Bezpečnost v informačních technologiích

Jaromír Plhák
xplhak@fi.muni.cz

Základní pojmy (1)

- Aktiva
  - Něco co mám a má to pro mne hodnotu
- Škoda
  - Snížení hodnoty aktiva
- Hrozba
  - Existuje pokud je systém zranitelný
- Zranitelnost
  - Zranitelné místo + potenciální útočník
- Útok
  - Útok může způsobit škodu
  - Je realizací hrozby

Základní pojmy (2)

- Důvěrnost dat (Confidentiality)
  - Informace jsou srozumitelné / přístupné / sdělené jen těm, kdo jsou k tomu oprávněni
- Integrita dat (Integrity)
  - Informace jsou správné, úplné, nebyly neautorizovaně změněny
- Dostupnost dat (Availability)
  - Informace / služby jsou autorizovaným uživatelům k dispozici kdykoli to potřebují resp. kdykoli je určeno, že mají být k dispozici

Základní pojmy (3)

- Autentičnost (Authenticity)
  - Integrita + zajištění původu (zpráv, dat, ..)
- Odpovědnost (Accountability)
  - Kdo za co odpovídá
- Nepopiratelnost (Nonrepudiation)
  - Nemožnost popřít deklarovaný původ (např. zprávy)

Základní pojmy (4)

- Autentizace
  - Proces ověření (a tím i ustavení) identity (s požadovanou mírou záruky)
- Autorizace
  - Udělení určitých práv a určení povolených aktivit
- Identifikace
  - Rozpoznání určité entity (systémem) v dané množině entit

Základní pojmy (5)

- Kryptografie
  - Ochrana významu (informační hodnoty) dat i „na dálku“
- Kryptoanalýza
  - Zjišťování slabin kryptografických algoritmů a parametrů
- Kryptologie
  - Kryptografie & kryptoanalýza
- Steganografie
  - Utajení samotné existence dat
- Vodotisk (watermarking)
  - Překryv se steganografií, metody vložení (ochranných) informací do dat

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

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

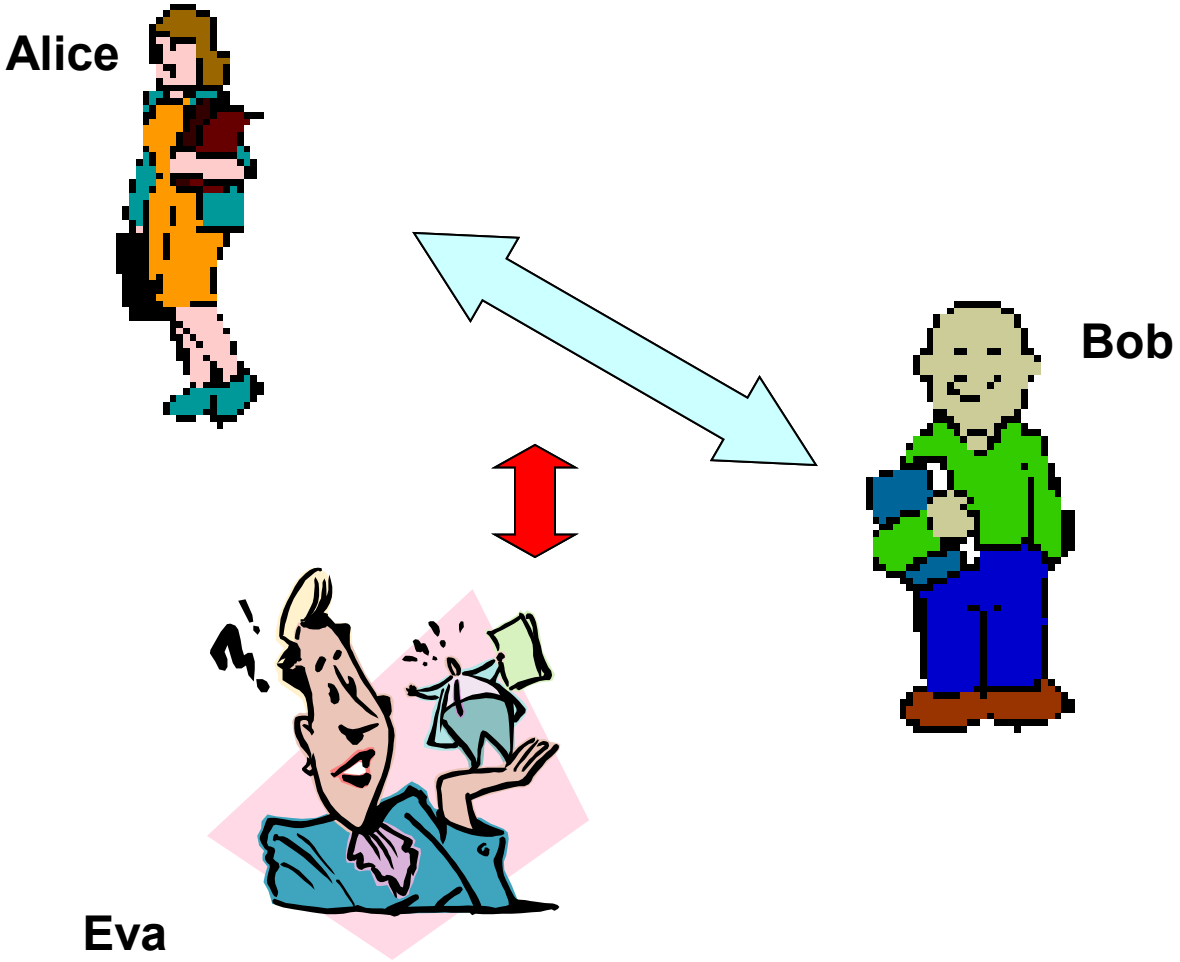
Kerckhoffsův princip

- Algoritmus – postup – je všem znám a všemi ověřitelný (jako bezpečný)
- Klíč – tajná informace – musí být chráněna před nepovolanými osobami

