Criptografie și Securitate

- Prelegerea 14.2 -
Message Digest 5 - MD5

Adela Georgescu, Ruxandra F. Olimid

Facultatea de Matematică și Informatică
Universitatea din București

Cuprins

Informații generale

MD5 este:

- definit în 1991 de R.Rivest ca înlocuitor pentru MD4
- publicat ca standard internet RFC1321 în 1992
- face parte dintr-o familie de funcții hash: MD2, MD4, MD6 (finalist SHA-3)
- realizat pentru calculatoarele pe 32-biți
- utilizat pentru stocarea parolelor în versiuni mai vechi de Moodle sau pentru a asigura integritatea fișierelor la download sau transfer

Descriere

- MD5 este o funcție hash cu ieșirea pe 128 biți:

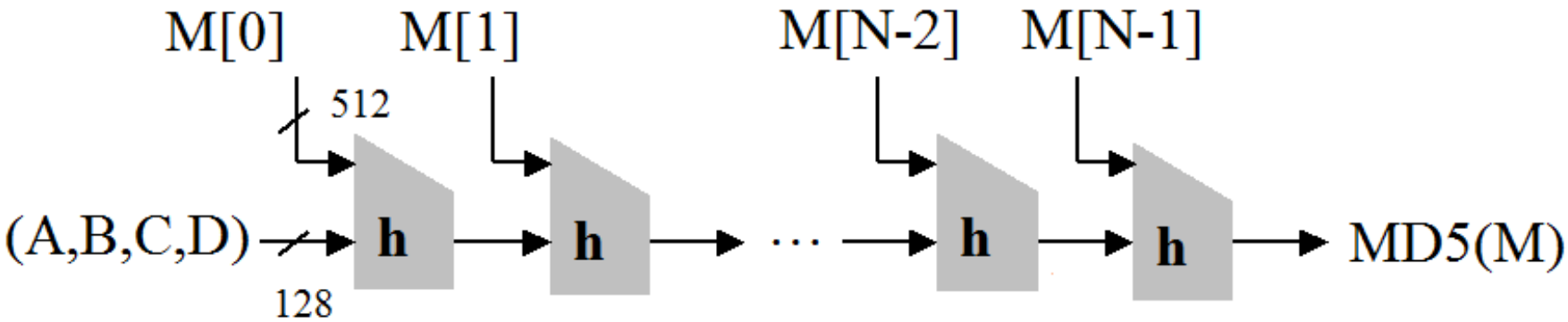
$$MD5 : \{0,1\}^* \rightarrow \{0,1\}^{128}$$

Descriere

- MD5 este o funcție hash cu ieșirea pe 128 biți:

$$MD5 : \{0,1\}^* \rightarrow \{0,1\}^{128}$$

- Folosește construcția Merkle-Damgård pentru blocuri de 512 biți și vector de inițializare de 128 biți:



Descriere

- Presupune 5 pași:
  - **Pas 1**: Padding
  - **Pas 2**: Concatenarea lungimii mesajului
  - **Pas 3**: Inițializarea buffer-ului MD
  - **Pas 4**: Procesarea mesajului
  - **Pas 5**: Ieșirea

Descriere

Pas 1. Padding

- Mesajul de intrare este spart în blocuri de 512 biți :

$$M[0], M[1], \ldots, M[N-2]$$

Descriere

Pas 1. Padding

- Mesajul de intrare este spart în blocuri de 512 biți :

$$M[0], M[1], \ldots, M[N-2]$$

- Ultimul bloc $M[N-1]$ este completat până la 448 biți cu secvența :

$$100\ldots0$$

Descriere

Pas 1. Padding

- Mesajul de intrare este spart în blocuri de 512 biți :

$$M[0], M[1], \ldots, M[N-2]$$

- Ultimul bloc $M[N-1]$ este completat până la 448 biți cu secvența :

$$100\ldots0$$

- Padding-ul se realizează întotdeauna, chiar dacă (din întâmplare) ultimul bloc are exact 448 biți.

