Karel Kohout
(karel.kohout@centrum.cz)

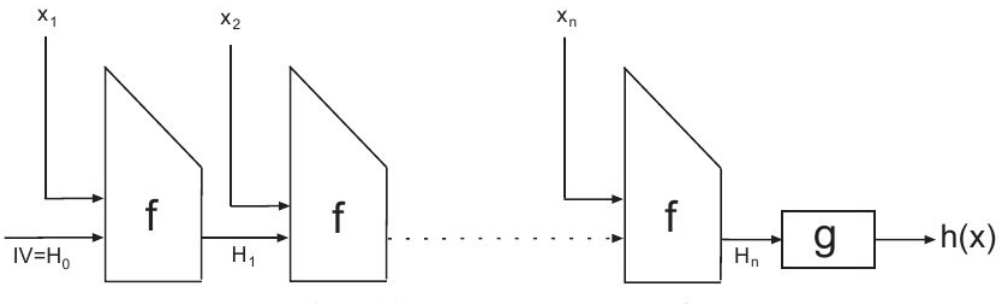
Vybrané útoky proti hašovací funkci MD5

1 Úvod, vymezení

V práci popisuji vybrané útoky proti bezpečnosti hašovací funkce MD5. Nejdříve uvádím zjednodušený algoritmus MD5 a následně rozebírám jednotlivé teoretické a praktické slabiny funkce. Nerozebírám teoretické předpoklady hašovacích funkcí.

2 Popis MD5

MD5[1] je algoritmus optimalizovaný pro 32 bitové procesory, vychází z MD4 (oproti MD4 je mírně pomalejší). Převádí řetězec libovolné délky na řetězec o délce 128 bitů. V algoritmu proběhne nejdříve doplnění zprávy, příprava inicializačního vektoru (čtyři 32bitová slova A, B, C, D) a následně je zpráva podle Merkle-Damgårdova schématu zpracována po blocích o velikosti 512 bitů.



Obrázek 1: Merkle-Damgårdovo schéma (struktura) (zdroj: [4, str. 200]); x_i jsou pro MD5 bloky o 512 bitech, H_i řetězce o délce 128 bitů a $h(x)$ výsledný hash.

Doplnění zprávy probíhá probíhá následovně: nejdříve je připojen jeden bit 1 a následně množství 0 tak, aby délka zprávy byla kongruentní s 448 modulo 512 (k doplnění dochází i v případě, že zpráva již podmínku splňuje). Následně je připojena do posledních 64 bitů délka zprávy (v případě délky větší než 2^{64} je použito pouze spodních 64 bitů).

Inicializační vektor – buffer je pevně stanovený:

A :	01	23	45	67
B :	89	ab	cd	ef
C :	fe	dc	ba	98
D :	76	54	32	10

[1] Message-Digest algorithm 5