

# Praktická stránka elektronického podpisu



---

Tomáš Rosa

**eBanka** a.s., Praha

Katedra počítačů, FEL, ČVUT v Praze

[trosa@ebanka.cz](mailto:trosa@ebanka.cz)



# Osnova přednášky

---

## ■ Kryptologie

- základní seznámení s oborem
- Podpisová schémata
  - elementární principy, schéma s dodatkem
  - metody RSA, DSA, ECDSA
  - kryptoanalýza podpisových schémat, útoky
- Nepopiratelnost digitálního podpisu
  - souvislost s nepadělatelností
  - univerzální nepopiratelnost
- Elektronický podpis
  - souvislost s digitálním podpisem
  - druhy elektronického podpisu



# Podpisová schémata

---

- Historické souvislosti
  - 1976, Diffie-Hellman: formulace základních principů asymetrických schémat
  - 1978, Rivest-Shamir-Adleman: metoda RSA
  - 1990, Rompel: *existence jednosměrných funkcí je nutnou a postačující podmínkou pro existenci podpisových schémat*
  - 1991, NIST: metoda DSA jako součást první verze standardu DSS
  - 1992, Vanstone: návrh ECDSA
  - 1998<sup>1</sup>, 1999<sup>2</sup>, 2000<sup>3</sup>: ECDSA přijato jako standard ISO<sup>1</sup>, ANSI<sup>2</sup>, IEEE<sup>3</sup> a NIST<sup>3</sup>



# Podpisová schémata

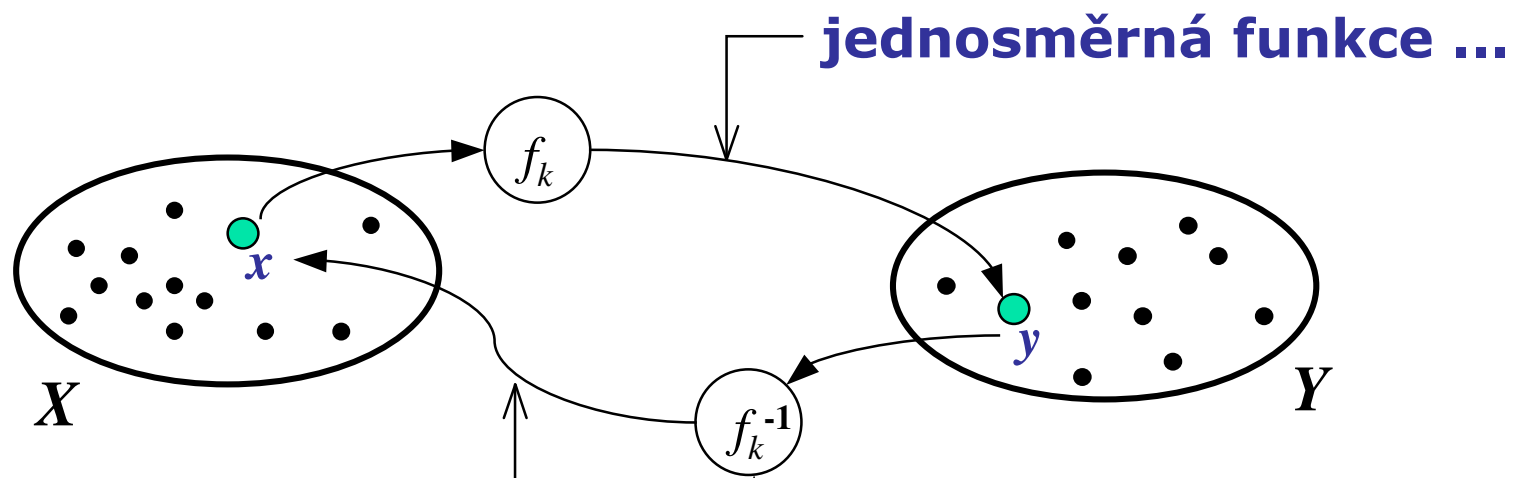
## -elementární principy- (1)

---

- Ukážeme si konstrukci podpisového schématu typu RSA
  - schéma se opírá o použití jednosměrné funkce s padacími vrátky
  - metody založené na čistě jednosměrných funkcích jsou poněkud odlišné (DSA, ECDSA)

# Podpisová schémata

## -elementární principy- (2)



... s padacími vrátky



# Podpisová schémata

## -elementární principy- (3)

---

### ■ Předpokládejme

- funkce  $f_k$  je spojena s určitým konkrétním subjektem - uživatelem  $A$ 
  - je to jeho veřejný klíč
- informace o padacích vrátkách  $k$  je známa pouze subjektu  $A$ 
  - je to jeho privátní klíč

# Podpisová schémata

## -elementární principy- (4)

---

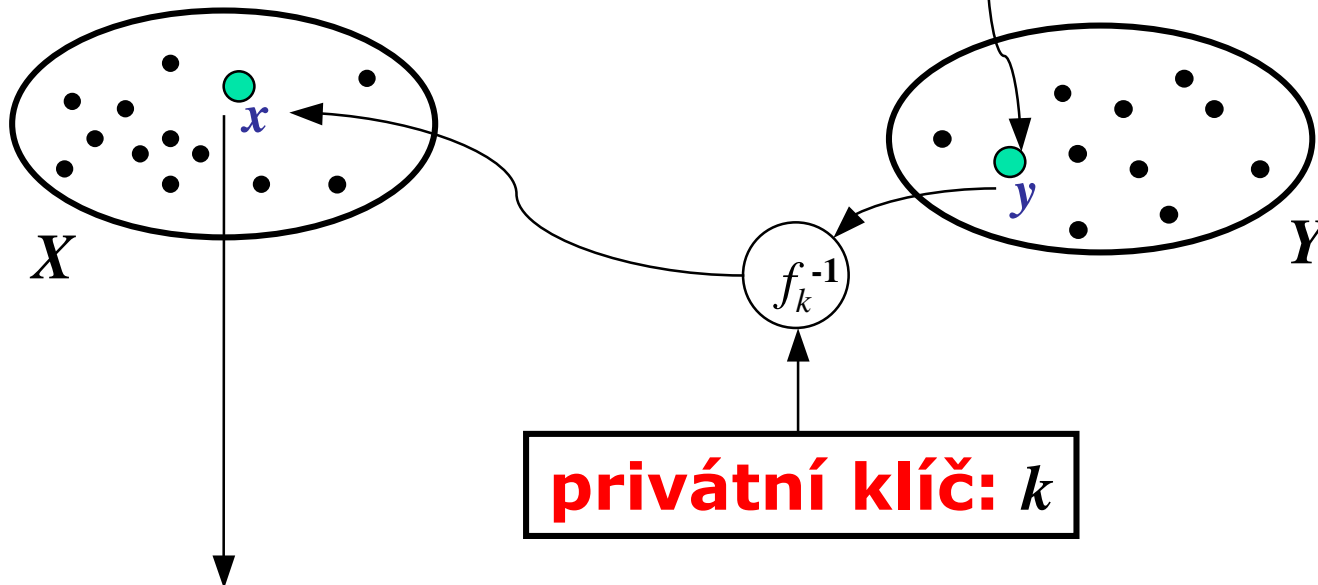
- Z vlastností  $f_k$  plyne
  - z pouhé znalosti  $f_k$  nelze najít výpočetně schůdnou inverzní funkci  $f_k^{-1}$
  - čili speciálně: ze znalosti veřejného klíče nelze nalézt klíč privátní
  - tedy nakonec prakticky: ten, kdo zná pouze veřejný klíč, dokáže podpis ověřit, ale nedokáže jej sám vytvořit