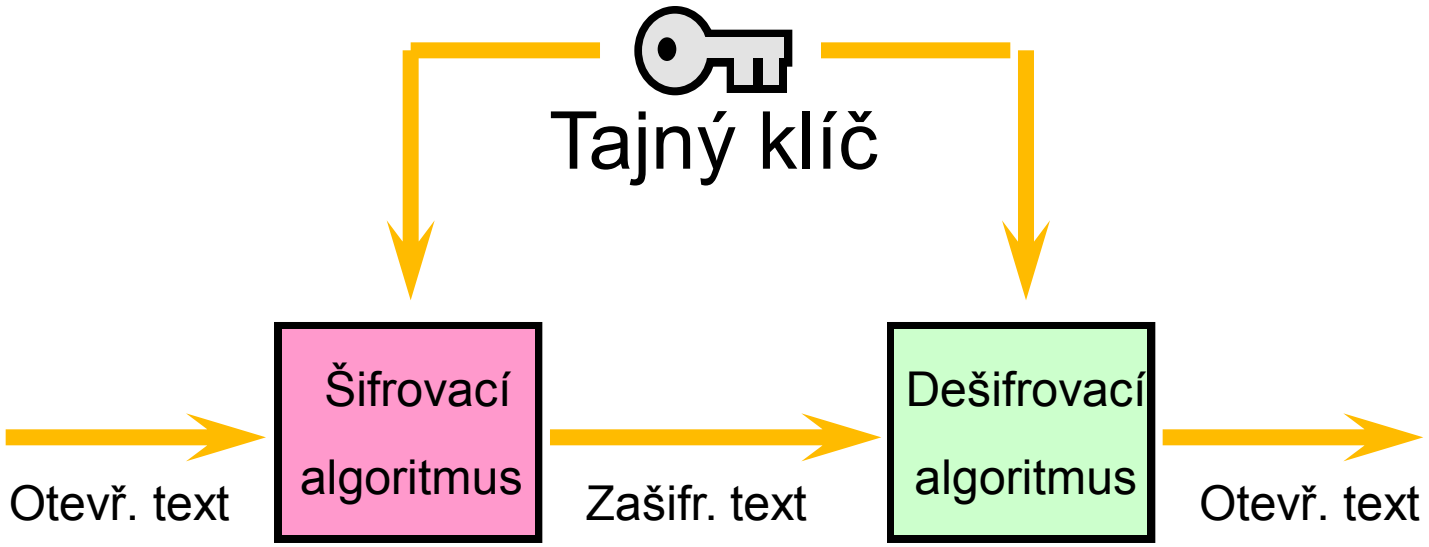
Co je hašování (hashování)

- “Otisk dat”
  - Malý a jedinečný reprezentant jakkoliv velkých dat
  - 01:A0:7D:2B:76:52:67:05:EC:43:6F:B3:68:CE:20:E7
- Hašovací funkce
  - Jednosměrnost, bezkoliznost
  - Dnes považovány za bezpečné – SHA-256 a verze vyšší
  - Nedostatečně bezpečné – SHA-1 (160 bit), MD5 (128 bit)

