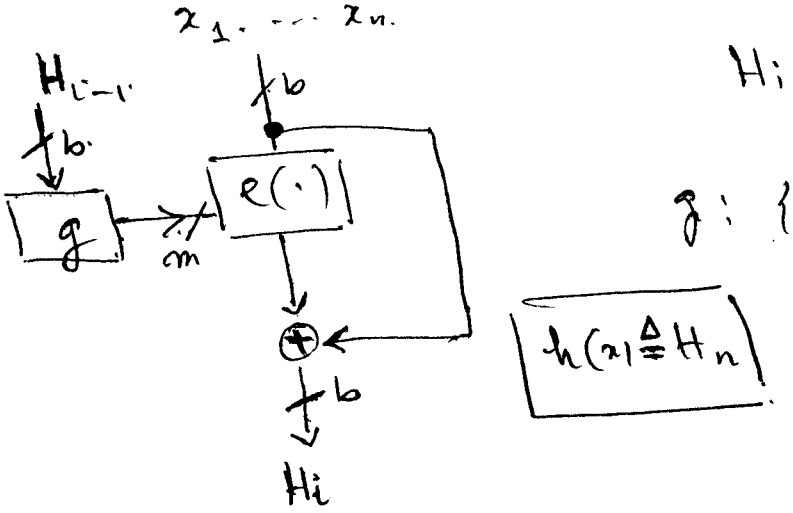
(A.) Dédié :

- Famille MD4 ; spécialement MD5 (Rivest).
- Famille (SHA) : Secure Hach Algorithm pour remplacer MD4. ; SHA1 très utilisé actuellement.

voir page 307 de Paar et al où SHA1 est étudiée en détail. (resumée au réseau de Ficstel).

(B). $x = x_1 \dots x_n$ (blocs de taille fixe b)



$$H_i = e_{g(H_{i-1})}(x_i) \oplus x_i$$

$$g : \{0,1\}^b \longrightarrow \{0,1\}^m$$

$h(x) \triangleq H_n$

$e(\cdot)$ cryptage par DES, AES, ...

- Il existe plusieurs variantes (page 306 de Paar et al).