# Podpisová schémata

-elementární principy- (5)

hašovací funkce  $h$   
 $y = h(m)$

podepisovaná zpráva:  $m$

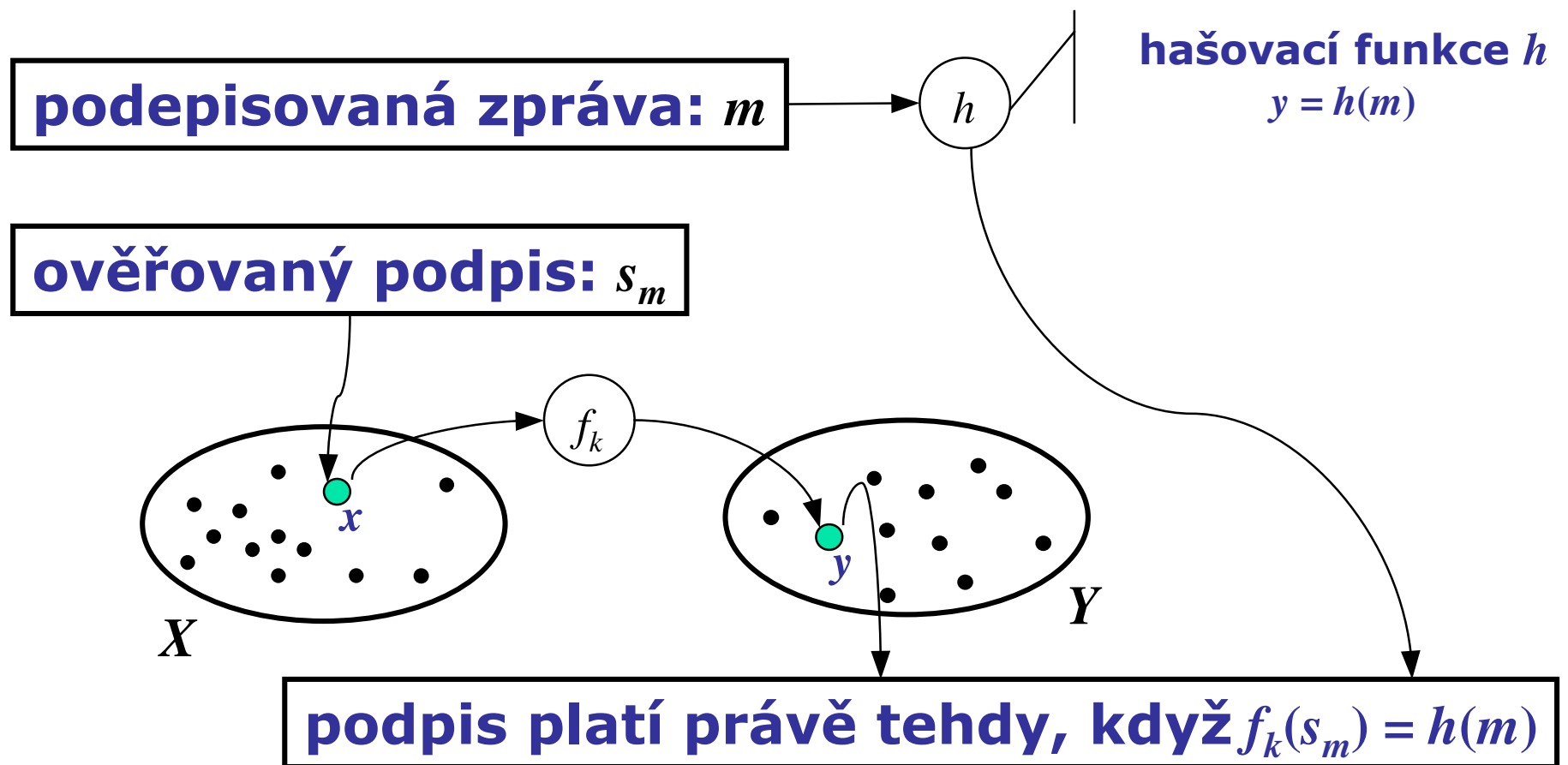


digitální podpis zprávy  $m$ :  $s_m = x = f_k^{-1}(y)$