Obvyklé označení činitelů

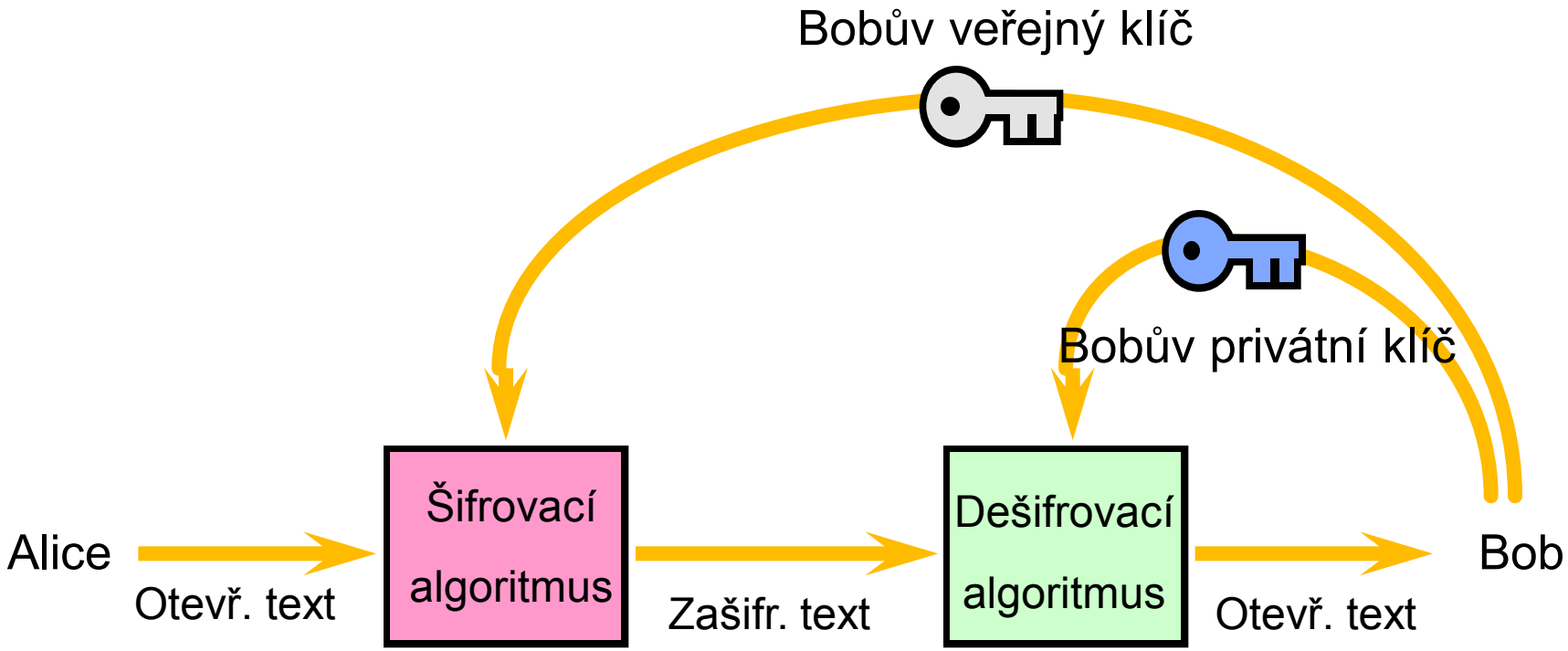


Zjednodušený model konvenčního šifrování



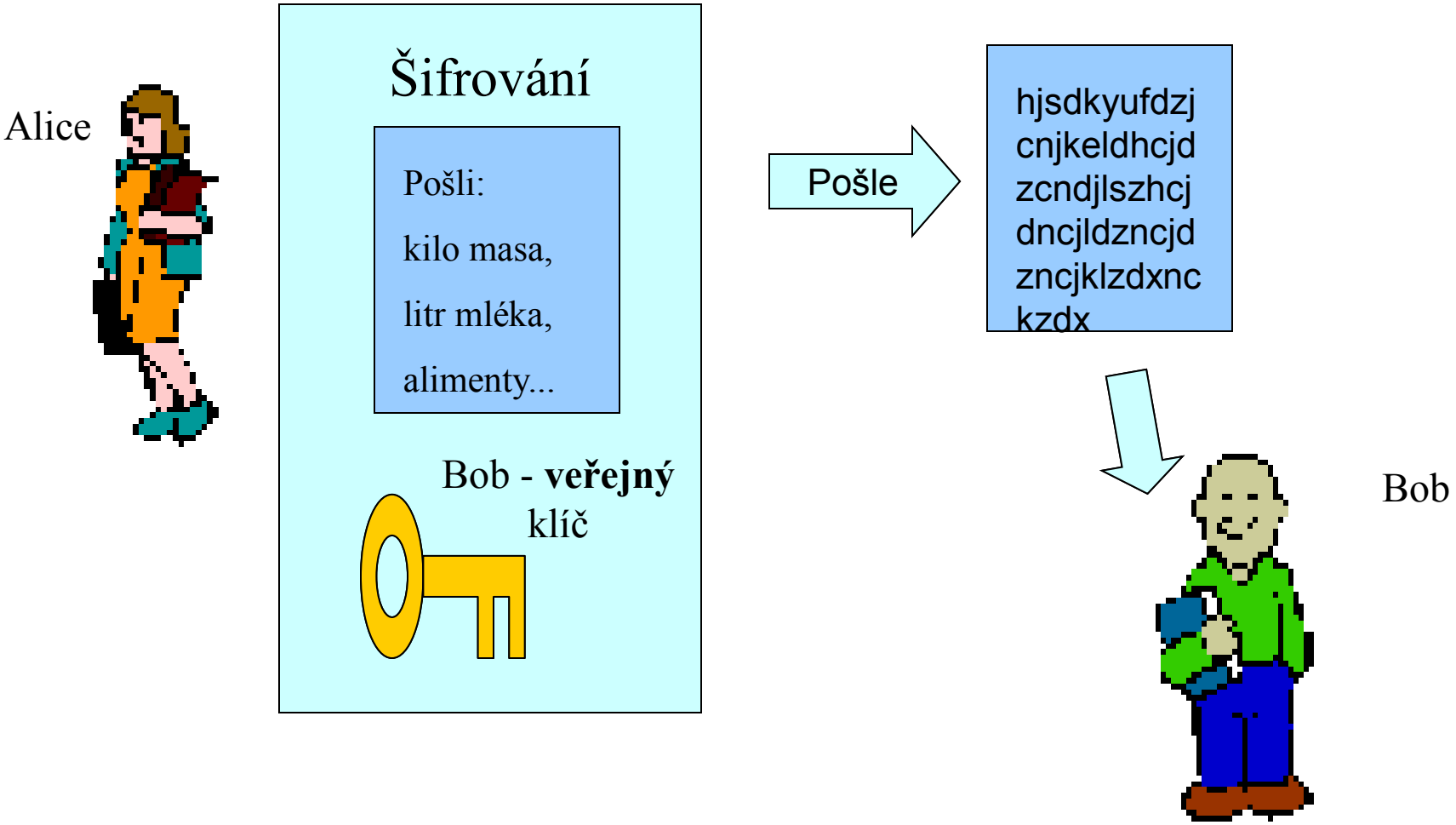
Převzato z: *Network and Internetwork Security* (Stallings)

