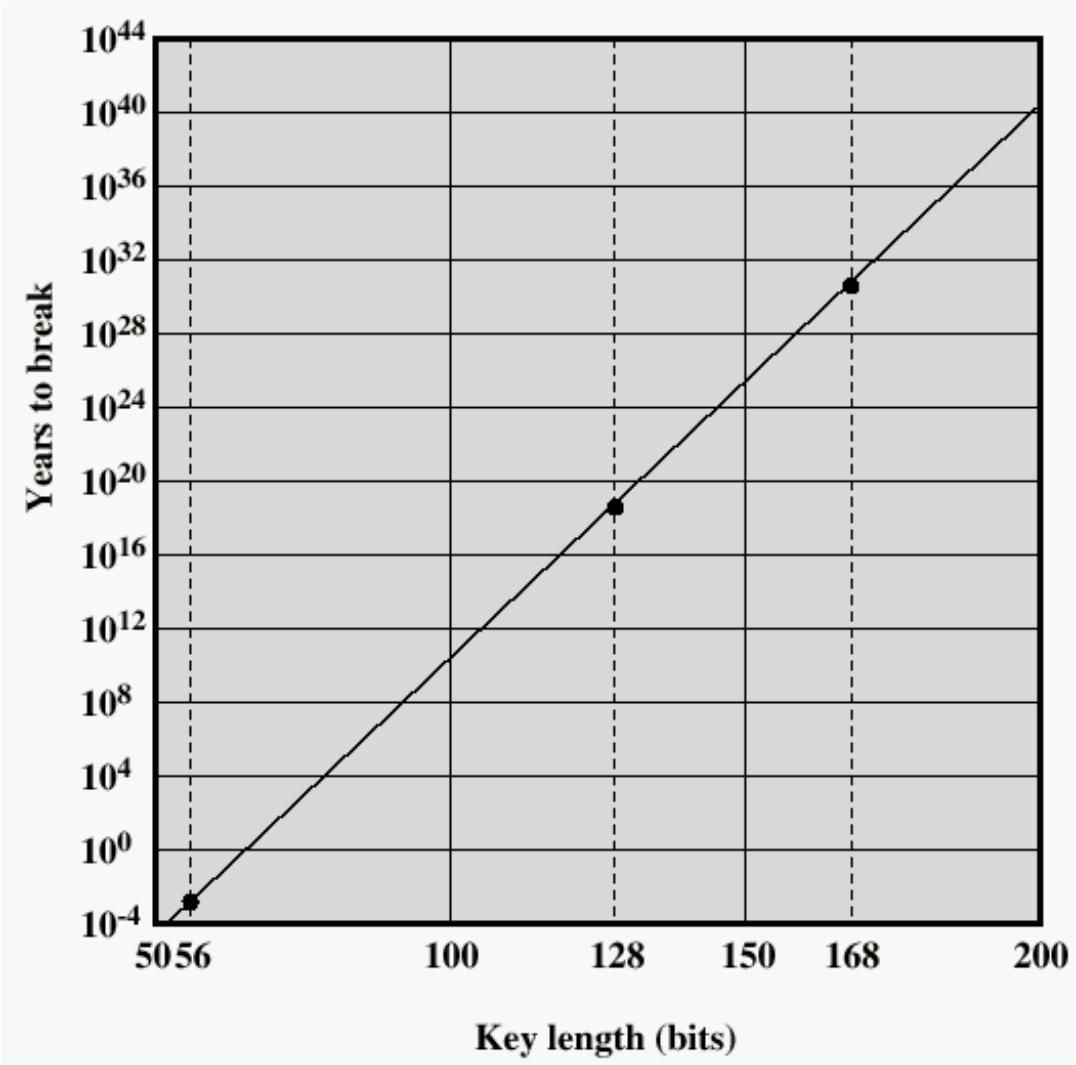
- Rozsáhlé řetězce bitů
  - náhodná čísla, prvočísla...
- Symetrická kryptografie
  - stejný klíč pro Alici i Boba
- Asymetrická kryptografie
  - privátní klíč (podpis, dešifrování)
  - veřejný klíč (ověření podpisu, šifrování)

...000100101010
01010100010100
10010101001001
00010111110101
01110101011100
10101100101000
10101001010010
10101011111101
10100110010001
00111010101010
110...

Čas potřebný pro prohledání prostoru možných klíčů (sym. krypt.)

Délka klíče (bit)	**Počet možných klíčů**	**Čas potřebný při 10^6 dešifrování/µs**
32	$2^{32} = 4.3 \times 10^9$	2.15 ms
56	$2^{56} = 7.2 \times 10^{16}$	10 hod
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} let
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} let

Čas potřebný k útoku hrubou silou (10^6 dešifrování/μs)



Čas potřebný k analýze NTLM hašů na anxurovi

n↓ c→	26 znaků	36 (alfan.)	62 (a/A,alfan)	95 (kláves.)
5	15 s	1,3 min	19,9 min	2,8 h
6	6,69 min	47,2 min	20,5 h	11 d
7	3 h	1,2 d	55 d	3,1 r
8	3,26 d	44 d	9,6 r	290 r
9	84,8 d	4,5 r	590 r	28000 r
10	7,1 r	180 r	42000 r	3000000 r