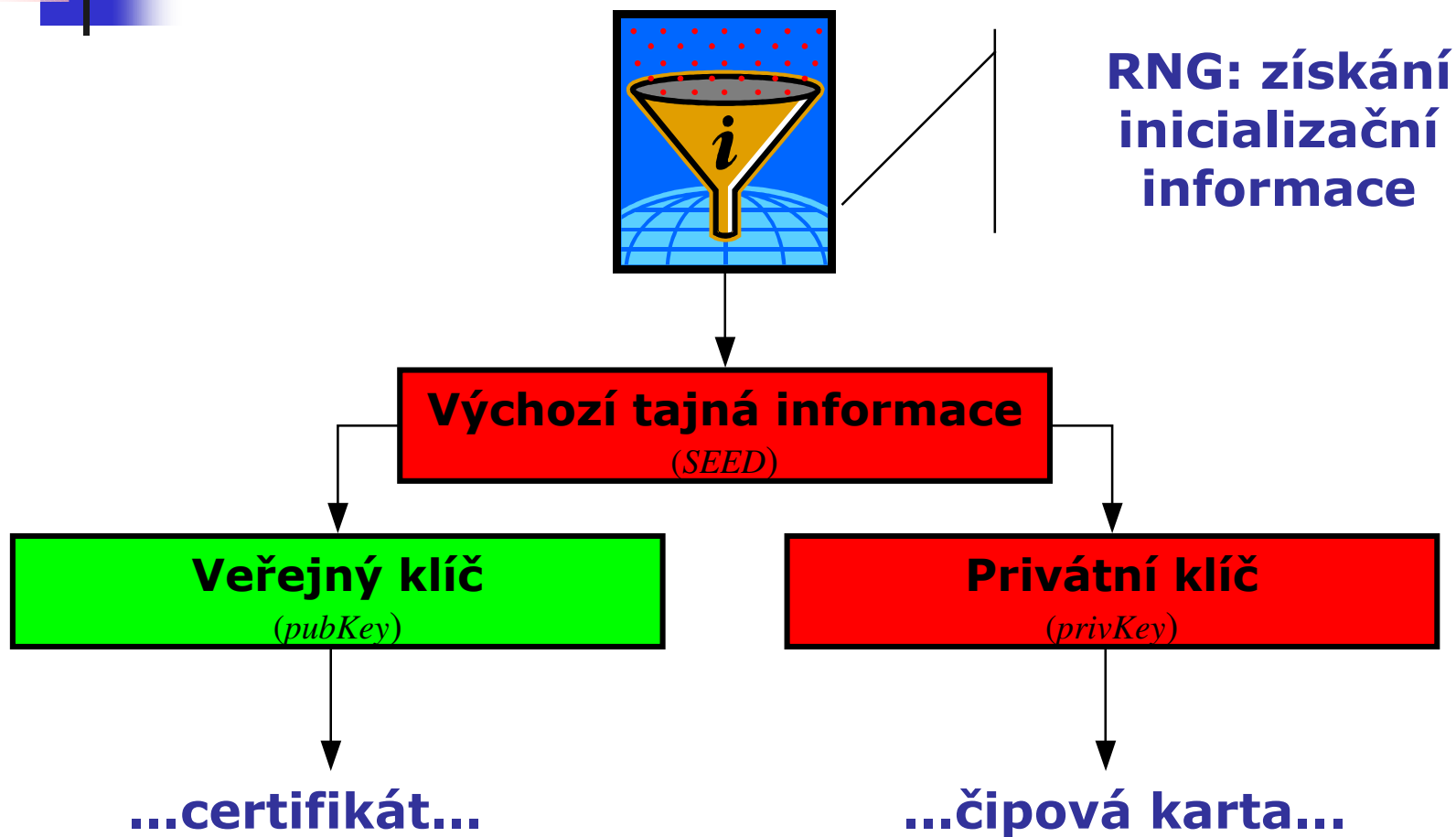
# Podpisová schémata

-elementární principy- (6)



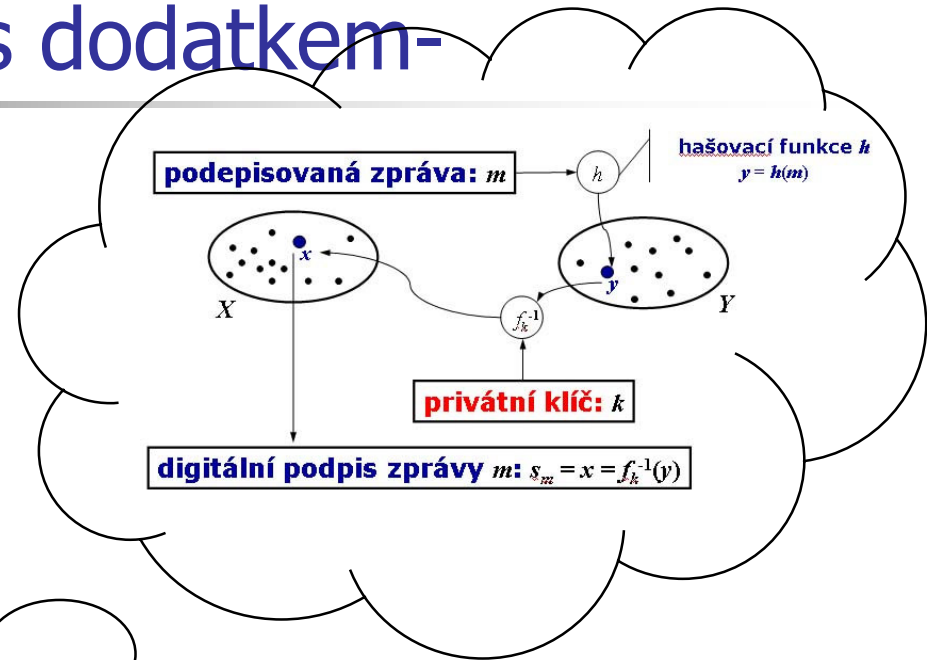
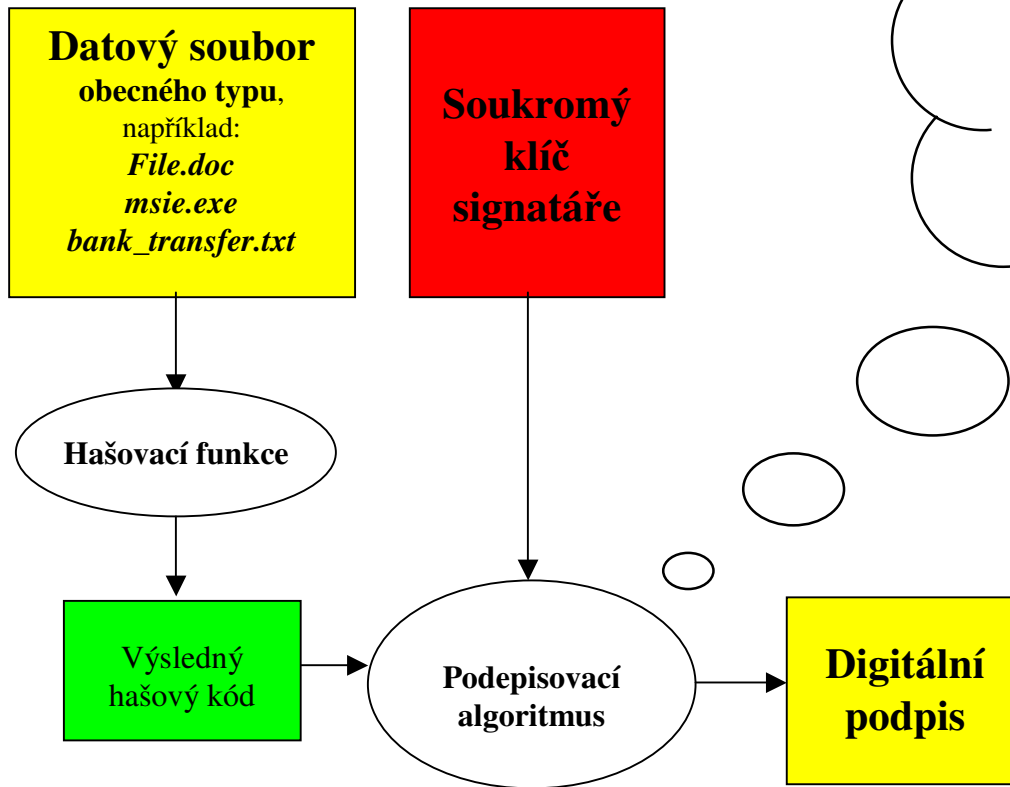
# Podpisová schémata