Zjednodušený model šifrování veřejným klíčem

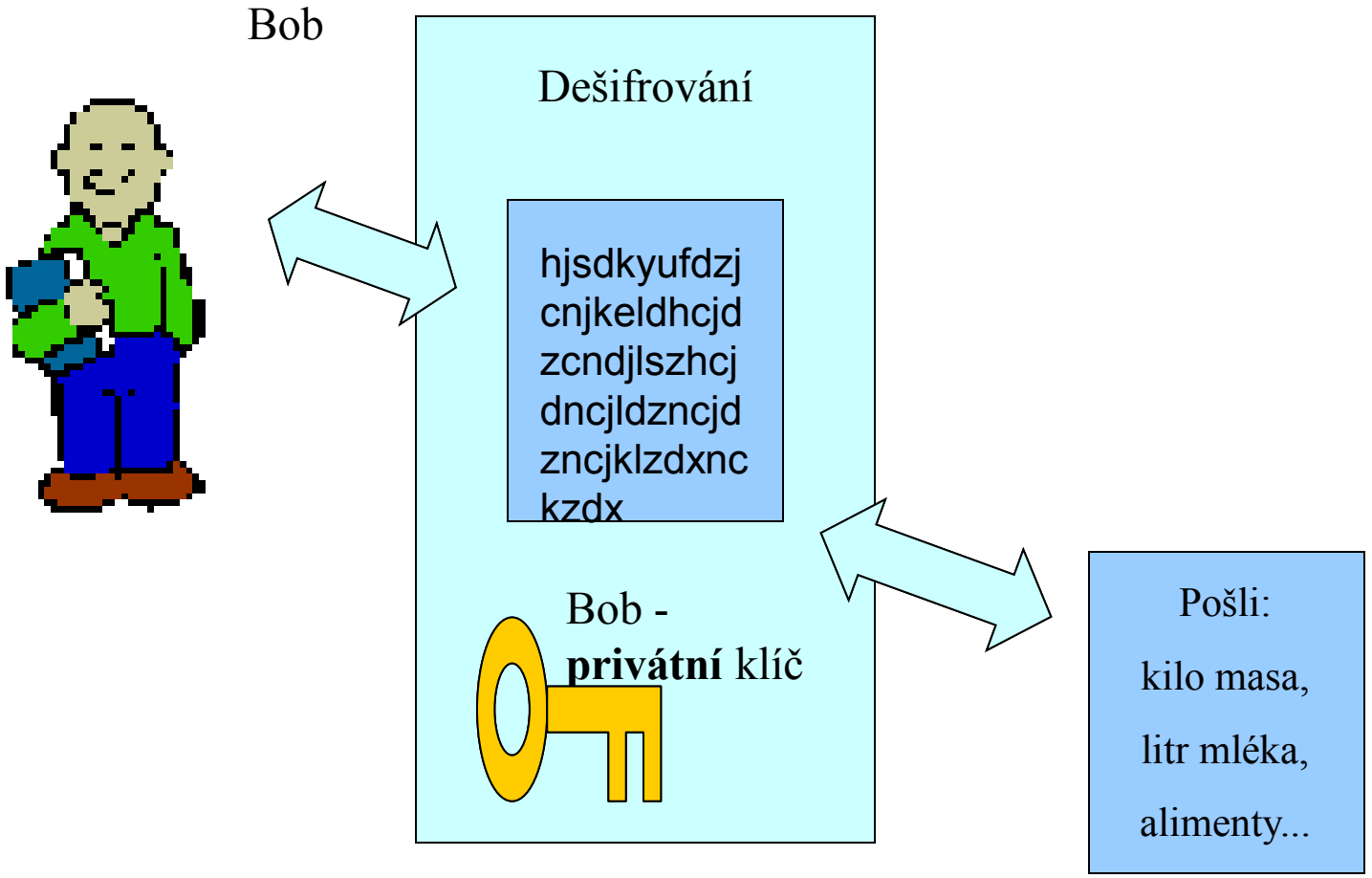


Převzato z: *Network and Internetwork Security* (Stallings)