Kryptografie – Kerckhoffsův princip

- Algoritmus – postup – je všem znám a všemi kontrolován jako správný

- Klíč – tajná informace – musí být chráněna před nepovolanými osobami

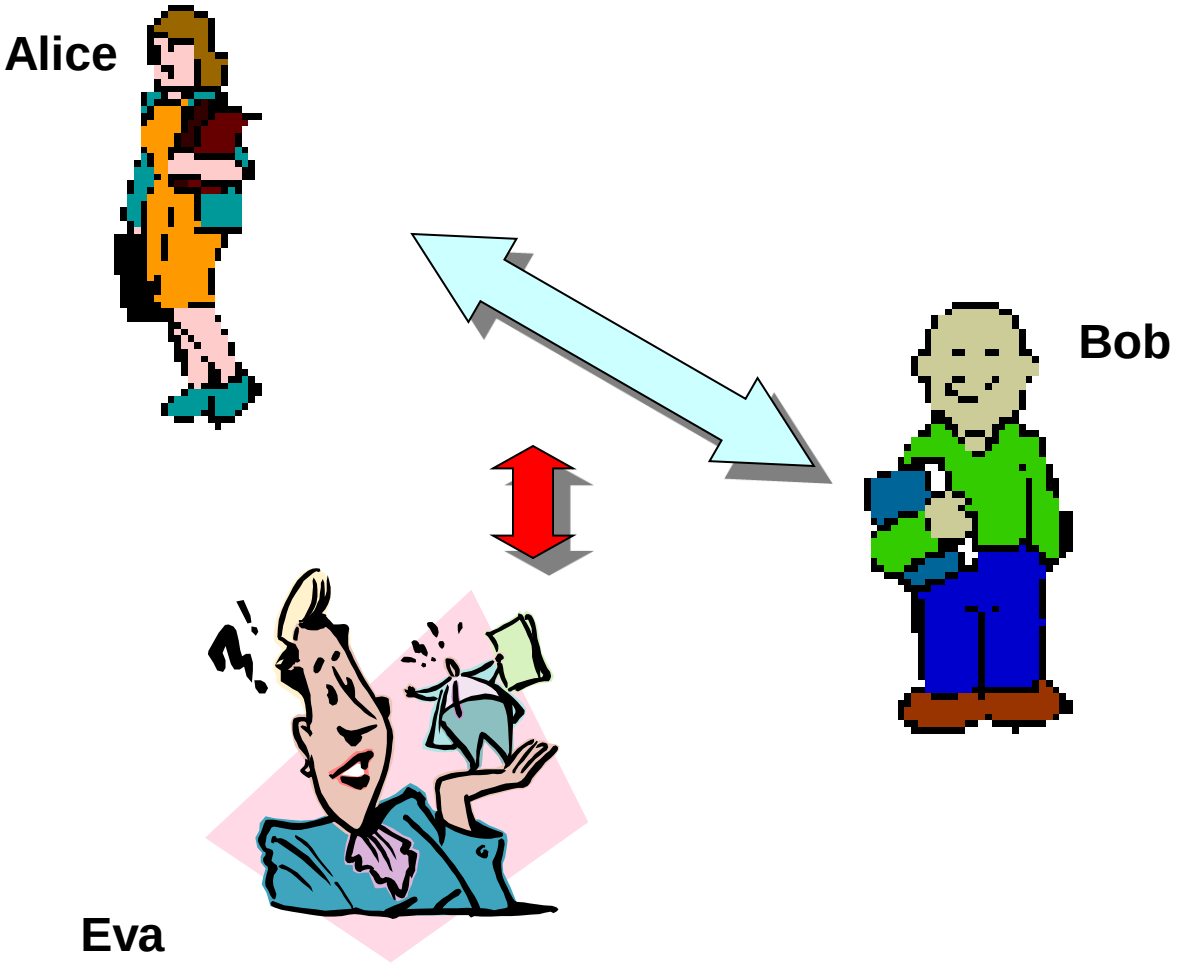
Doporučené délky klíčů

- Ošemetný, příliš zjednodušující, ukazatel
- Závisí na
  - kvalitě algoritmu,
  - výpočetních kapacitách dostupných útočníkovi,
  - a řadě dalších faktorů (dostupný kryptografický materiál...);
  - a většinou není nejslabším místem. ☺
- Asi 90b pro sym. alg. a všechny (?) útočníky
- Asi 1200b pro RSA (nejčastěji používaný asym. alg.) a (snad) všechny útočníky

