ELEKTRONICKÝ OTLAČOK SPRÁVY

HASHING OF MESSAGE

Ladislav Schwartz, Dušan Trstenský
Katedra telekomunikácií, Elektrotechnická fakulta, Žilinská univerzita v Žiline, Veľký Diel, 010 26 Žilina

Abstrakt Na identifikáciu akejkoľvek správy nie je potrebné mať k dispozícií celú správu, ale stačí na jej hodnovernosť jej elektronický otlačok. Elektronický otlačok správy sa používa pri ukladaní hesiel, dešifrovacích kľúčov, autentizácii a elektronickom podpise. Dôležitá je jeho jednocestnosť a odolnosť voči kolíziám. Najbezpečnejšie štandardy pre elektronický otlačok sú SHA-1 a RIPEMD-160.

Summary For identification of any message it is not necessary to have available all message, but it is sufficient for its autentication its hashing. Hashing is used at safe put passwords, decode keys, authentication and electronic signature. Important is its one way and resistance for collisions. Most safety are standards for hashing SHA-1 and RIPEMD-160.

1. ÚVOD

Príkladov použitia funkcií elektronického otlačku správy je mnoho. Ako niektoré príklady možno uviesť Internetovské prehliadače a aplikácie, sieťové programové vybavenie, elektronickú poštu, autentizáciu, digitálny podpis, bezpečnostné protokoly a pod. Vstupom funkcie elektronického otlačku H je dátový súbor M (správa) o premennej a prakticky neobmedzenej dĺžke. Jej výstupom je hodnota elektronického otlačku (kód elektronického otlačku) $H(M)$ pevnej a relatívne veľmi malej dĺžky (väčšinou desiatky až stovky bitov).

Funkcia elektronického otlačku správy plní dve úlohy. Prvou úlohou je „kompresia". Veľmi dlhý vstup (pri funkcii elektronického otlačku SHA-1 až $2^{64} - 1$ bitov!) je „komprimovaný" na veľmi krátky výstup (pri SHA-1 je to 160 bitov). O komprimovaní hovoríme v úvodzovkách preto, že pôvodná informácia nemôže byť v kóde elektronického otlačku obsiahnutá celá, takže z kódu elektronického otlačku správy nie je možné obnoviť pôvodnú správu.

Druhou úlohou je vlastný elektronický otlačok správy, teda „zomletie" vstupných dát. Výstupné dáta sú skutočne akýmsi vzorkom „zomletých" vstupných dát. Hodnota elektronického otlačku správy je výťažkom z takto získaného produktu, čo stačí na posúdenie celku.

U človeka by hodnote elektronického otlačku mohol zodpovedať napríklad otlačok prsta, genetický kód alebo snímok dúhovky oka. Dôležité je si uvedomiť dôležitú vlastnosť, že z otlačku prsta nie je možné človeka vytvoriť, ale je možné ho jednoznačne identifikovať.

Aby funkcie elektronického otlačku správy správne pracovali, musia spĺňovať nasledujúce požiadavky:

Jednocestnosť:

- ak je dané M, je jednoduché vypočítať $H(M)$,
- ak je dané $H(M)$, je veľmi ťažké (rozumej: výpočtovými prostriedkami prakticky nevykonateľné) vypočítať M,
- ak je dané M, je veľmi ťažké nájsť M' tak, aby $H(M)=H(M')$.

Odolnosť proti kolízii:

- je veľmi ťažké nájsť akékoľvek (teda i náhodné) rôzne M a M' tak, aby $H(M)=H(M')$, t.j. aby došlo k takzvanej kolízii.

Pokiaľ si tieto vlastnosti z modelu „správa – elektronický otlačok" prenesieme do situácie „človek – otlačok prsta" dostaneme tieto bezpečnostné požiadavky vo veľmi zrozumiteľnej forme:

Jednocestnosť:

- otlačok prsta je možné získať ľahko,
- ak máme otlačok prsta, je ťažké (prakticky nemožné) z neho zrekonštruovať jeho nositeľa,
- ak máme k dispozícii nejakého konkrétneho človeka, je ťažké k nemu nájsť iného s rovnakým otlačkom prsta.

Odolnosť proti kolízii:

- je veľmi ťažké nájsť akýchkoľvek dvoch ľudí, ktorí by mali rovnaký otlačok prsta.