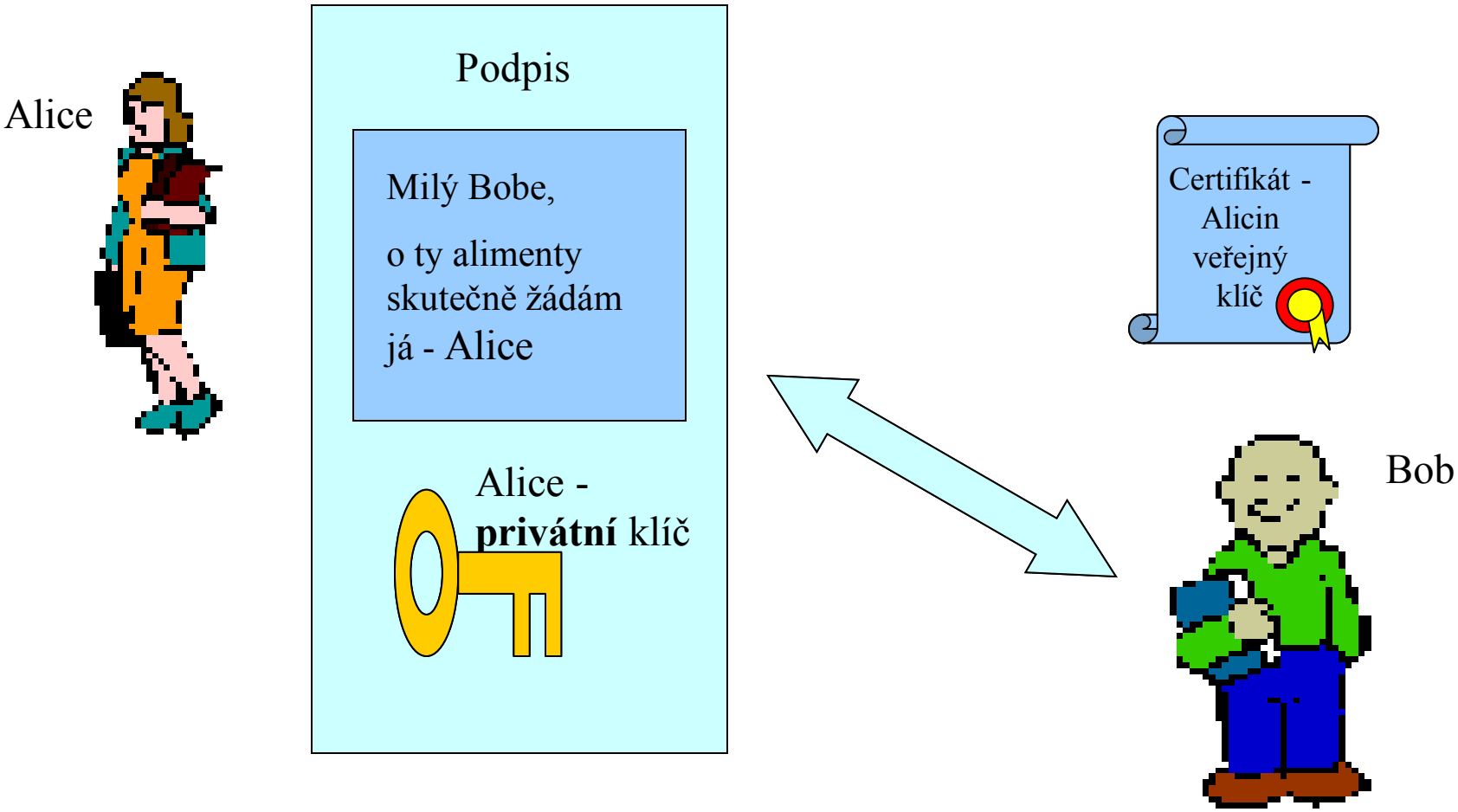
Šifrování veřejným klíčem

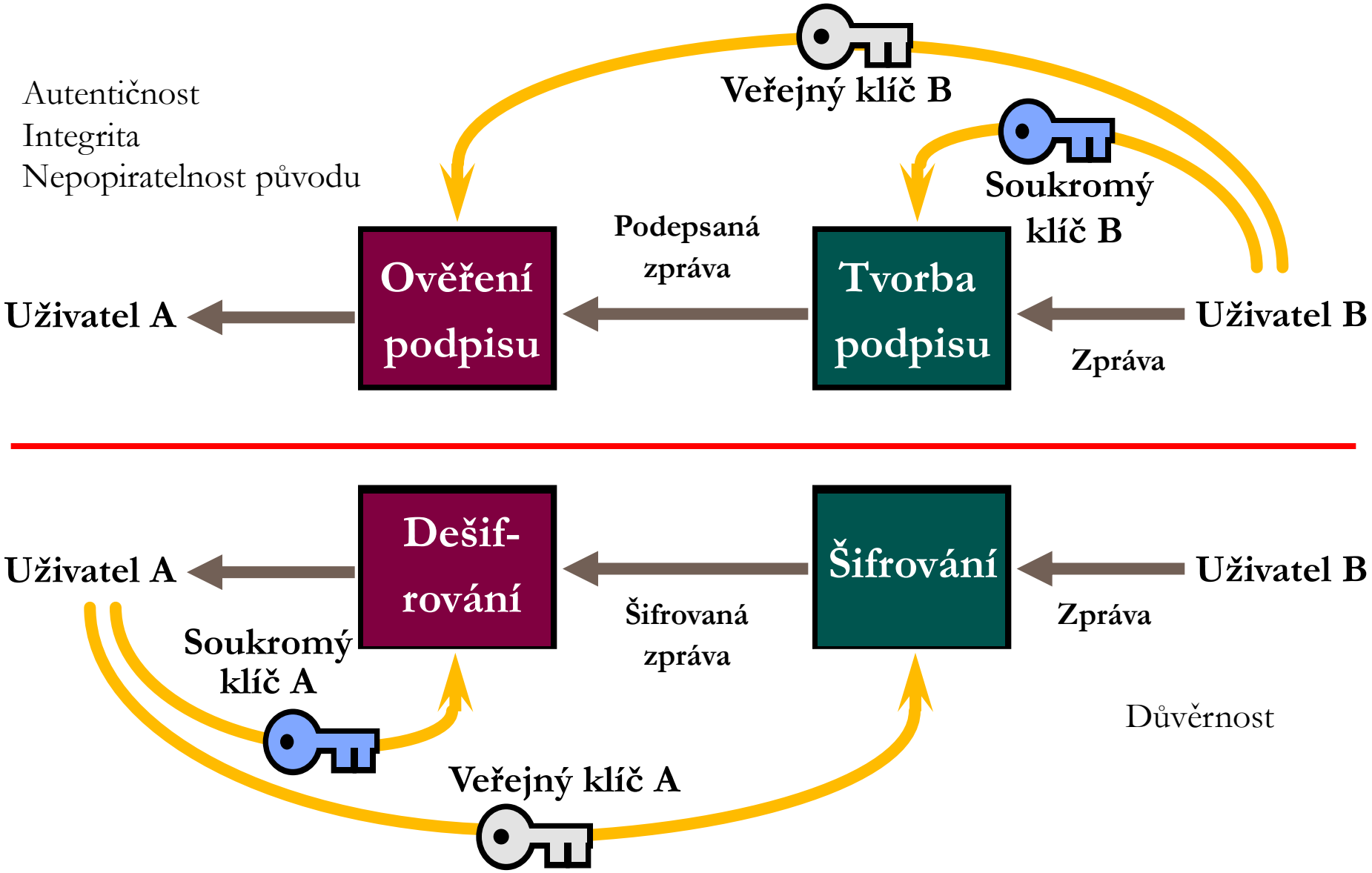


Dešifrování zprávy od Alice



Co je digitální podpis?




Autentičnost
Integrita
Nepopiratelnost původu
Veřejný klíč B
Soukromý klíč B
Podepsaná zpráva
Ověření podpisu
Tvorba podpisu
Uživatel A
Uživatel B
Zpráva
Dešif-rování
Šifrování
Šifrovaná zpráva
Soukromý klíč A
Veřejný klíč A
Důvěrnost

Certifikát

- **Certifikát** – veřejný klíč uživatele podepsaný soukromým klíčem důvěryhodné třetí strany
- Certifikát spojuje jméno držitele páru soukromého a veřejného klíče s tímto veřejným klíčem a potvrzuje tak identitu osoby
- Poskytuje záruku že identita spojená s vlastníkem daného veřejného klíče není podvržená
- Případně také představuje doklad o tom, že totožnost držitele veřejného klíče byla ověřena

Elektronický podpis

- Zákon o elektronickém podpisu č. 227/2000 Sb. (změněn několika novelizacemi)
- *„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

Není podpis jako podpis (1)

- Elektronický podpis
  - Téměř cokoliv
- Zaručený elektronický podpis
  - V podstatě digitální podpis
- Zaručený elektronický podpis založený na kvalifikovaném certifikátu
  - Digitální podpis, certifikát veřejného klíče vydán kvalifikovanou CA (splnila podmínky zákona a oznamovací povinnost)