-inicializace instance-



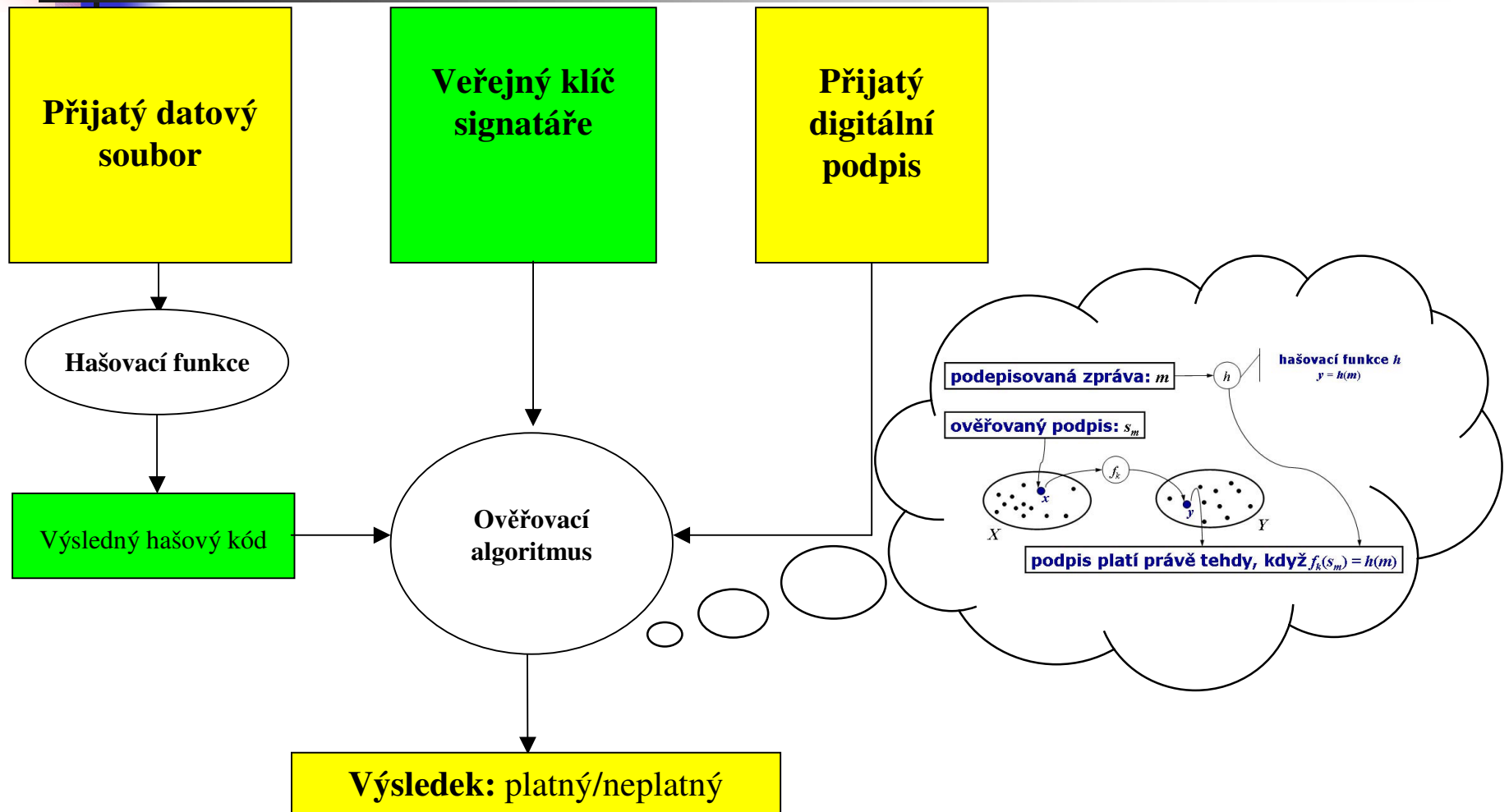
# Podpisová schémata

## -výpočet podpisu s dodatkem-



# Podpisová schémata

## -ověření podpisu s dodatkem-





# O vztahu asymetrických šifer a podpisových schémat

---

- Obecně: Asymetrické šifry a podpisová schémata nejsou jedno a totéž
- Speciální případy: Za určitých okolností lze asymetrickou šifru převést na podpisové schéma a obráceně
  - pozor na terminologii: odšifrování  $\sim$  podpis!
- Společný rys:
  - využití jednosměrných funkcí a jednosměrných funkcí s padacími vrátky
  - rozhodující vliv na bezpečnost má způsob kódování šifrované či podepisované zprávy

## ■ Inicializace schématu

- Vygenerujeme nezávisle dvě velká (zhruba stejně) prvočísla  $p, q$ ,  $p \neq q$ .
- Spočtáme  $N = pq$ ,  $\lambda = \text{lcm}(p-1, q-1)$ .
- Zvolme náhodné číslo  $e$ ,  $1 < e < \lambda$ ,  $\text{gcd}(e, \lambda) = 1$ .
  - Někdy se volí  $e$  pevně (zejména  $e = 3, 65537$ ).
- Spočtáme  $d$  splňující:  $1 < d < \lambda$ ,  $ed \equiv 1 \pmod{\lambda}$ .
  - Použijeme rozšířený Eukleidův algoritmus.
- Veřejným klíčem budiž dvojice  $(N, e)$ .
  - $N$  nazýváme modul a  $e$  veřejný exponent RSA.
- Privátním klíčem budiž dvojice  $(N, d)$ .
  - $d$  nazýváme privátní exponent RSA.
  - Pro bezpečnost je nutné ošetřit integritu dvojice  $(N, d)$ .



# RSA

(2)

- Podepisovací transformace:  $RSASP((N, d), m)$ 
  - Vstup: Privátní klíč RSA  $(N, d)$ , zformátovaná zpráva pro podpis  $m$ ,  $0 \leq m \leq N-1$ .
  - Výpočet:
    - $RSASP((N, d), m) = m^d \bmod N$
- Ověřovací transformace:  $RSAVP((N, e), s)$ 
  - Vstup: Veřejný klíč RSA  $(N, e)$ , ověřovaný podpis  $s$ ,  $0 \leq s \leq N-1$ .
  - Výpočet:
    - $RSAVP((N, e), s) = s^e \bmod N$

- Podpisové schéma
  - Vystavěno na transformacích RSASP(.) a RSAVP(.).
    - Důležité jsou přídatné funkce ENCODE/VERIFY.
  - Schéma s obnovou zprávy
    - Zprávu a její podpis nelze jednoznačně oddělit. Používá se zřídka pro velmi krátké zprávy.
    - ISO/IEC 9796 – závažné problémy
  - Schéma s dodatkem
    - Podpis tvoří jasně identifikovatelný doplněk k podepsané zprávě.
    - V současnou dobu toto schéma převažuje.