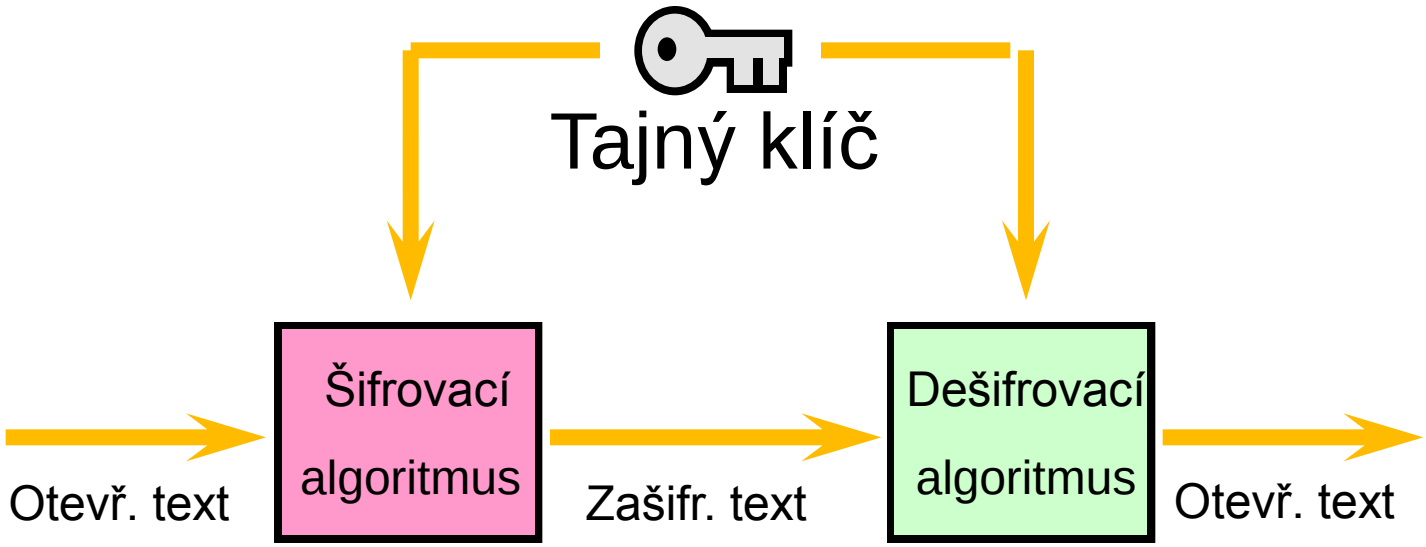
Proprietární algoritmy

- V extrémních situacích, kdy lze alespoň částečně věřit v možnost utajení algoritmu
  - IMHO, velmi diskutabilní závislost
- Ani tak by neměla bezpečnost (ve smyslu robustnosti vůči útoku hroubou silou) klíče být rozhodně zanedbána
  - Často využití principů (znalostí o) veřejně známých šifer
- Základní dilema – otevřená/veřejná verifikace vs. přístupnost znalostí o (ne)kvalitě