Není podpis jako podpis (2)

- Zaručený elektronický podpis založený na kvalifikovaném certifikátu od akreditovaného poskytovatele certifikačních služeb
  - Také nazýván jako „uznávaný podpis“
  - Digitální podpis, certifikát veřejného klíče vydán akreditovanou CA (splnila podmínky zákona a získala akreditaci)
  - Jen tento podpis je uznáván v komunikaci se státní správou a samosprávou
  - V ČR dnes tři akreditované CA (I.CA, PostSignum a eIdentity)

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

Elektronická značka

- Jednoznačně spojena s označující osobou (i právnickou osobou nebo i org. složkou státu) a umožňuje její identifikaci prostřednictvím kvalifikovaného systémového certifikátu
- Byla vytvořena a připojena k datové zprávě pomocí prostředku pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou
- Je k datové zprávě, ke které se vztahuje, připojena takovým způsobem, že je možné zjistit jakoukoli 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)

Elektronický podpis vs. značka (1)

- Rozdíl je pouze procedurální
  - „Datová zpráva je podepsána, pokud je opatřena elektronickým podpisem. Pokud se neprokáže opak, má se za to, že se podepisující osoba před podepsáním datové zprávy s jejím obsahem seznámila.“ (§3 odst. 1)
    „Použití zaručeného elektronického podpisu založeného na kvalifikovaném certifikátu a vytvořeného pomocí prostředku pro bezpečné vytváření podpisu umožňuje ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu.“ (§3 odst. 2)

Elektronický podpis vs. značka (2)

- „Použití elektronické značky založené na kvalifikovaném systémovém certifikátu a vytvořené pomocí prostředku pro vytváření elektronických značek umožňuje ověřit, že datovou zprávu označila touto elektronickou značkou označující osoba.“ (§3a odst. 1)
  „Pokud označující osoba označila datovou zprávu, má se za to, že tak učinila automatizovaně bez přímého ověření obsahu datové zprávy a vyjádřila tím svou vůli. “ (§3a odst. 2)

Elektronický podpis a značka

- Technologicky jde o totéž
  - Jen automatizace použití a správa soukromého klíče je jiná
  - Viz §17 a §17a zákona
- Podle vyhlášky č. 378/2006 Sb. se jedná o klasické algoritmy digitálního podpisu
  - ETSI technical specifications
  - ETSI technical reports

Digitální podpis – algoritmy

- První algoritmy asymetrické kryptografie na začátku 70. let 20. století
  - Britská tajná služba GCHQ (Clifford Cocks)
  - Veřejné oznámení až koncem 20. století (1997)
  - Aplikaci algoritmů pro autentizaci – podpis – „objevila“ později až akademická komunita u svých veřejných algoritmů
- První veřejné algoritmy koncem 70. let 20. století (W. Diffie a M. Hellman ovlivněni prací R. Mercla)
- Nejznámější algoritmus RSA (Rivest, Shamir, Adelman) publikován v roce 1977, patentován v roce 1983 (v současné době patent již vypršel)

Digital Signature Algorithm

- V roce 1994 proběhl v USA výběr Digital Signature Standard (DSS) – vyhrál DSA (Digital Signature Algorithm) modifikovaný algoritmus ElGamal, založený na diskrétním logaritmu v Z_p
- Další algoritmy, mj. založeny i na eliptických křivkách
- NIST FIPS 186-3 nyní podporuje RSA (podle PKCS#1), DSA (3072 bitů) a ECDSA (podle ANSI X9.62)

Digitální podpis – délky klíčů

- Algoritmus RSA
  - Při jednom z popisů algoritmu (ve „Scientific American“ v roce 1977) autoři publikovali příklad kryptosystému (prvočísla měla 64 a 65 bitů), o kterém věřili, že je bezpečný
  - Tento příklad byl rozlomen v roce 1994
  - Koncem roku 1999 došlo k prolomení 512bitového modulo RSA (několik set rychlých počítačů pracovalo přes 4 měsíce), v roce 2010 byl faktorizován 768 bitový RSA klíč
  - V současné době se používá modulo o délkách 1024 až 4096 bitů

Digitální podpis – RSA– matematika

- Násobení prvočísel snadné, ale faktorizace čísel výpočetně náročná
- Velká prvočísla **p** a **q**, **n** = **p·q**, **ϕ(n) = (p-1)(q-1)**
- Zvolíme velké **e** takové, že **gcd(e, ϕ(n)) = 1**
- Spočítáme **$d = e^{-1} \pmod{\phi(n)}$**
- Veřejný klíč – **n, e**
  Neveřejné parametry – **p, q, d**
- Šifrování – **$c = w^e \bmod n$**
- Dešifrování – **$w = c^d \bmod n$**

RSA příklad (1)

- Karel má veřejný klíč (e, n) = (13, 77)
- Zašifrujte vzkaz pro Karla, jímž je číslo m = 26
- Označme zašifrovaný text jako c
- Je to číslo z množiny {0, . . . , 76} splňující vztah
  - $c \equiv m^e \pmod{n}$

RSA příklad (2)

- Řešíme kongruenci $c \equiv 26^{13} \pmod{77}$
- Je zbytečné počítat číslo 26^{13} - místo toho postupujeme následovně
  - $26^1 \equiv 26 \pmod{77}$
  - $26^2 \equiv 676 \equiv -17 \pmod{77}$
  - $26^4 \equiv (-17)^2 \equiv -19 \pmod{77}$
  - $26^8 \equiv (-19)^2 \equiv -24 \pmod{77}$
  - $c \equiv 26^{13} \equiv 26^{8+4+1} \equiv -24 \cdot (-19) \cdot 26 \equiv 75 \pmod{77}$
    - $\Rightarrow$ Zašifrovaný text je $c = 75$

RSA příklad (3)