# RSA

(4)

## podpisové schéma s dodatkem-

- Výpočet podpisu zprávy
  - Vstup: privátní klíč RSA  $(N, d)$ , zpráva pro podpis  $M$  (jako binární řetězec).
  - Výpočet:
    1.  $H = \text{hash}(M)$ 
      - Na úrovni stejných hašových kódů jsou dvě různé zprávy nerozlišitelné.
    2.  $m = \text{ENCODE}(H)$
    3.  $s = \text{RSASP}((N, d), m)$
    4. Výsledkem budiž  $s$ .

# RSA

(5)

## podpisové schéma s dodatkem-

---

- **Ověření podpisu zprávy**
  - Vstup: veřejný klíč RSA  $(N, e)$ , zpráva pro ověření podpisu  $M$  (jako binární řetězec), ověřovaný podpis  $s$ .
  - Výpočet:
    1.  $m = \text{RSAVP}((N, e), s)$
    2.  $H = \text{hash}(M)$
    3.  $V = \text{VERIFY}(H, m)$ ,  $V \in \{\text{ANO}, \text{NE}\}$
    4. Výsledkem budiž  $V$ .

- Standardizován ve FIPS PUB 186-2
  - DSS – *Digital Signature Standard*, popisuje DSA – *Digital Signature Algorithm* a navíc stanoví, že jako hašovací funkce (dále  $h$ ) se má použít SHA-1 (FIPS PUB 180-2).
  - Zatím není DSA standardizován pro SHA-256,-384,-512 (nově zavedeny ve FIPS PUB 180-2).
    - Tento krok lze očekávat v následujících verzích FIPS PUB 186.
- Algebraicky připomíná ElGamal přenesený na podgroupu prvočíselného řádu.
  - Souvisí také se Schnorrovým schématem.

- Inicializace schématu

- Vygenerujeme náhodné prvočíslo  $q$ ,  $2^{159} < q < 2^{160}$ .
- Vygenerujeme náhodné prvočíslo  $p$ ,  $2^{1023} < p < 2^{1024}$  tak, aby  $q|(p-1)$ .
- Nalezněme generátor  $\alpha$  cyklické podgrupy grupy  $\mathbf{Z}_p^*$  řádu  $q$ .
- Zvolme privátní exponent  $x$ ,  $0 < x < q$ .
- Vypočtěme veřejný klíč  $y$ ,  $y = \alpha^x \bmod p$ .
- Veřejné parametry schématu jsou  $(p, q, \alpha)$ .
  - Někdy je veřejný klíč uváděn ve tvaru  $(p, q, \alpha, y)$ .
- Privátní klíč je čtveřice  $(p, q, \alpha, x)$ .
  - Je nutné zajistit integritu čtveřice  $(p, q, \alpha, x)$ .
  - Ačkoliv to tak řada popisů dělá, není vhodné vnímat  $x$  samostatně jako privátní klíč.

## ■ Podpis zprávy

- Vstup: Privátní klíč  $(p, q, \alpha, x)$ , zpráva pro podpis  $m$ , hašovací funkce  $h$  (v DSS  $h=SHA-1$ ).
- Výpočet:
  1. Vygenerujeme tajné náhodné číslo  $k$ ,  $0 < k < q$ .
    - Parametr  $k$  bývá označován jako *dočasný klíč zprávy*.
    - Kompromitace  $k$  vede ke kompromitaci privátního klíče.
  2. Vypočtíme  $r = (\alpha^k \bmod p) \bmod q$ .
  3. Vypočtíme  $s = k^{-1}(h(m) + xr) \bmod q$ , kde  $kk^{-1} \equiv 1 \pmod{q}$ .
  4. Ověříme, že  $r \neq 0$  a  $s \neq 0$ , jinak se výpočet opakuje.
  5. Podpisem budiž dvojice  $(r, s)$ .

- Ověření podpisu
  - Vstup: Veřejné parametry a klíč  $(p, q, \alpha, \gamma)$ , zpráva  $m$ , ověřovaný podpis  $(r, s)$ , hašovací funkce  $h$  (v DSS  $h=\text{SHA-1}$ ).
  - Výpočet:
    1. Ověříme, že  $0 < r < q$  a  $0 < s < q$ . Jinak podpis odmítneme jako neplatný.
    2. Vypočtíme  $w = s^{-1} \bmod q$ .
    3. Vypočtíme  $u_1 = w * h(m) \bmod q$  a  $u_2 = r * w \bmod q$ .
    4. Vypočtíme  $v = (\alpha^{u_1} \gamma^{u_2} \bmod p) \bmod q$ .
    5. Podpis prohlásíme za platný iff  $v = r$ .



# ECDSA

---

- Algebraické rozšíření DSA.
- Namísto  $\mathbf{Z}_p^*$ , respektive její cyklické podgrupy, je použita eliptická křivka  $E(\mathbf{F}_q)$ , respektive její cyklická podgrupa prvočíselného řádu  $n$ , kde  $n > 2^{160}$ .
- Použitá křivka je generována náhodně nebo je použita některá ze standardizovaných křivek.
  - U ECDSA je běžné sdílení veřejných parametrů (těleso, křivka, generátor podgrupy a jeho řád).
  - Při generování nových křivek je třeba pečlivě kontrolovat možné anomálie, které mohou vést k efektivním útokům.



# Kryptoanalýza podpisových schémat

---

- Potenciální místa útoku
  - základní kryptografické transformace
    - inverze jednosměrných funkcí, kolize hašovacích funkcí,...
  - formátování podepisovaných dat
    - vážný problém u ISO 9796 – schéma s obnovou zprávy
    - u používaných schémat s dodatkem zatím nezjištěny vážnější slabiny
  - generování klíčů a ukládání klíčů
    - nevědomé či záměrné generování slabých klíčů
    - útoky na čipové karty postranními kanály
  - vyšší procesy informačního systému
    - trójský kůň – podstrčení dokumentu pro podpis, atp.
    - nedodržení okrajových podmínek použitých kryptografických mechanismů





# Řešení úloh faktorizace<sup>1</sup>, DLP<sup>2</sup> a ECDLP<sup>3</sup>

---

- Bezprostředně souvisí s bezpečností RSA<sup>1</sup>, DSA<sup>2</sup> a ECDSA<sup>3</sup>
  - význam pro dlouhodobé plánování
  - bezprostřední dopad „běžných objevů“ na současné dobře navržené systémy zanedbatelný
  - bezpečnost praktických implementací více ohrožují jiné a závažnější objevy
    - na první pohled však nejsou tak markantní