Obvyklá označení činitelů

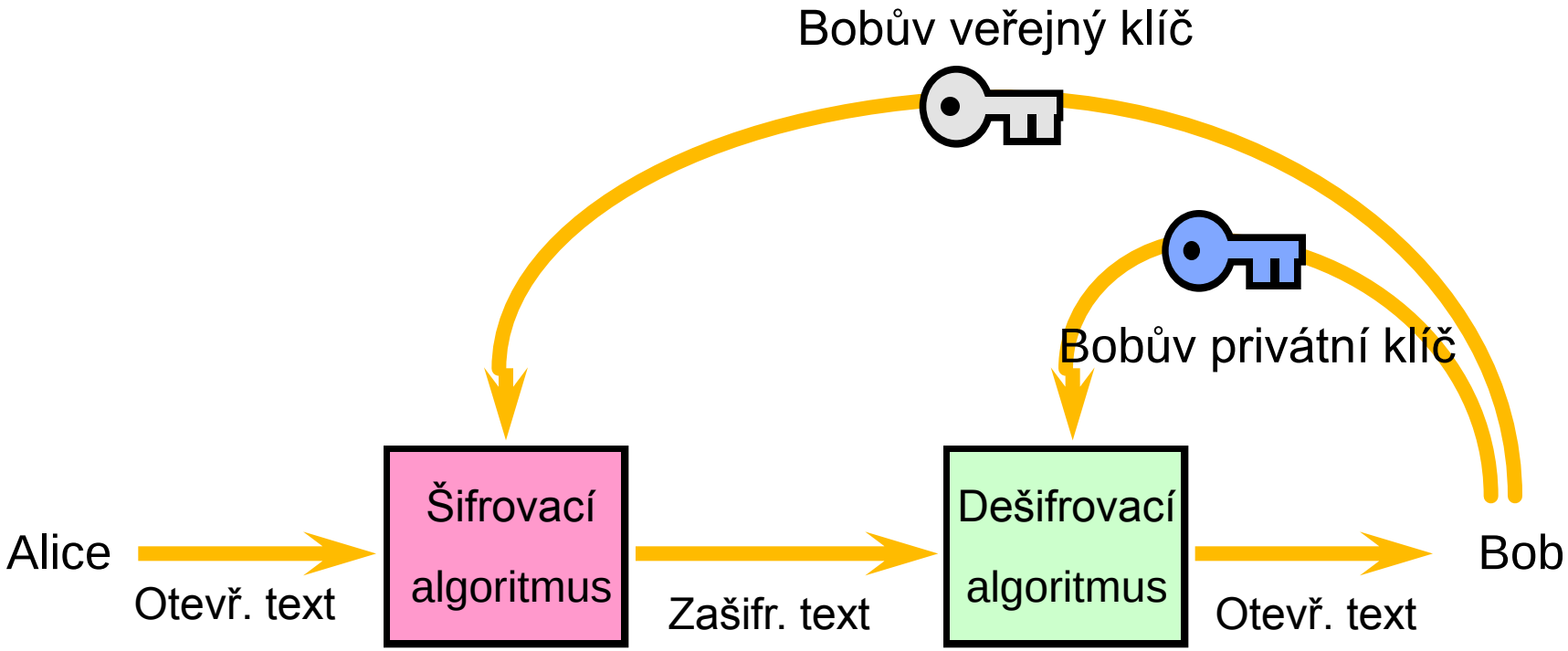


Zjednodušený model konvenčního šifrování



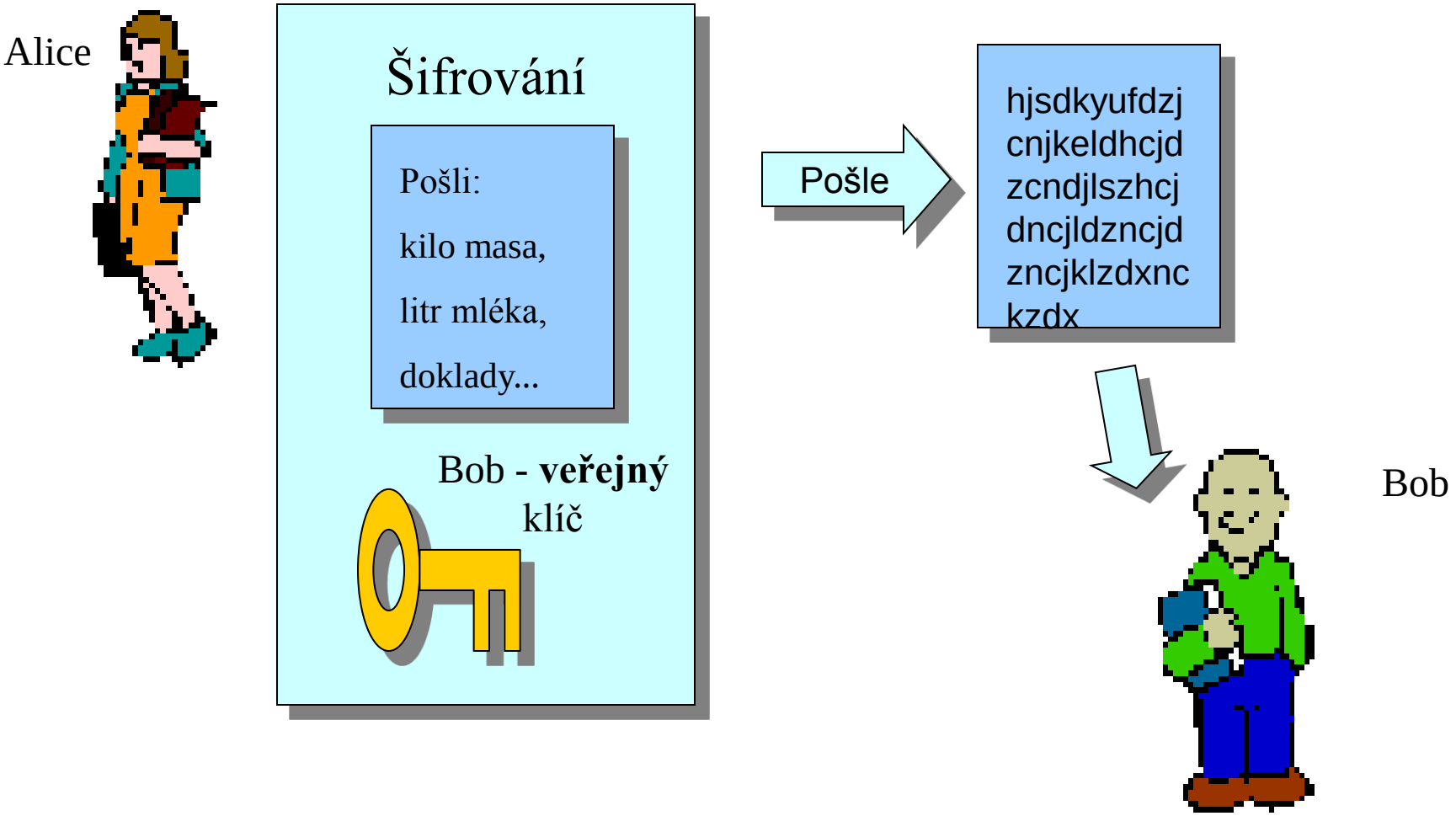
Převzato z: *Network and Internetwork Security* (Stallings)