- Dešifrujte vzkaz pro Karla, jímž je číslo c = 75 pomocí jeho soukromého klíče (d, n) = (37, 77) (d je dešifrovací exponent).
- Označme dešifrovaný text jako m. Je to číslo z množiny {0, . . . , 76} splňující vztah
  - $m \equiv c^d \pmod{n}$ $m \equiv 75^{37} \pmod{77}$

RSA příklad (4)

- Řešíme kongruenci $m \equiv 75^{37} (\mathrm{mod}\ 77)$
- Je zbytečné počítat číslo 75^{37} - místo toho postupujeme následovně
  - $75^1 \equiv 75\ (\mathrm{mod}\ 77)$
  - $75^2 \equiv 5625 \equiv 4\ (\mathrm{mod}\ 77)$
  - $75^4 \equiv (4)^2 \equiv 16\ (\mathrm{mod}\ 77)$
  - $75^8 \equiv (16)^2 \equiv 25\ (\mathrm{mod}\ 77)$
  - $75^{16} \equiv (25)^2 \equiv 9\ (\mathrm{mod}\ 77)$
  - $75^{32} \equiv (9)^2 \equiv 4\ (\mathrm{mod}\ 77)$
  - $m \equiv 75^{37} \equiv 75^{32+4+1} \equiv 4 \cdot 16 \cdot 75 \equiv 26\ (\mathrm{mod}\ 77)$
    - $\Rightarrow$ Dešifrovaný text je m = 26

RSA příklad (5)

- $n = 77 = p \cdot q = 7 \cdot 11$
- $\phi(n) = (p-1)(q-1) = 6 \cdot 10 = 60$
- $\gcd(e, \phi(n)) = 1$, platí $\gcd(13, 60) = 1$
- $d = e^{-1} \pmod{\phi(n)}$
- $x \cdot 60 + y \cdot 13 \equiv 1 \pmod{60}$ a $x \cdot 60 \equiv 0 \pmod{60}$
- $60 = 4 \cdot 13 + 8 \Rightarrow 8 = 60 - 4 \cdot 13$
- $13 = 1 \cdot 8 + 5 \Rightarrow 5 = 13 - 1 \cdot 8 \Rightarrow 5 = 13 - 1 \cdot (60 - 4 \cdot 13) \Rightarrow 5 = 5 \cdot 13 - 60$
- $8 = 1 \cdot 5 + 3 \Rightarrow 3 = 8 - 1 \cdot 5 \Rightarrow 3 = 60 - 4 \cdot 13 - 1 \cdot (5 \cdot 13 - 60) \Rightarrow 3 = 120 - 9 \cdot 13$
- $5 = 1 \cdot 3 + 2 \Rightarrow 2 = 5 - 1 \cdot 3 \Rightarrow 2 = 5 \cdot 13 - 60 - 1 \cdot (120 - 9 \cdot 13) \Rightarrow 2 = 14 \cdot 13 - 180$
- $3 = 1 \cdot 2 + 1 \Rightarrow 1 = 3 - 1 \cdot 2 \Rightarrow 1 = 120 - 9 \cdot 13 - 1 \cdot (14 \cdot 13 - 180) \Rightarrow 1 = 300 - 23 \cdot 13 \Rightarrow 1 = 5 \cdot 60 - 23 \cdot 13$ a $-23 \equiv 37 \pmod{60}$

Výpočetní bezpečnost

- Bezpečnost RSA je založena na nesnadnosti faktorizace čísel
- Je zřejmé, že pouhým „vyzkoušením“ všech čísel do odmocniny z n se nám podaří n faktorizovat
- Bezpečnost RSA je založena na tom, že faktorizovat velká čísla (tím v současné době myslíme čísla o tisících bitů) v rozumném čase neumíme
- Pokrok v oblasti faktorizace čísel (například nalezení nového algoritmu) však může znamenat, že z veřejného klíče budeme schopni odvodit klíč privátní
- Tento algoritmus je založen na tzv. „výpočetní bezpečnosti“ (nejen tento algoritmus, „výpočetní bezpečnost“ je běžně používaný přístup)

Hašovací funkce

- **Kryptografická** hašovací funkce
  - Vstup libovolné délky
  - Výstup pevné délky – n bitů
  - Funkce není prostá (vznikají kolize)
  - Haš slouží jako kompaktní reprezentace vstupu (nazýváme též otisk, anglicky imprint, digital fingerprint nebo message digest)
- Hašovací funkce často používáme při zajišťování integrity dat. Spočítáme nejprve haš a pak pracujeme s tímto hašem (například jej podepíšeme)
- Od 2012 již třetí verze SHA-3!

Vlastnosti hašovacích funkcí

- Jednosměrnost
  - Pro libovolné x je snadné spočítat h(x)
  - V rozumném čase nejsme schopni pro pevně dané **y** najít takové **x**, že h(x) = y
- Bezkoliznost
  - (Slabá) – pro dané x nejsme schopni v rozumném čase najít x’ (x ≠ x’) takové, že h(x) = h(x’)
  - (Silná) – v rozumném čase nejsme schopni najít libovolná x, x’ taková, že h(x) = h(x’)

Příklad hašovací funkce

- Uvažujme následující hašovací funkci
  - Jednoduchý součet bajtů modulo 256
  - Fixní osmibitový výstup
  - Pro text „ahoj“ získáme 97 + 104 + 111 + 106 (mod 256) = 162
- Tuto funkci je sice jednoduché spočítat, není to však dobrá kryptografická hašovací funkce, neboť nemá vlastnost bezkoliznosti
  - h(„ahoj“) = h(„QQ“) = h(„zdarFF“)

Běžné kryptografické hašovací funkce (1)

- MD4 – výstup 128 bitů
  - Dnes se již nepoužívá
  - Byly nalezeny slabiny v algoritmu (umožňující nalezení kolizí, snižující efektivní výstup asi na 20 bitů)
- MD5 – výstup 128 bitů
  - Dnes ještě používána, ačkoliv byly nalezeny významné slabiny a algoritmus pro nalezení kolizí
  - 128 bitů se již nepovažuje za dostatečně bezpečnou délku!