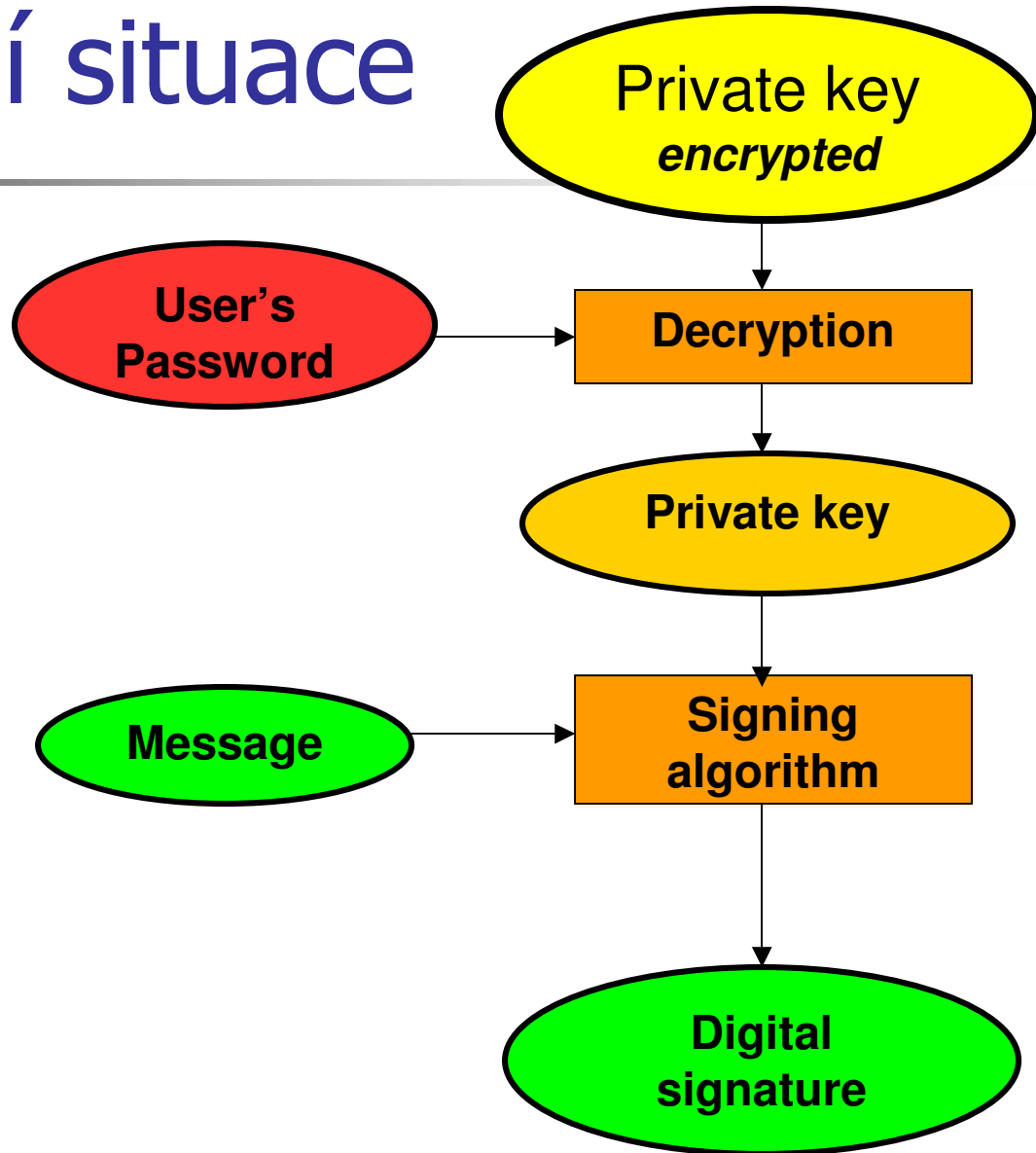
# Řešení úloh faktorizace<sup>1</sup>, DLP<sup>2</sup> a ECDLP<sup>3</sup>

---

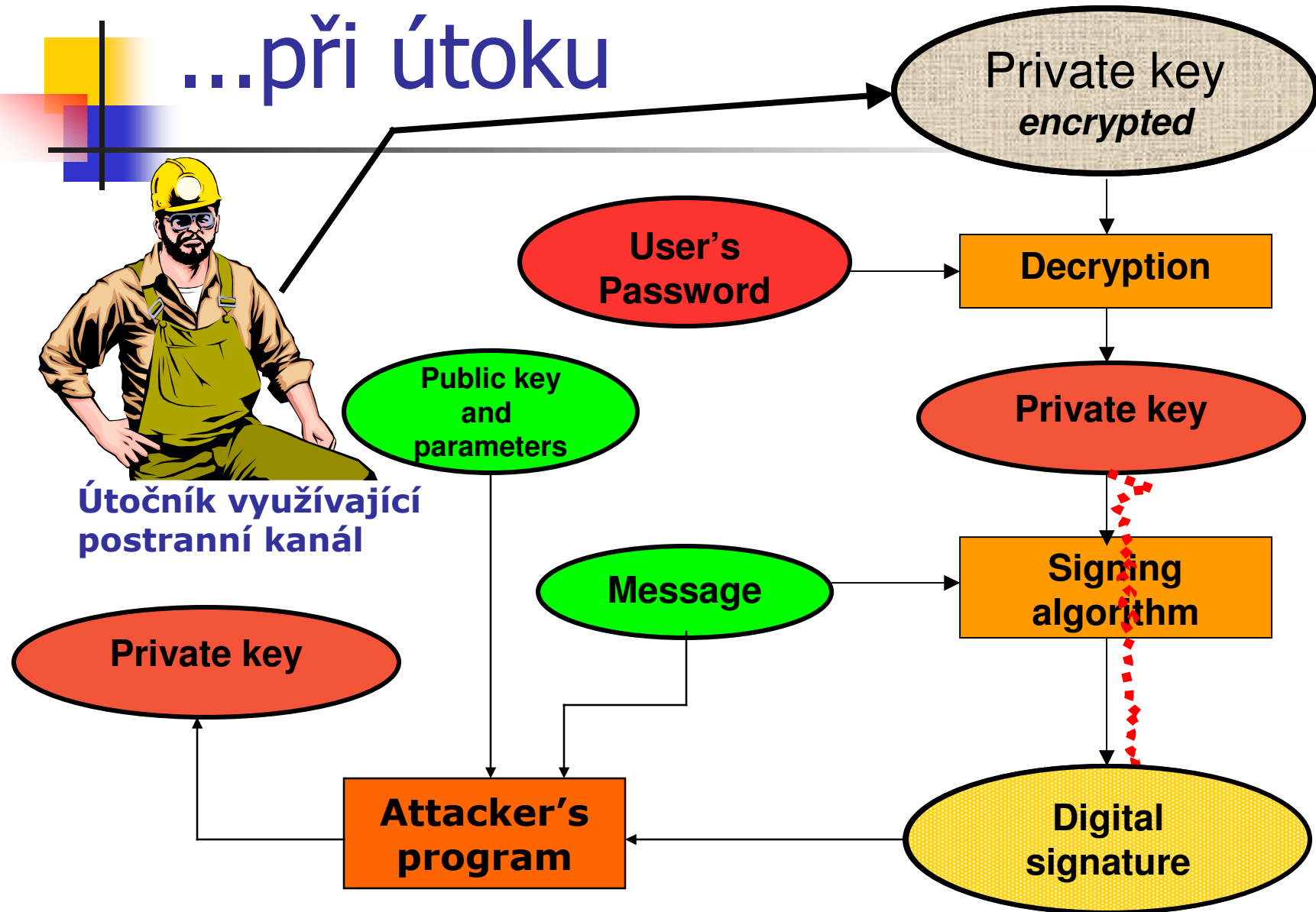
- Klasické metody
  - NFS<sup>1</sup>, NFS/Index-calculus<sup>2</sup>, Pollardovy metody<sup>1,2,3</sup>  $\rho$  a  $\lambda$
  - rozvoj zatím víceméně stagnuje
- Speciální akcelerátory
  - TWINKLE<sup>1,2</sup>, TWIRL<sup>1,2</sup>
    - elektrooptické prosévací zařízení
- Kvantové počítače
  - Shorův algoritmus<sup>1,2,3</sup>