Zjednodušený model šifrování veřejným klíčem

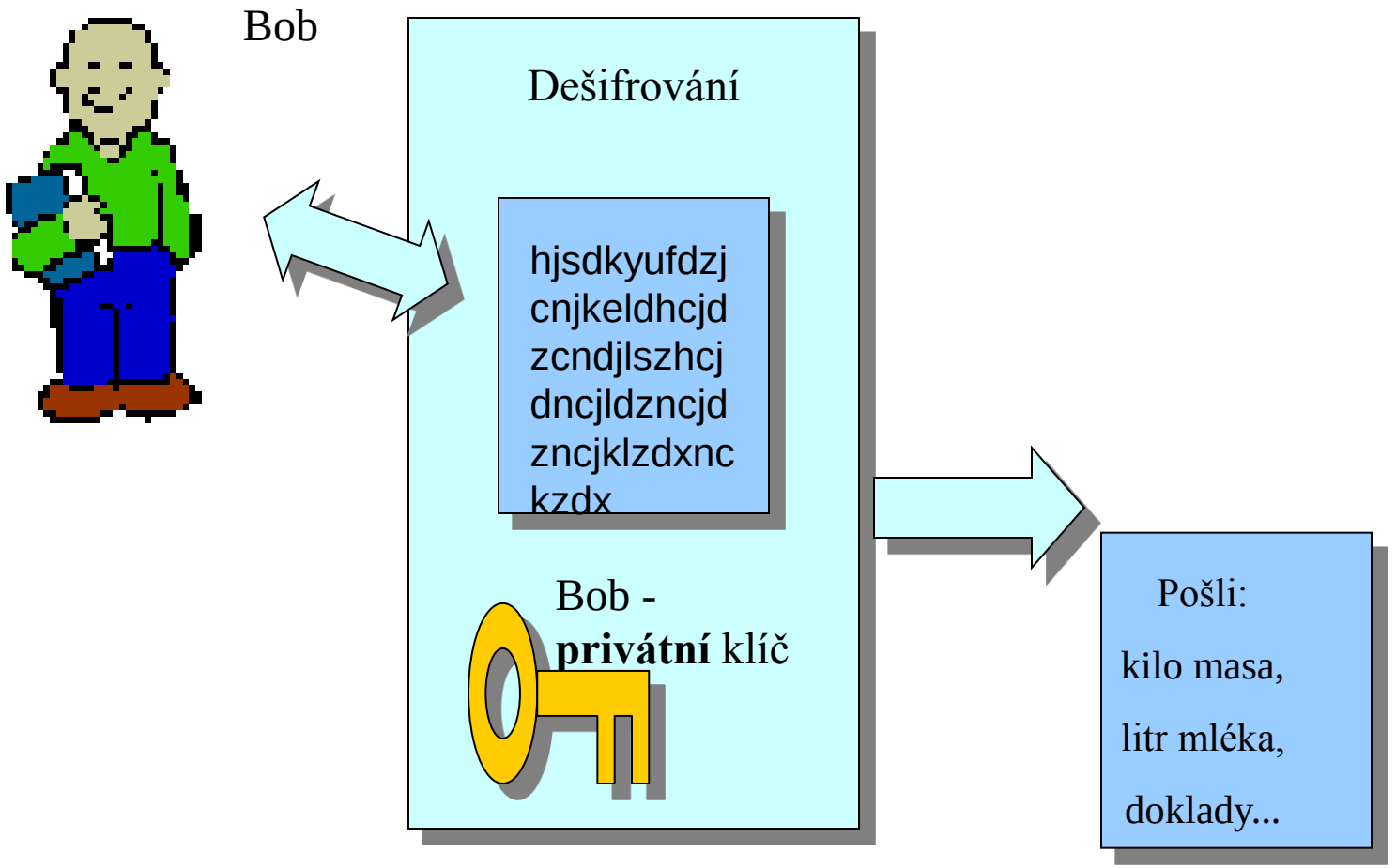


Převzato z: *Network and Internetwork Security* (Stallings)

Šifrování veřejným klíčem



Dešifrování zprávy od Alice



Realita – Hybridní kryptosystémy

- Problémy
  - Asymetrické algoritmy jsou pomalejší (pro srovnatelnou úroveň bezpečnosti)
  - Symetrické alg. obtížněji využitelné v situacích vyžadujících autentizaci (většina situací ☺)
- Řešení – vzájemná kombinace
  - Šifrování: RNG klíče pro symetrickou šifru, tou+tím zašifruji data, klíč pak veřejným klíčem adresáta
  - Podpis: vytvořím haš dat, až ten podepíši svým soukromým klíčem

Sen Velkého bratra

• Mnohé vlády chtějí:

1) Mít jistotu, že používání kryptografických systémů nesníží schopnost dopadnout nežádoucí osoby a skupiny osob (*kdo je nežádoucí???*).

DEPOZITOVAT POUŽÍVANÉ KLÍČE (*ale i 2)*)

2) Zajistit, aby používání kryptografických systémů nepůsobilo proti národním zájmům dané země. (*co jsou a kdo definuje národní zájmy?*)

KONTROLOVAT EXPORT KRYPTOGRAFIE (*ale i 1)*)

• Přímý dopad na *informační soukromí*

– Firmy mohou v určité míře přemístit centrum svých aktivit, ale co občan?

Depozitování klíčů (key escrow)

- Zástěrka(?): boj proti zločinu na vlastním území
- Aspekty:
  - sledování komunikace mezi "problémovými skupinami" (extrémisté, přátelé a rodiny známých zločinců, političtí oponenti…)
  - dle studií britské vlády je jen 2-5 % případů neoprávněného použití informací držených vládou způsobeno "zvenčí" (hackery atd.)
- Problém: fyzické sledování i odposlech telefonů v analogových sítích má technické a finanční limity (vládně-společenský konsensus), filtrování digitální komunikace je relativně jednoduché a levné

Exportní kontroly

- Zástěrka(?): boj proti mezinárodním mafiím, zemím podporujícím terorismus atd.

