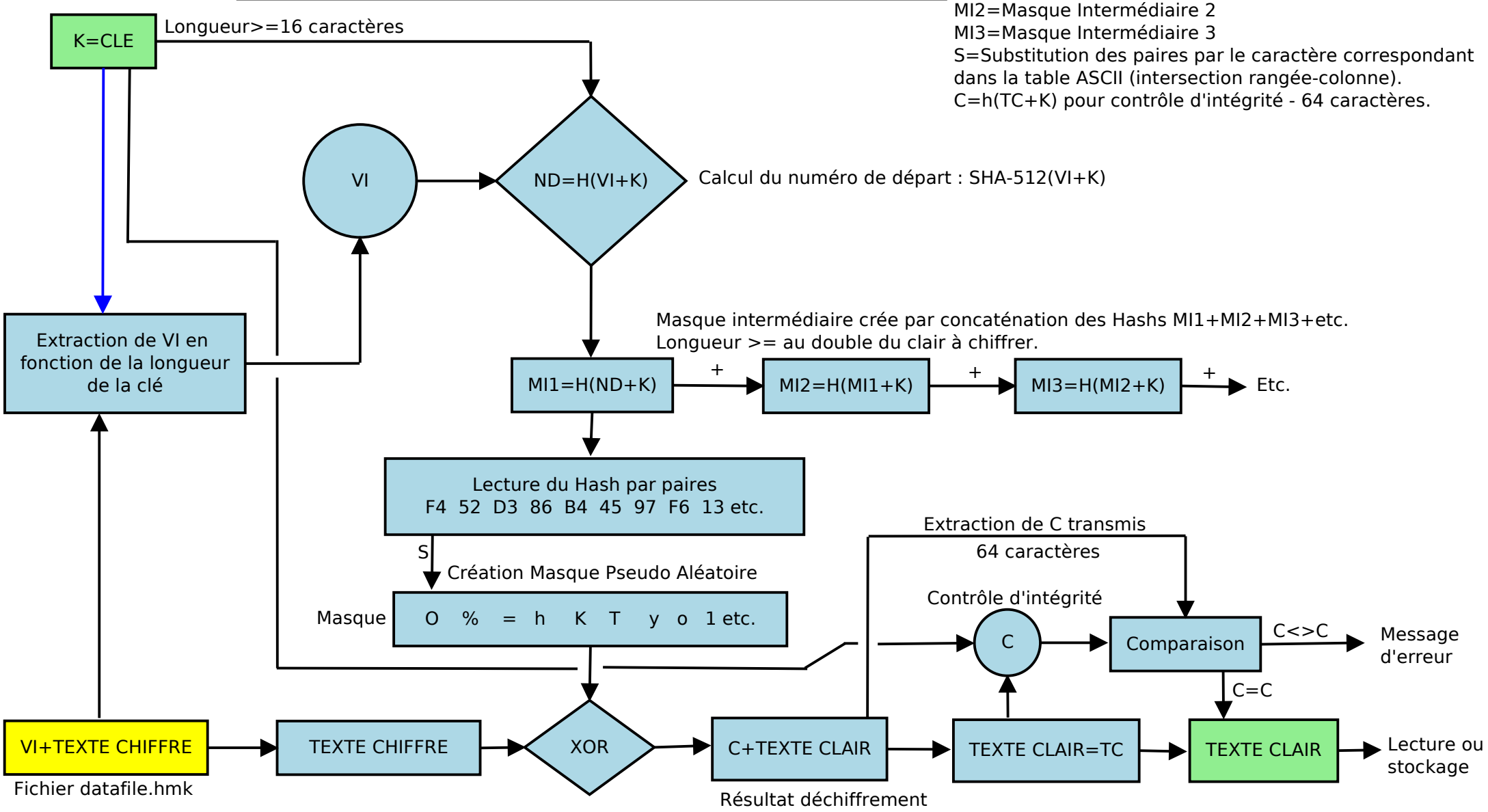
HMK v.03
Philippe Lheureux & Dimitri Mestdagh
Schéma de principe déchiffrement

LEGENDE
h = SHA-256
H= SHA-512
ND=Numéro de Départ.
+=Concaténé avec.
VI=Vecteur d'initialisation de longueur=longueur de la clé.
MI1=Masque Intermédiaire 1
MI2=Masque Intermédiaire 2
MI3=Masque Intermédiaire 3
S=Substitution des paires par le caractère correspondant dans la table ASCII (intersection rangée-colonne).
C=h(TC+K) pour contrôle d'intégrité - 64 caractères.



16-05-2012