# Normální situace

Podepsání zprávy



# ...při útoku





# Nepopiratelnost digitálního podpisu

---

- **Definice.** *Nezávislá třetí strana je schopna jednoznačně ověřit, že daný subjekt předložený dokument podepsal (respektive nepodepsal).*
- V současných systémech není nepopiratelnosti dosaženo automaticky
- Příslušný systém musí být s ohledem na požadovanou vlastnost nepopiratelnosti speciálně navržen a konstruován
  - pozor na změnu pohledu: Útočníkem je zde často sám majitel privátního klíče!



# Nepadělatelnost digitálního podpisu

---

- **Definice.** *Neexistuje zpráva, jejíž podpis je možné najít s pouhou znalostí veřejného klíče a jiných podepsaných zpráv.*
  - odpovídá mezím teoreticky prokazatelných vlastností
  - ve skutečnosti však odstiňuje pouze část možných útoků
  - reálné útoky probíhají za volnějších podmínek
    - postranní kanály
    - obecně „povolená“ interakce s podepisovacím modulem
    - trójský kůň...



# Nepadělatelnost vs. nepopiratelnost

---

- nepopiratelnost  $\Rightarrow$  nepadělatelnost
  - čili zajištění nepadělatelnosti je vhodné chápat v kontextu zajištění nepopiratelnosti
- z praktického hlediska je vhodné soustředit se na nepopiratelnost
  - omezení se pouze na nepadělatelnost je zavádějící

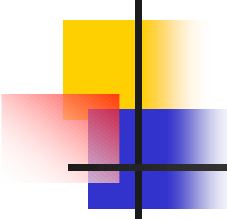


# Univerzální nepopiratelnost

---

- I při nepopiratelnosti mohou hrozit útoky
  - vycházejí zejména z technických slabin konkrétního IS
  - podstata: lokální zmatení konkrétní osoby ověřující daný podpis
    - výrok této osoby se bude lišit od pozdějšího (správného) výroku soudce
- Řešení: univerzální nepopiratelnost
  - taková nepopiratelnost, kde role třetí strany není omezena na určitou skupinu vybraných autorit
    - čili každá ověřující osoba je schopna vydat rozhodnutí o pravosti podpisu konvenující s pozdějším verdiktem soudce





# Zajišťování (univerzální) nepopiratelnosti

---

- Vyžaduje pečlivý formální rozbor procesů celého IS
  - mimo jiné se dotýká klíčového hospodářství
    - nikdo (ani sám majitel daného klíče) nesmí být schopen zcela ovlivnit hodnotu generovaných klíčů
  - zahrnuje i ostatní partie
    - formáty zpracovávaných dokumentů
    - architekturu adresářových a síťových služeb



# Útoky na nepopiratelnost

---

- Využívají kryptoanalytické útoky na použité podpisové schéma k zajištění dílčích cílů hlavního útoku
- Cíl hlavního útoku
  - získat profit z napadení výroku o pravosti/nepravosti předloženého podpisu
    1. útočník před soudem popírá svůj vlastní podpis
      - nejčastější případ
    2. útočník\* prokazuje, že někdo jiný podepsal jím\* předložený dokument v jím\* předložené podobě



# Popírání podpisu

---

- Základní princip: *alternativní vysvětlení*
  - útočník předkládá soudu (alternativní) vysvětlení toho, proč se u předloženého dokumentu nachází jeho (matematicky) platný podpis, jestliže on dokument nepodepsal
- Kryptologická opora soudních verdiktů
  - spočívá v tom, že nelze nalézt alternativní vysvětlení
    - čili, existuje pouze jedno matematicky korektní vysvětlení dané situace