Descriere

Pas 2. Concatenarea lungimii mesajului

- Lungimea mesajului (în biți) se reprezintă pe 64 de biți;

Descriere

Pas 2. Concatenarea lungimii mesajului

- Lungimea mesajului (în biți) se reprezintă pe 64 de biți;
- În cazul (foarte puțin probabil!) că lungimea $\geq 2^{64}$, se folosesc numai ultimii 64 biți din reprezentarea binară;

Descriere

Pas 2. Concatenarea lungimii mesajului

- Lungimea mesajului (în biți) se reprezintă pe 64 de biți;
- În cazul (foarte puțin probabil!) că lungimea $\geq 2^{64}$, se folosesc numai ultimii 64 biți din reprezentarea binară;
- Rezultatul se concatenează la ultimul bloc $M[N-1]$, care devine complet (512 biți);

Descriere

Pas 2. Concatenarea lungimii mesajului

- Lungimea mesajului (în biți) se reprezintă pe 64 de biți;
- În cazul (foarte puțin probabil!) că lungimea $\geq 2^{64}$, se folosesc numai ultimii 64 biți din reprezentarea binară;
- Rezultatul se concatenează la ultimul bloc $M[N-1]$, care devine complet (512 biți);
- Mesajul rezultat conține numai blocuri de 512 biți:

$$M[0], M[1], \ldots, M[N-1]$$

Descriere

Pas 3. Inițializarea buffer-ului MD

- Inițializarea construcției Merkle-Damgård necesită un vector de inițializare pe 128 biți;

Descriere

Pas 3. Inițializarea buffer-ului MD

- Inițializarea construcției Merkle-Damgård necesită un vector de inițializare pe 128 biți;
- Acesta este sub forma unui buffer de 4 word-uri (A, B, C, D), care va prelua valori intermediare după fiecare transformare a unui bloc:

Descriere

Pas 3. Inițializarea buffer-ului MD

- Inițializarea construcției Merkle-Damgård necesită un vector de inițializare pe 128 biți;
- Acesta este sub forma unui buffer de 4 word-uri (A, B, C, D), care va prelua valori intermediare după fiecare transformare a unui bloc:
- Inițializarea se face la valorile indicate:

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

Descriere

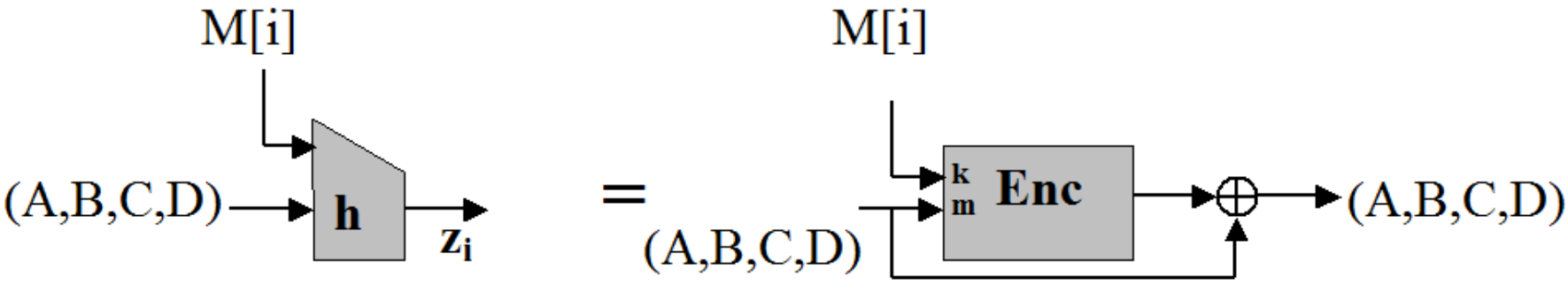
Pas 4. Procesarea mesajului

- Procesarea mesajului se realizează în blocuri de câte 16 word-uri;

Descriere

Pas 4. Procesarea mesajului

- Procesarea mesajului se realizează în blocuri de câte 16 word-uri;
- Compresia este de fapt o construcție Davies-Meyer unde adunarea se face modulo 2^{32}:



Descriere

Pas 4. Procesarea mesajului

- Se definesc 4 funcții auxiliare:

F(X,Y,Z) = dacă X, atunci Y; altfel Z
G(X,Y,Z) = dacă Z, atunci X; altfel Y
H(X,Y,Z) = X xor Y xor Z
I(X,Y,Z) = Y xor (X and (not Z))

Descriere

Pas 4. Procesarea mesajului

- Se definesc 4 funcții auxiliare:

  F(X,Y,Z) = dacă X, atunci Y; altfel Z
  G(X,Y,Z) = dacă Z, atunci X; altfel Y
  H(X,Y,Z) = X xor Y xor Z
  I(X,Y,Z) = Y xor (X and (not Z))

- Se definește o tabelă calculată folosind funcția *sin*:

$$T[i] = 4294967296 \cdot abs(sin(i))$$

Descriere

Pas 4. Procesarea mesajului

- Funcția de criptare din construcția Davies-Meyer este constituită din 4 runde;

Descriere

Pas 4. Procesarea mesajului

- Funcția de criptare din construcția Davies-Meyer este constituită din 4 runde;
- Fiecare rundă folosește una dintre funcțiile auxiliare F, G, H, I;

Descriere

Pas 4. Procesarea mesajului

- Funcția de criptare din construcția Davies-Meyer este constituită din 4 runde;
- Fiecare rundă folosește una dintre funcțiile auxiliare F, G, H, I;
- Pentru exemplificare, introducem prima rundă:

```
/* Round 1. */
/* Let [abcd k s i] denote the operation
     a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s). */
/* Do the following 16 operations. */
[ABCD  0  7  1]  [DABC  1 12  2]  [CDAB  2 17  3]  [BCDA  3 22  4]
[ABCD  4  7  5]  [DABC  5 12  6]  [CDAB  6 17  7]  [BCDA  7 22  8]
[ABCD  8  7  9]  [DABC  9 12 10]  [CDAB 10 17 11]  [BCDA 11 22 12]
[ABCD 12  7 13]  [DABC 13 12 14]  [CDAB 14 17 15]  [BCDA 15 22 16]
```

[RFC1321]

Descriere

Pas 5. Ieșirea

- Valoarea funcției hash este dată de valoarea finală a bufferului (după aplicarea transformării Merkle-Damgård pe întreg mesajul M):

$$MD5(M) = ABCD$$

Securitate

- "Atacul zilei de naștere" asupra MD5 necesită numai $\approx 2^{128/2} = 2^{64}$ evaluări;

Securitate

- "Atacul zilei de naștere" asupra MD5 necesită numai $\approx 2^{128/2} = 2^{64}$ evaluări;
- În 1996, au fost determinate coliziuni în MD5:

"The presented attack does not yet threaten practical applications of MD5, but it comes rather close. In view of the flexibility of the new analytic techniques it would be unwise to assume that the attack could not be improved."

(Hans Dobbertin: The Status of MD5 After a Recent Attack, RSA Laboratories' CryptoBytes vol.2, no.2, 1996)

Securitate

- Și într-adevăr, MD5 devine inutilizabil în practică...

Securitate

- Și într-adevăr, MD5 devine inutilizabil în practică...
- MD5 era folosit pentru a asigura integritatea fișierelor la descărcare;

Securitate

- Și într-adevăr, MD5 devine inutilizabil în practică...
- MD5 era folosit pentru a asigura integritatea fișierelor la descărcare;
- Serverul pune la dispoziția utilizatorului o valoare MD5 precalculată corespunzătoare fișierelor descărcate (*md5sum*);

Securitate

- Și într-adevăr, MD5 devine inutilizabil în practică...
- MD5 era folosit pentru a asigura integritatea fișierelor la descărcare;
- Serverul pune la dispoziția utilizatorului o valoare MD5 precalculată corespunzătoare fișierelor descărcate (*md5sum*);
- Utilizatorul primește fișierele, calculează valoarea hash MD5 și verifică dacă este identică celei inițiale;

Securitate

- Și într-adevăr, MD5 devine inutilizabil în practică...
- MD5 era folosit pentru a asigura integritatea fișierelor la descărcare;
- Serverul pune la dispoziția utilizatorului o valoare MD5 precalculată corespunzătoare fișierelor descărcate (*md5sum*);
- Utilizatorul primește fișierele, calculează valoarea hash MD5 și verifică dacă este identică celei inițiale;
- Această utilizare nu mai este sigură în practică:

> *"Two researchers from the Institute for Cryptology and IT-Security have generated PostScript files with identical MD5-sums but entirely different (but meaningful!) content."*
>
> (Bruce Schneier: Schneier on Security, 10 iunie 2005)

Important de reținut!

- MD5 NU este o funcție hash sigură!