Seznámení s asymetrickou kryptografií, díl 2.

Ing. Tomáš Rosa
ICZ a.s., Praha
Katedra počítačů, FEL, ČVUT v Praze
tomas.rosa@i.cz

Osnova přednášky

- Podpisová schémata
  - elementární principy, schéma s dodatkem
  - metody RSA, DSA, ECDSA
  - kryptoanalýza podpisových schémat, útoky
- Nepopiratelnost digitálního podpisu
  - souvislost s nepadělatelností
  - univerzální nepopiratelnost
  - fyzické předměty a autonomní podpisové moduly

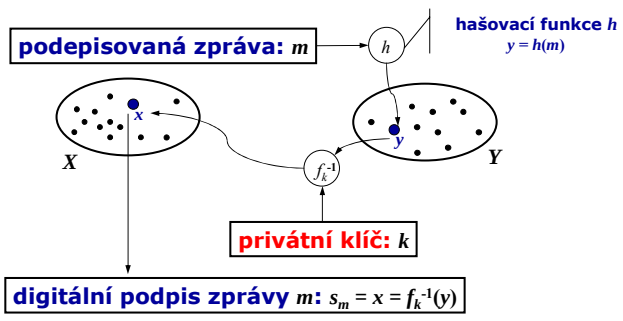
Podpisová schémata

- 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[1], 1999[2], 2000[3]: ECDSA přijato jako standard ISO[1], ANSI[2], IEEE[3] a NIST[3]

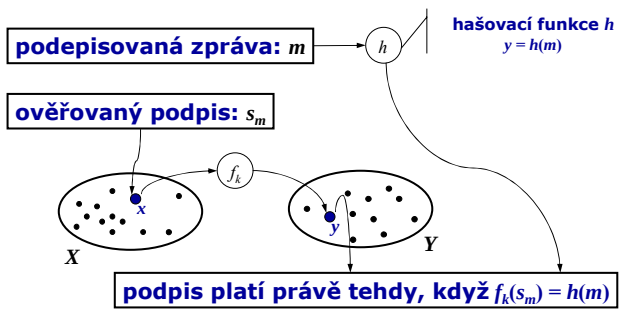
Podpisová schémata
-elementární principy- (1)

- 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)

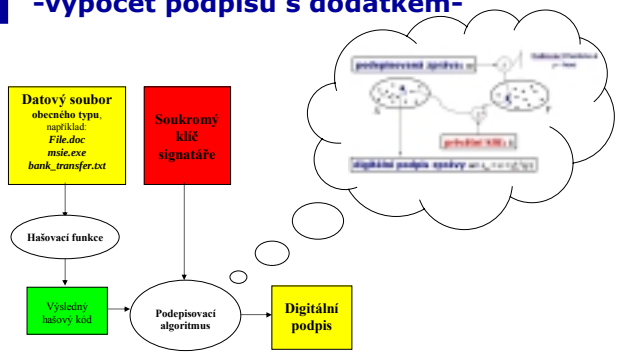
Podpisová schémata
-elementární principy- (2)



Podpisová schémata
-elementární principy- (3)

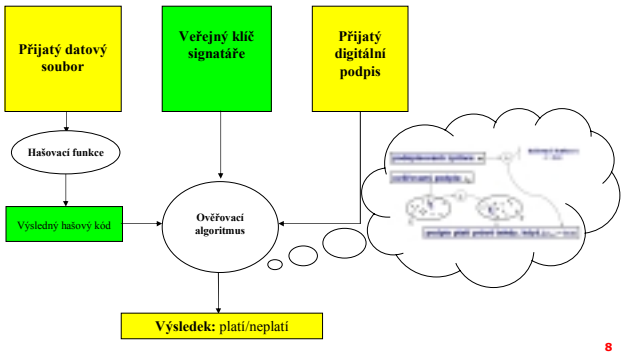


Podpisová schémata
-výpočet podpisu s dodatkem-



7

Podpisová schémata
-ověření podpisu s dodatkem-



8

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 ~ podpis!
- Společný rys:
  - využití jednosměrných funkcí a jednosměrných funkcí s padacími vrátky
  - rozhodující vliv na bezpečnost má způsob kódování šifrované či podepisované zprávy

9

RSA (1)

- Podpisové schéma
  - vystavěno na transformacích RSASP(.) a RSAVP(.)
    - důležité jsou přídavné 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

10

RSA (2)
-podpisové schéma s dodatkem-

- Výpočet podpisu zprávy
  - vstup: privátní klíč RSA (n, d), zpráva pro podpis M (jako binární řetězec)
  - výpočet:
    1. H = hash(M)
       - na úrovni stejných hašových kódů jsou dvě různé zprávy nerozlišitelné
    2. m = ENCODE(H)
    3. s = RSASP((n, d), m)
    4. výsledkem budiž s

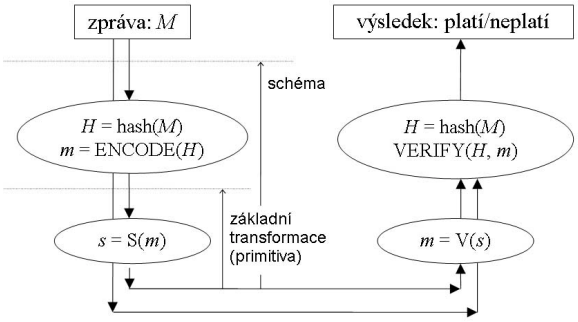
11

RSA (3)
-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 = RSAVP((n, e), s)
    2. H = hash(M)
    3. V = VERIFY(H, m), $V \in$ {platí, neplatí}
    4. výsledkem budiž V