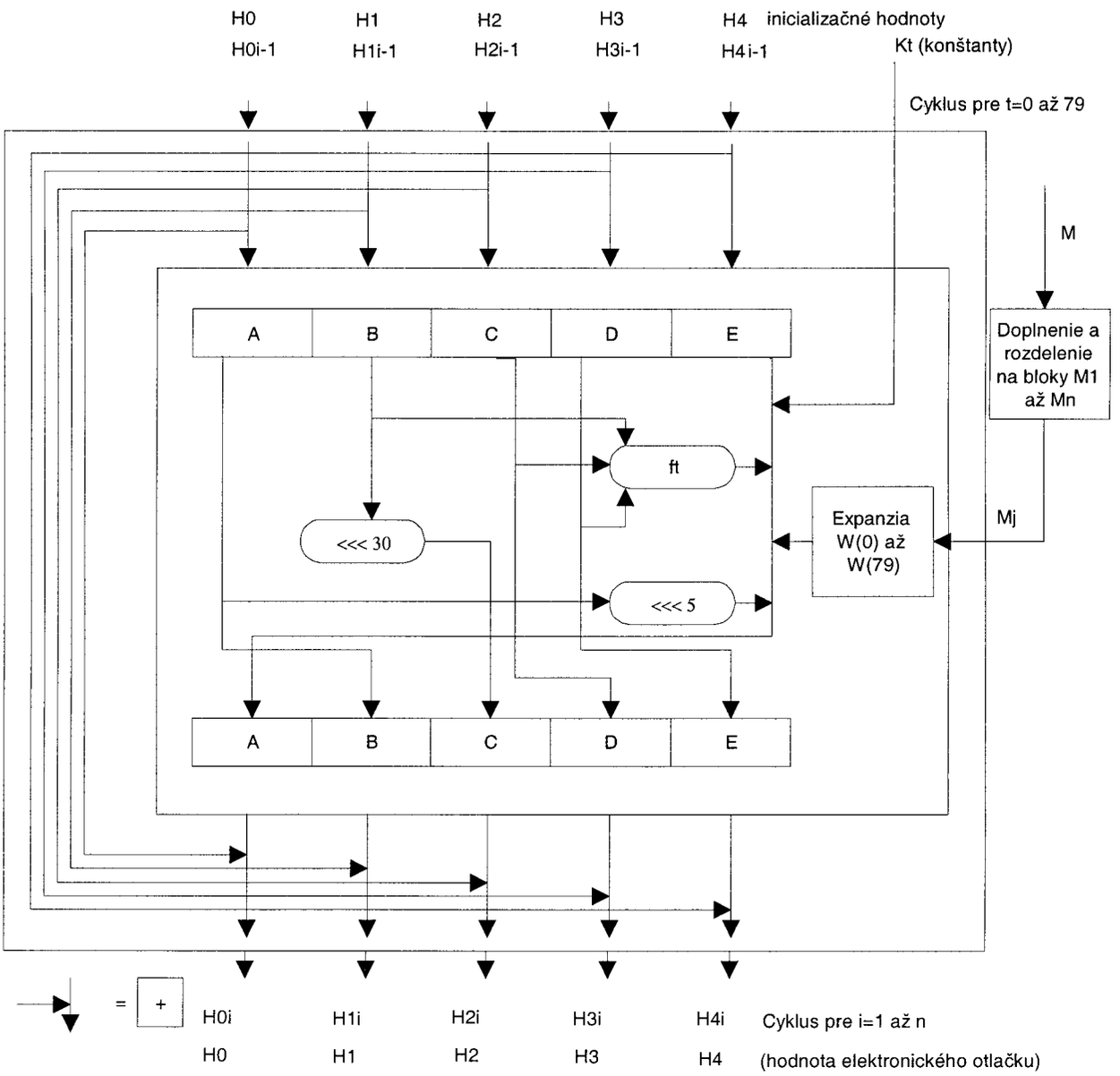
Digitálny podpis správy M sa až na výnimky uskutočňuje tak, že sa digitálne podpisuje len výťah správy, t.j. najprv sa vypočíta hodnota elektronického otlačku správy $H(M)$, a na tú sa potom aplikuje digitálny podpis.

2. OPIS SHA-1

SHA-1 (Secure Hash Algorithm) bol navrhnutý ako štandardná funkcia elektronického otlačku správy so vstupom od 0 až do $2^{64} - 1$ bitov a výstupom 160 bitov [1] . SHA-1 je americký štandard.

Doplnenie správy

Predpokladajme, že máme správu M, ktorá má m bitov. SHA-1 spracováva bloky dát po 512 bitoch, takže najprv dôjde k doplneniu správy M na dĺžku, ktorá je celočíselným násobkom 512 bitov. Doplnenie sa robí v každom prípade a je definované tak, že M sa najprv doplní jedničkovým bitom a potom 0 až 511 nulovými bitmi tak, aby dĺžka správy bola rovná $512.(n - 1) + 448$, kde n je vhodné prirodzené číslo. Zvyšujúcich 64 bitov bude doplnených 64 bitovým číslom, ktoré vyjadruje počet bitov pôvodnej správy (m). Poznamenajme, že prázdna správa má $m = 0$ bitov a doplňuje sa rovnakým spôsobom ako každá iná. Takto vždy vznikne n 512 bitových blokov dát, ktoré označíme $M1$ až Mn



Obr. 1 Funkcie elektronického otlačku správy pre SHA-1
Fig. 1 Functions of hashing for SHA-1

Logické funkcie a konštanty

V ďalšom opise budeme pracovať s 32 bitovými slovami (ďalej len slová) *A* až *E* a *TEMP*, konštantami *H0* až *H4*, *K0* až *K79* a funkciami *f0* až *f79*.