- Problémy
  - aktivity zpravodajských služeb v ISP (především US),
  - vybudování satelitních sítí bez dostatečné ochrany je „výhrou“ na dalších 15-20 let pro vlády, které mají informační výhody

- Aspekty
  - pomoc vlád firmám - průmyslová špionáž (Francie, Japonsko, Rusko…)
  - sledování komunikace v cizích zemích

Digitální podpis

- Jedna ze stěžejních aplikačních oblastí kryptografie

- Využití asymetrické kryptografie k podpisu zjištěno až po letech znalosti principů šifrování (dle dokumentů britské GCHQ)

Podpis v digitální formě - požadavky

- Musí zajistit autentizaci podepsaných dat.
  - Integrita
  - Prokázání původu dat
- Měl by podporovat ověření data/času podpisu.
- Měl by být ověřitelný i třetími stranami.
- Měl by podporovat mechanismy nepopiratelnosti

Co je digitální podpis?

Agáta

Podpis

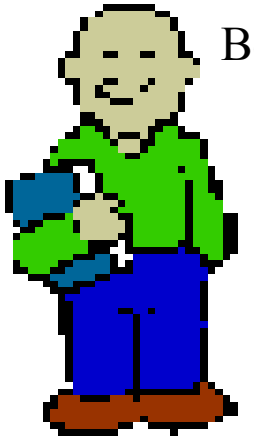
Milý Bořivoji,

o ty doklady skutečně žádám já - Agáta

Agáta - **privátní** klíč

Certifikát - Agátin veřejný klíč

Bořivoj



Digitální podpis

- Nezajišťuje důvěrnost (šifrování)
- Nejznámější algoritmy – RSA, DSA
- Obecně existují algoritmy
  - s obnovou zprávy (podpis „obsahuje“ podepisovaná data),
  - **bez obnovy zprávy (podpis „neobsahuje“ data)**
- Asym. algoritmy jsou relativně pomalé, proto se podepisuje haš – „otisk dat“
- Fáze postupu:
  - Vytvoření a registrace klíčů (certifikát)
  - Vlastní podepsání
    - Dokument $\Rightarrow$ haš $\Rightarrow$ podpis
  - Ověření podpisu

Asymetrická kryptografie

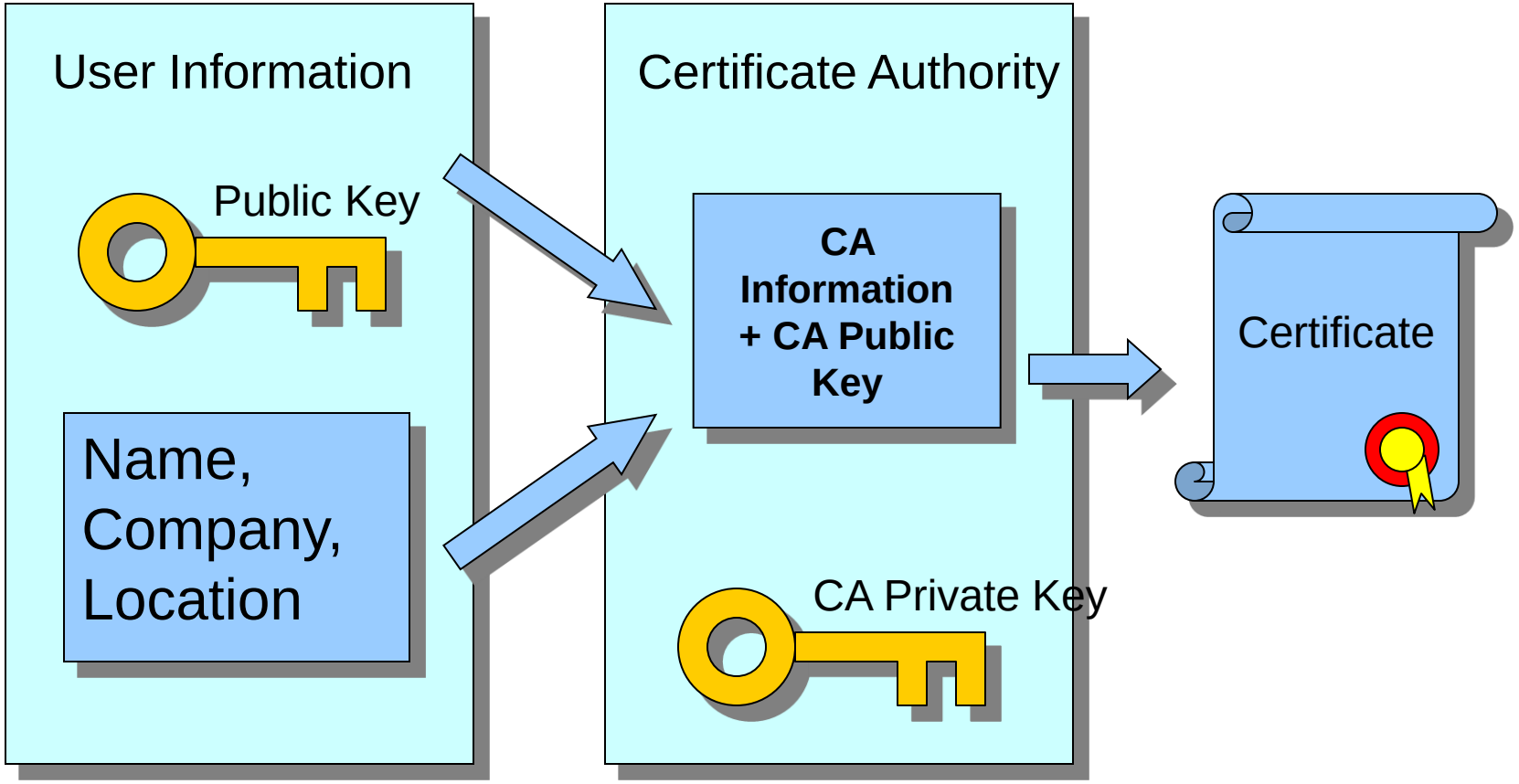
- Veřejné klíče
  - Šifrování
  - Ověření podpisu
- Soukromé klíče
  - Dešifrování
  - Tvorba podpisu