12

RSA (4)
-schéma vs. transformace-



13

Standard PKCS#1 v. 1.5

příklad 1024bitového modulu n				
11001110	.....	.....	.....	.....
kódování EMSA-PKCS1-v1_5				
00000000	00000001	FFF ... FF	00000000	T

$T = ID_{hash} \,||\, hash(m)$, kde *hash* je použitá hašovací funkce a ID_{hash} je její identifikátor

14

DSA (1)

- 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
  - narozdíl od ElGamalu využívá podgrupu prvočíselného řádu q grupy $\boldsymbol{Z}_p^*$, $q|(p-1)$
    - tím předchází hned několika útokům
  - souvisí také se Schnorrovým schématem

15

DSA (2)

- Inicializace schématu
  - vygenerujme náhodné prvočíslo q, $2^{159} < q < 2^{160}$
  - vygenerujme náhodné prvočíslo p, $2^{1023} < p < 2^{1024}$ tak, aby $q|(p-1)$
  - nalezněme generátor α cyklické podgrupy grupy $\boldsymbol{Z}_p^*$ řádu q
  - volme privátní exponent x, $0 < x < q$
  - vypočtěme veřejný klíč y, $y = \alpha^x \bmod p$
  - veřejné parametry schématu jsou (p, q, α)
    - někdy je veřejný klíč uváděn ve tvaru (p, q, α, y)
  - privátní klíč je čtveřice (p, q, α, x)
    - je nutné zajistit integritu čtveřice (p, q, α, x)
    - ačkoliv to tak řada popisů dělá, není vhodné vnímat x samostatně jako privátní klíč

16

DSA (3)

- Podpis zprávy
  - vstup: privátní klíč (p, q, α, x), zpráva pro podpis m, hašovací funkce h (v DSS h=SHA-1)
  - výpočet:
    1. vygenerujme tajné náhodné číslo k, $0 < k < q$
       - parametr k bývá označován jako *dočasný klíč zprávy*
       - kompromitace k vede ke kompromitaci privátního klíče
    2. vypočtěme $r = (\alpha^k \bmod p) \bmod q$
    3. vypočtěme $s = k^{-1}(h(m) + xr) \bmod q$, kde $kk^{-1} \equiv 1 \pmod q$
    4. ověřme, že $r \neq 0$ a $s \neq 0$, jinak se výpočet opakuje
    5. podpisem budiž dvojice (r, s)

17

DSA (4)

- Ověření podpisu
  - vstup: veřejné parametry a klíč (p, q, α, y), zpráva m, ověřovaný podpis (r, s), hašovací funkce h (v DSS h=SHA-1)
  - výpočet:
    1. ověřme, že $0 < r < q$ a $0 < s < q$, jinak podpis odmítneme jako neplatný
    2. vypočtěme $w = s^{-1} \bmod q$
    3. vypočtěme $u_1 = w*h(m) \bmod q$ a $u_2 = r*w \bmod q$
    4. vypočtěme $v = (\alpha^{u1} y^{u2} \bmod p) \bmod q$
    5. podpis prohlásíme za platný iff $v = r$

18

ECDSA

- Algebraické rozšíření DSA
- Namísto $\boldsymbol{Z}_p^*$, respektive její cyklické podgrupy, je použita eliptická křivka $E(\boldsymbol{F}_q)$, 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

19

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
    - trojský kůň – podstrčení dokumentu pro podpis, atp.
    - nedodržení okrajových podmínek použitých kryptografických mechanizmů

20

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!

21

Nepadělatelnost digitálního podpisu

- **Definice (silná).** *Neexistuje zpráva, jejíž podpis je výpočetně schůdné 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
    - trojský kůň...

22

Nepadělatelnost vs. nepopiratelnost

- Nepopiratelnost ⇒ 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

23

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

24

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

25

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

26

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

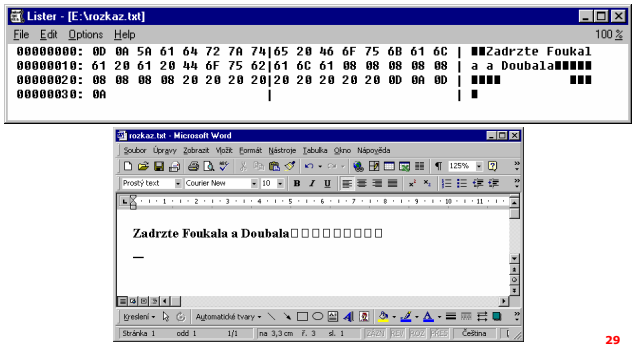
27

Hledání alternativního vysvětlení

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

28

Příklad
–kódování zpráv- (1)



29

Příklad
–kódování zpráv- (2)

30

Nepopiratelnost a fyzické předměty

- Typicky se dnes jedná o čipové karty
  - privátní klíč je uložen na kartě a chráněn mechanizmem 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 podepisovanou zprávu není pod kontrolou čipové karty
  - zpochybnění kvality klíče generovaného na kartě (slabiny (P)RNG)

31

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 autority
  - notářské služby
  - ...

32

Závěr

- Na bezpečnosti digitálního 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

33