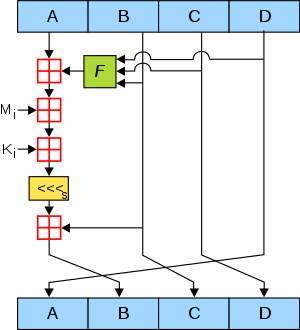
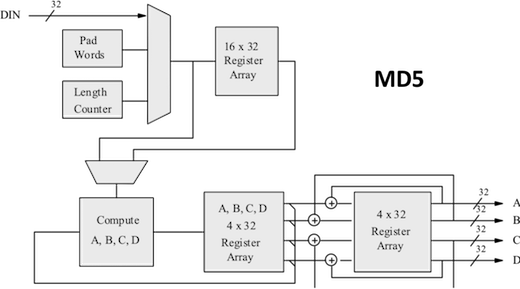
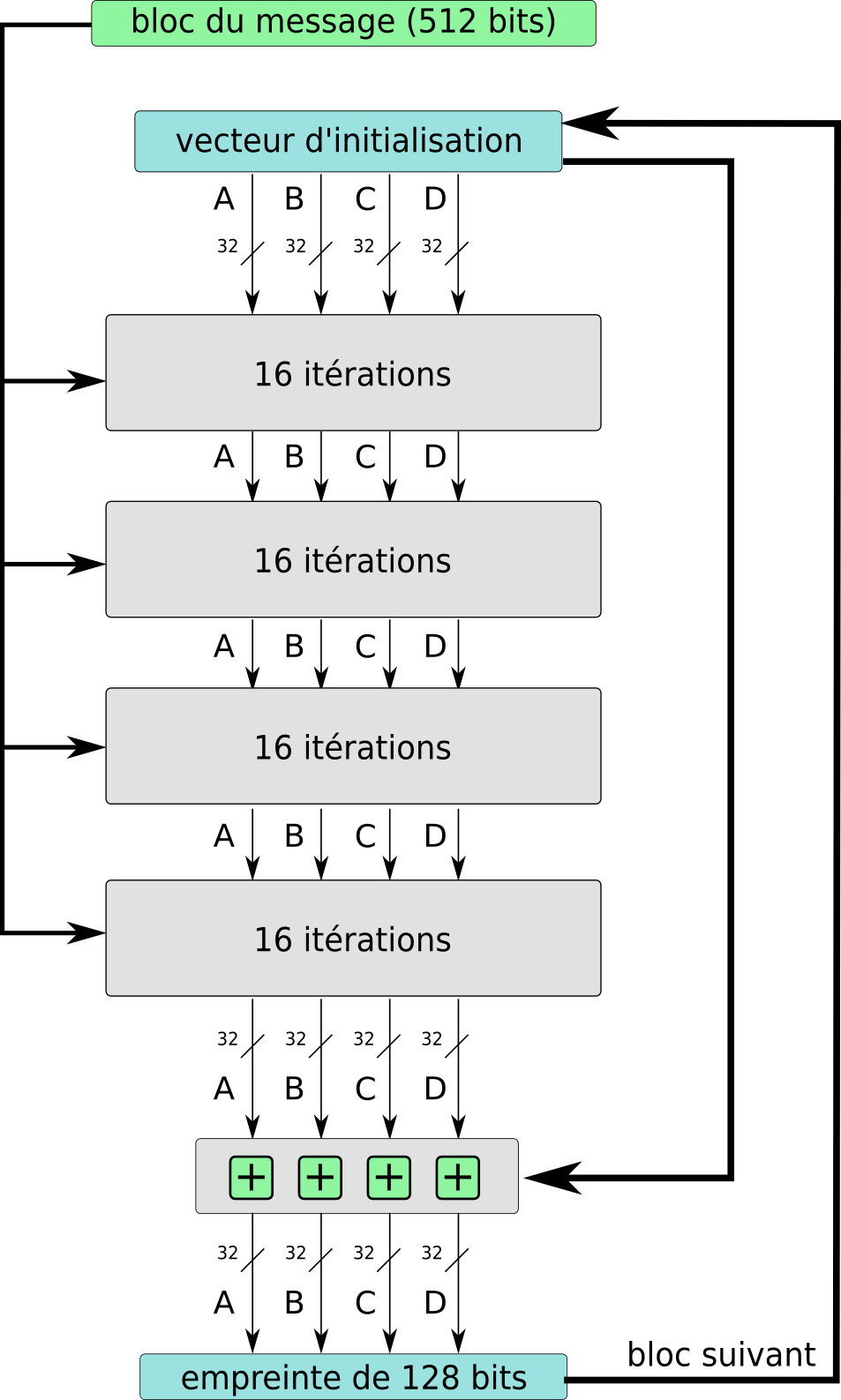
MD5 Recherche

https://www.ietf.org/rfc/rfc1321.txt

# Schéma

http://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/md5





# Etape

## STEP 1

Message à taille variable,

Bloc initial de **512** bits

* Partie du message en binaire sur **64** bits
* 1
* 0 pour que le message étendu atteigne 448 modulo 512

Fait x fois pour avoir tout le message 🡪 tération sur chaque bloc

## STEP 2

4 buffers A, B, C, D de **32** bits

* A ⬄ 01234567
* B ⬄ 89abcdef
* C ⬄ fedcba98
* D ⬄ 76543210

4 fonctions

* F(X,Y,Z) = (X AND Y) OR (not(X) AND Z)
* G(X,Y,Z) = (X AND Z) OR (Y AND not(Z))
* H(X,Y,Z) = X xor Y xor Z
* I(X,Y,Z) = Y xor (X OR not(Z))

Calcul de T[i] partie entière de 4294967296 × abs(sin(i)) pour i de 0 à 15 ; 4294967296 ⬄ 232

Calcul de X pour la rotation **COMMENT**

## STEP 3 : à chaque bloc

* 1. scindage

divise en 16 blocs de 32 bits dans M[i]

* 1. Modification des buffers

4 rondes de 16 étapes

Utilisation des fonctions

* 1. Bla bla

## STEP X

final de **128** bits par la concaténation de chaque buffer