- Nemusí jít o stejný pár klíčů pro oba druhy operací!

K použití veřejných klíčů

- Digitální podpis – spojí nerozdělitelně klíč s označením entity – certifikát veřejného klíče.
- Spojení veřejného klíče s označením entity je kritické
  - *S kým komunikuji?*
- Digitální podpis děláme vždy přes přístroj!!!

Co je certifikát?



(X.509v3) Certifikát

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate       TBSCertificate,
     signatureAlgorithm   AlgorithmIdentifier,
     signature            BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
     version         [0]  Version DEFAULT v1,
     serialNumber         CertificateSerialNumber,
     signature            AlgorithmIdentifier,
     issuer               Name,
     validity             Validity,     -- notBefore,
notAfter
     subject              Name,
     subjectPublicKeyInfo SubjectPublicKeyInfo,  -- algID,
bits
     issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
     subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
     extensions      [3]  Extensions OPTIONAL
                -- sequence of: extnID, crit, value }
```

Certifikační autorita

- Potvrdí platnost veřejného klíče
  - Patří někomu? Komu?
  - Způsob prokázání identity.
  - Má daný člověk odpovídající soukromý klíč?
  - Je platnost klíče omezena?
  - Je poskytnuto ručení? Do jaké výše?

  ...
- Certifikační politika

Certifikační autorita – struktura

- „Certifikační autorita“ je rozdělena do více částí
  - Certifikační autorita – vydává certifikáty na základě požadavků od (RA)
  - Registrační autorita – ověřuje identitu žadatele, posílá požadavek na vystavení certifikátu
  - Revokační autorita – požadavky vlastníků certifikátů na revokaci

Akreditované cert. autority v ČR

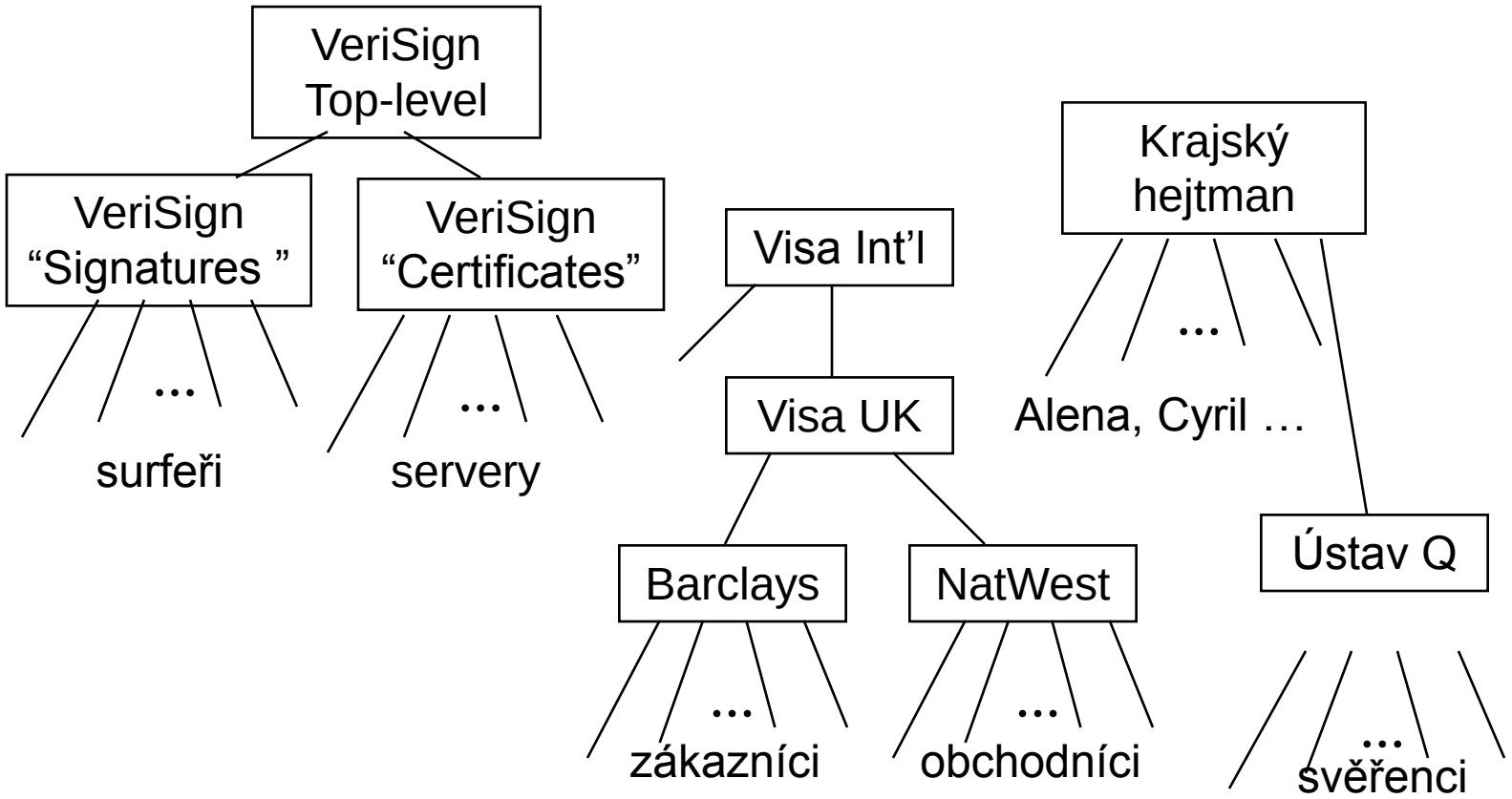
- První certifikační autorita a.s. (ICA) – akreditovaná od 18.3.2002 – http://www.ica.cz/
- Česká pošta s.p. – akreditovaná od 3.8.2005 – https://qca.postsignum.cz/
- eIdentity a.s. – akreditovaná od září 2005 – http://www.eidentity.cz/

Kontrola veřejného klíče

- *Konzervativně*: klíč/certifikát je **neplatný** pokud nejsme spolehlivě informováni o opaku.
  - Čerstvé potvrzení.
  - Potvrzení od důvěryhodné strany.
  - Použitelné v případě sporu.

- *Liberálně*: klíč/certifikát je **platný** pokud nejsme spolehlivě informováni o opaku.
  - Seznam revokovaných cerifikátů (CRL - Certificate Revocation List).

Hierarchie certifikačních autorit



A co privátní klíč...

…když jej ztratíte?