Běžné kryptografické hašovací funkce (2)

- SHA-1 (Secure Hash Algorithm)
  - Výstup 160 bitů
  - NIST standard, používána v DSS (Digital Signature Standard)
  - Považována za bezpečnou pro jen nejbližší rok(y)
- „SHA-2“
  - SHA-256, SHA-384, SHA-512 (a dodána SHA-224)
  - Doporučuje se používat především tyto funkce!
  - Definovány ve standardu (NIST) FIPS 180-2

Hašovací funkce – příklady

- MD5
  - Vstup – „Autentizace“
  - Výstup – 2445b187f4224583037888511d5411c7
  - Výstupem je 128 bitů, zapisujeme hexadecimálně
  - Vstup – „Cutentizace“
  - Výstup – cd99abbba3306584e90270bf015b36a7
  - Změna jednoho bitu vstupu → velká změna výstupu
- SHA-1
  - Vstup – „Autentizace“
  - Výstup – dfcee447d609529f0335e67016557c281fc6eb44

Protokoly vyšší úrovně – SSL/TLS

- Protokol SSL/TLS poskytuje
  - Autentizaci stran – strany jsou autentizovány pomocí certifikátů a protokolu výzva-odpověď
  - Integritu – autentizační kódy (message authentication code – MAC) zajišťují integritu a autenticitu dat
  - Důvěrnost – po úvodní inicializaci („handshake“), je ustaven symetrický šifrovací klíč, kterým je šifrována všechna následující komunikace (včetně přenosu hesel apod.)

Principy SSL/TLS

- Pozice SSL/TLS
- Mezi aplikační vrstvou a protokolem TCP
- SSL/TLS nevidí do aplikačních dat
- SSL/TLS neprovádí elektronické podepisování přenášených dat

Aplikační vrstva
SSL/TLS
TCP/UDP
IP
Linková vrstva
Fyzická vrstva

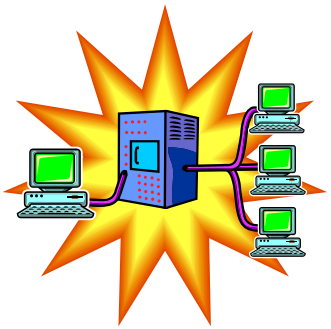
Klíče v SSL/TLS

- Použití klíčů
  - Klient generuje PreMasterSecret, šifruje veřejným klíčem serveru a posílá serveru
  - Obě strany vytvoří blok klíčů z PreMasterSecret (posílá se šifrovaně) a náhodných čísel ClientHello a ServerHello (posílají se nešifrovaně)
  - Blok klíčů tvoří klíče pro
    - MAC klient → server
    - MAC server → klient
    - Šifrování klient → server
    - Šifrování server → klient
    - Inicializační vektory

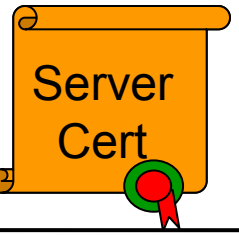
SSL/TLS

Client

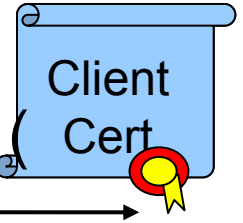
Server



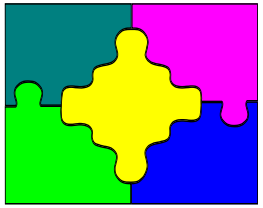
Client Hello



Server Hello, (, Client Cert Request,…)



Client Key Exchange, Cipher Spec, (, …)



Application Data

S E C U R E

Autentizace uživatelů tajnými informacemi

- „Něco, co uživatel zná“ (a ostatní ne)
- Hesla
  - Druhy hesel a jejich použití
  - Správná práce s hesly
- PINy
- Výhody a nevýhody těchto autentizačních metod

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

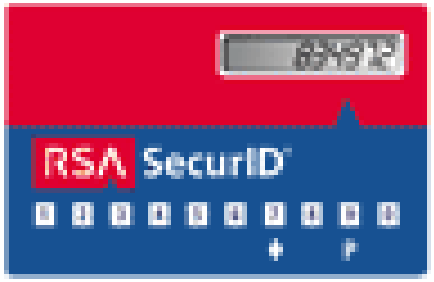
Autentizace uživatelů tokeny

- Token – „něco, co uživatel má“ (a ostatní ne)
- Inteligentní token
  - Základní druhy
  - Jejich princip a použití
- Čipové karty – využití, parametry, bezpečnost
- Výhody a nevýhody těchto autentizačních metod

Nejčastější tokeny v IT/IS

- Karty
  - S magnetickým proužkem
  - Čipové
  - Kontaktní / bezkontaktní

- Čtečka na straně dotazovatele / kontrolovaného (mobil)
  - Autentizační kalkulátory
  - S tajnou informací
  - S hodinami
  - Způsob vstupu/výstupu

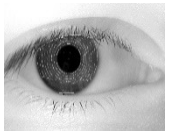


Úvod do biometrik

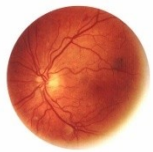
- „Něco, co uživatel je“ (a ostatní ne)
- Měřitelné biologické charakteristiky člověka-uživatele
- Fyzické – parametry částí těla
- Chování (behaviorální) – parametry činnosti
- Míra tolerance – prahová hodnota
- Nesprávné odmítnutí/přijetí

Biometrické autentizační metody

- Otisk prstu
- Vzor oční duhovky



- Vzor oční sítnice



- Srovnání obličeje

- Geometrie ruky

- Verifikace hlasu

- Dynamika podpisu

- Dynamika psaní na klávesnici

Využití biometrik

- Problémy biometrik – bezpečnost
- Otázky praktického použití
  - Současná omezení a použitelnost
  - Vhodné použití
  - Nevhodné použití
- Vztah biometrik a kryptografie