Vstupom každej funkcie *ft*, kde $0 \leq t \leq 79$, sú tri slová *B, C, D*. Výstupom *ft* je slovo definované takto:

ft(B,C,D) = (B AND C) OR ((NOT B) AND D)
pre $0 \leq t \leq 19$,

ft(B,C,D) = B XOR C XOR D pre $20 \leq t \leq 39$,

ft(B,C,D) = (B AND C) OR (B AND D) OR (C AND D)
pre $40 \leq t \leq 59$,

ft(B.C.D) = B XOR C XOR D pre $60 \leq t \leq 79$.

Ďalej sa využívajú konštanty *K0* až *K79*, ktoré sú v hexadecimálnom tvare rovné:

Kt = 5A827999 pre $0 \leq t \leq 19$,

Kt = 6ED9EBA1 pre $20 \leq t \leq 39$,

Kt = 8F1BBCDC pre $40 \leq t \leq 59$,

Kt = CA62C1D6 pre $60 \leq t \leq 79$.

Ďalej označme „*W <<< s*“ ako cyklickú rotáciu slova *W* o *s* bitov doľava. Výpočet hodnoty elektronického otlačku správy sa vykonáva postupným spracovaním blokov *M1* až *Mn*, ako je uvedené ďalej.

Hlavná slučka

Spracovanie blokov *Mi* ($i = 1$ až n) sa vykonáva v piatich krokoch:

a) *Mi* rozdelíme na 16 slov *W(0)* až *W(15)*,

b) Vykonáme expanziu na slová *W(16)* až *W(79)*:
W(t) = (W(t – 3) XOR W(t – 8) XOR W(t – 14) XOR W(t – 16)) <<< 1,

c) Do *A* až *E* skopírujeme posledné hodnoty slov *H0* až *H4*: *A = H0, B = H1, C = H2, D = H3, E = H4*,

d) V nasledujúcich 80-ich prechodoch ($t = 0, \ldots 79$) k slovám *A* až *E* primiešavame slova *W* podľa symbolického zápisu:

$TEMP = (A <<< 5) + ft(B,C,D) + E + W(t) + Kt$
$E = D$
$D = C$
$C = B <<< 30$
$B = A$
$A = TEMP,$

e) Aktualizujeme hodnoty *H0* až *H4* podľa vzťahov: $H0 = H0 + A$, $H1 = H1 + B$, $H2 = H2 + C$, $H3 = H3 + D$, $H4 = H4 + C$.

Po spracovaní posledného bloku *Mn* je hodnota elektronického otlačku správy definovaná ako 160 bitový reťazec tvorený slovami *H0* až *H4*.

3. ZÁVER

Funkcií elektronického otlačku správy existujú desiatky. Najrozšírenejšie sú tri hlavné triedy: MD-x, RIPEMD-x, SHA-x, kde x označuje príslušnú verziu.

MD2 bola zabudnutá, MD4 zavrhnutá z bezpečnostného hľadiska (kolízie) a taktiež MD5 sa neodporúča používať pre digitálne podpisy.

V Európe bola navrhnutá funkcia elektronického otlačku správy RIPEMD-160 s 160 bitovým kódom. Tiež boli navrhnuté funkcie RIPEMD-128 pre prípady kde nie je možné použiť 160 bitový kód, a RIPEMD-256 a RIPEMD-320 pre prípady, kde sa vyžaduje ešte väčšia bezpečnosť.

V USA bola navrhnutá SHA-1, ktorá odstraňuje nedostatok SHA-0.

Tab. 1 Vlastnosti elektronických otlačkov správy
Tab. 1 Characteristics of hashing.of message

Funkcie elektronického otlačku	MD2	MD4	MD5	RIPEMD	RIPEMD--128	RIPEMD--160	SHA-0	SHA-1
Kód elektronického otlačku	128 bitov	128 bitov	128 bitov	128 bitov	128 bitov	160 bitov	160 bitov	160 bitov
Bezpečnosť	Kolízia kompresnej funkcie, malá dĺžka kódu	Kolízia celej MD4, malá dĺžka kódu	Kolízia kompresnej funkcie, malá dĺžka kódu	Malá dĺžka kódu	Malá dĺžka kódu	Bezpečná	Kolízia kompresnej funkcie, (ale vysoká zložitosť nájdenia – 2^{61}	Bezpečná
Poznámka				2 paralelné línie	2 paralelné línie	2 paralelné línie		

LITERATÚRA

[1] Klíma, V.: Výživná haše. CHIP 3/1999

[2] Klíma, V.: Jak se melou data. CHIP 4/1999

[3] Hottmar, V., Tichá D.: Architektúry výpočtových systémov pre ITKR. TKR – QUO VADIS? 01, Konferencia so zahraničnou účasťou, Žilina 2001, Zborník str. 104 – 112, ISBN 80-7100-826-5

[4] Hottmar, V., Neuschl Š.: Modelovanie výpočtového systému pomocou teórie hromadnej obsluhy. ISTEP 2000, International SYMPOSIUM on Telemedicine and Teleeducation in Practice, Zborník 22-24, March 2000, Košice, str. 147 – 152, ISBN 80-88964-38-5

[5] Čepčianký, G.: Hodnotenie technickej akosti digitálnej siete. Telekomunikace. 4/1995