# Hledání alternativního vysvětlení

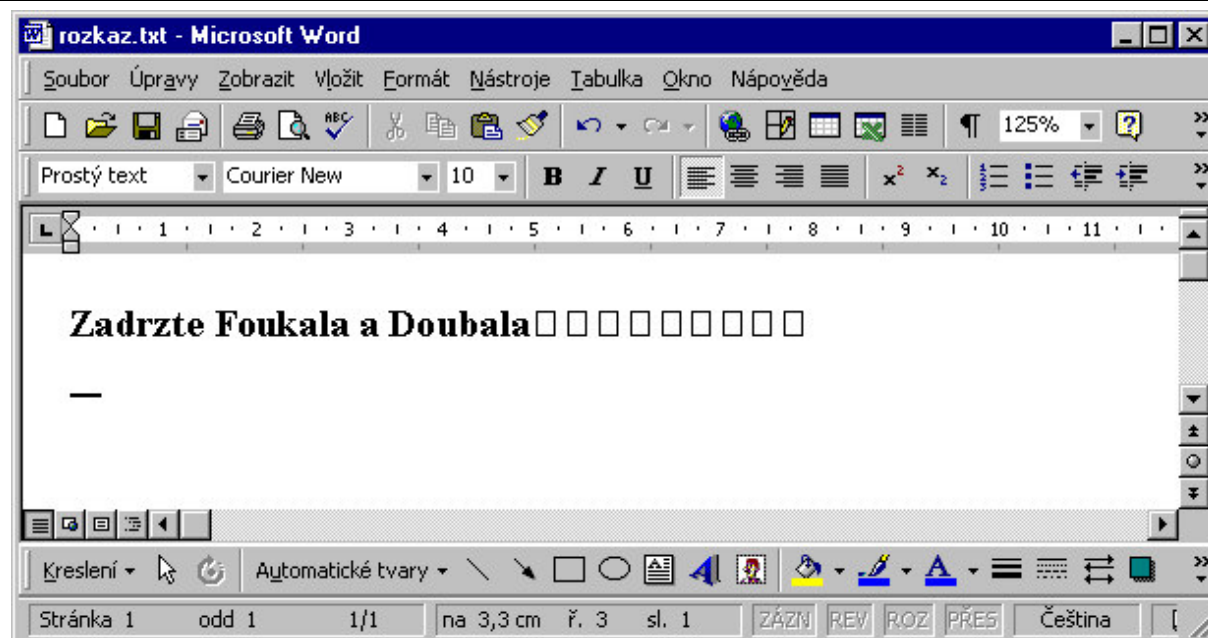
---

- Nalezení kolize
  - zpráv
  - veřejných klíčů
- Zpochybnění
  - neпадělatelnosti podpisů v daném schématu
  - kvality generování a ochrany privátních klíčů
  - bezpečnosti podepisovacího modulu
- Předstírání zmatení
  - kódování podepisovaných zpráv
  - trójský kůň

# Příklad


## -kódování zpráv- (1)

```
Lister - [E:\rozkaz.txt]
File Edit Options Help 100%
00000000: 0D 0A 5A 61 64 72 7A 74|65 20 46 6F 75 6B 61 6C | ■■Zadržte Foukal
00000010: 61 20 61 20 44 6F 75 62|61 6C 61 08 08 08 08 08 | a a Doubala■■■■■
00000020: 08 08 08 08 20 20 20 20|20 20 20 20 20 0D 0A 0D | ■■■■ ■■■■
00000030: 0A
|
```



# Příklad

-kódování zpráv- (2)



```
MS-DOS C:\WINNT\system32\cmd.exe
E:\>type rozkaz.txt
Zadržte Foukala
E:\>
```



# Nepopiratelnost a fyzické předměty

---

- Typicky se dnes jedná o čipové karty
  - privátní klíč je uložen na kartě a chráněn mechanismem PIN
  - volitelně lze privátní klíč na kartě i vygenerovat a provádět s ním podepisovací transformaci přímo v prostředí karty
    - klíč prokazatelně nikdy neopustí kartu
- Snižuje možnost alternativního vysvětlení
  - uživatel má klíč pod jistou úrovní své kontroly
- Sama karta ale nestačí
  - předstírání zmatení – aplikace zobrazující podepsovanou zprávu není pod kontrolou čipové karty
  - zpochybnění kvality klíče generovaného na kartě (slabiny (P)RNG)



# Nepopiratelnost a autonomní podpisové moduly

---

- Cílem je dále snížit riziko nalezení alternativního vysvětlení
  - součástí modulu může být i zobrazovací jednotka a klávesnice
  - lze očekávat lepší řešení problémových oblastí čipových karet – RNG, apod.
- Pro plošné nasazení však zatím nedostupné
  - řádově vyšší cena
  - možné problémy s kompatibilitou
- Nasazovány jako jádra klíčových systémů
  - certifikační authority
  - notářské služby
  - ...





# Elektronický podpis (1)

---

- Úzce spojen s podpisem digitálním
  - nejsou to ovšem zcela totožné pojmy
  - digitální podepisování chápeme jako bezpečnostně nejlepší způsob realizace podepisování elektronického
- Pojmy z jiné oblasti
  - digitální podpis je pojem kryptologický
  - elektronický podpis je pojem zejména právní a normotvorný
- Odlišný pohled
  - definice elektronického podpisu stanovuje požadavky
    - způsob realizace není v popředí zájmu
  - schémata digitálního podpisu se soustředí na plnění stanovených požadavků



# Elektronický podpis (2)

---

- V ČR upraven zákonem
  - č. 227/2000 Sb., č. 226/2002 Sb.
  - včetně souvisejících vyhlášek a nařízení
- Vyhláška ÚOOÚ č. 366/2001 Sb.
  - doplňuje technické a technologické aspekty zákona
  - stanovuje přípustné kryptografické mechanismy
  - styčná plocha mezi kryptologickým a legislativním pohledem



# Elektronický podpis (3)

-korespondence pojmů-

---

- Data pro vytváření elektronického podpisu
  - privátní klíč uživatele
- Data pro ověřování elektronického podpisu
  - veřejný klíč uživatele



# Elektronický podpis (4)

## -druhy podpisu a požadavky-

---

- Elektronický podpis (EP)
  - základní druh
  - není požadována nepopiratelnost
  - nestanovuje žádné další bezpečnostní vlastnosti
- Zaručený elektronický podpis (ZEP)
  - EP, který splňuje jisté bezpečnostní nároky
  - požaduje nepopiratelnost
  - lze jej chápat jako soubor požadavků na službu elektronického podepisování v daném IS jako celku
    - i když je definován jako soubor vlastností datové položky



# Elektronický podpis (5)

## -druhy podpisu a požadavky-

---

- Kvalifikovaný elektronický podpis
  - není přímo pojem zákona
    - ten však používá jeho opisnou definici
  - ZEP, který splňuje rozšířené bezpečnostní nároky
    - veřejný klíč je certifikován *kvalifikovaným certifikátem* (viz zákon)
    - podpis je prováděn *prostředkem pro bezpečné vytváření podpisu* (viz zákon)
  - zvyšuje kvalitu nepopiratelnosti
    - snižuje možnost zmatení
    - požaduje autonomní podepisovací modul



# Závěr

---

- Na bezpečnosti elektronického podepisování se podílí řada faktorů
  - počínaje kvalitou matematických primitiv a konče odolností pracovních stanic uživatelů
  - z kryptologického hlediska se jedná zejména o typ použitého schématu, kvalitu RNG, generování a uchovávání klíčů
- Hlavním cílem je nepopiratelnost
  - musíme být schopni útočníkovi\* dokázat, že sám nebyl předmětem jiného útoku a tím zmařit jeho\* útok
- Elektronické podepisování vs. digitální podepisování
  - legislativní vs. matematicko-technický pohled na dvě pronikající se oblasti



# Další informace...

---

- Archiv českých článků o kryptologii
  - <http://crypto.hyperlink.cz>
  - <http://cryptography.hyperlink.cz>
- Ministerstvo informatiky České republiky
  - <http://www.micr.cz>
- EESSI - The European Electronic Signature Standardization Initiative
  - <http://www.ict.etsi.org/eessi/EESSI-homepage.htm>