…když jej někdo zjistí?

…když změníte zaměstnavatele?

…když změníte jméno?

…když zaměstnavatel chce dokumenty, které jste zašifrovali?

…když si vaše data žádá soud?

…když...

Aspekt času

- Návaznost operací, např.
  - Vytvoření podpisu
  - Vyzrazení tajného klíče
  - Ověření podpisu
- Spolehlivé označování času (časové razítko) – angl. timestamping
- Kritický parametr!!!

Problém nepopiratelnosti

- Podpis – nepopiratelnost
- Nepopiratelnost původu
  - V zásadě stačí podpis
- Nepopiratelnost přijetí
  - Nerovnoprávnost vztahu odesilatel-příjemce
- Vhodné ověření/potvrzení (čas!) třetí stranou

Český zákon o e-podpisu (227/2000)

- e-podpis: „obyčejný“ a zaručený, značka(!)
- Kvalifikovaný certifikát!
- Podepisuje fyzická osoba!
- Úřad pro dohled nad CA – Min. inf. (dříve odbor ÚOOÚ)

Elektronický podpis

- Zákon o elektronickém podpisu č. 227/2000 Sb.
  - změněn zákony č. 226/2002, 517/2002, 440/2004, 501/2004, 635/2004, 444/2005, 230/2006, 110/2007, 124/2008, 190/2009, 223/2009, 227/2009, 281/2009, 101/2010, 424/2010 a 167/2012 Sb.
- *„Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě“*
- Elektronickým podpisem tak může být i pouhé jméno napsané na klávesnici.

Zaručený elektronický podpis

- Je jednoznačně spojen s podepisující osobou (jen fyzická osoba!);
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě;
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou;
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.

Elektronický podpis vs. značka

- Elektronický podpis
  - podepisující osoba je fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby;
  - pro ověření podpisu je vydáván certifikát (veřejného klíče).
- Elektronická značka
  - označující osobou fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou;
  - pro ověření podpisu je vydáván systémový certifikát (veřejného klíče).
- Technologicky jde o totéž
  - Jen úroveň ochrany soukromého klíče je jiná.

Použití podpisu

- Autentizace dat (aplikace tajných dat – soukromého klíče)
- Autentizace počítačů/tokenů (schopnost aplikovat tajná data)
  - Výzva-odpověď
- Autentizace osob (schopnost spustit aplikaci tajných dat na počítači/tokenu).

Prosba – terminologie

- Nekryptujeme ani neenkryptujeme – **šifrujeme**
- Nešifrujeme soukromým klíčem – **podepisujeme**
- Nerozšifrováváme – **dešifrujeme**
- Neautentikujeme, neautentifikujeme a neidentizujeme – **autentizujeme** a **identifikujeme**

- Haš, hash – oba OK
- Čistý text, vstupní text, otevřený text – OK