NORME INTERNATIONALE

ISO/CEI 10116

Première édition
1991-09-01

Technologies de l'information — Modes opératoires d'un algorithme de chiffrement par blocs de *n*-bits

Information technology — Modes of operation for an n-bit block cipher algorithm

Numéro de référence
ISO/CEI 10116:1991(F)

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment ensemble un système consacré à la normalisation internationale considérée comme un tout. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement des Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des différents domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales ou non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux.

Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour approbation, avant leur acceptation comme Normes internationales. Les Normes internationales sont approuvées conformément aux procédures qui requièrent l'approbation de 75 % au moins des organismes nationaux votants.

La Norme internationale ISO/CEI 10116 a été élaborée par le comité technique ISO/CEI JTC 1, *Technologies de l'information*.

Les annexes A à C de la présente Norme internationale sont données uniquement à titre d'information.

Technologies de l'information — Modes opératoires d'un algorithme de chiffrement par blocs de *n*-bits

1 Domaine d'application

La présente Norme internationale décrit quatre modes opératoires d'un algorithme de chiffrement par blocs de *n*-bits.

NOTE 1 L'annexe A (informative) contient des commentaires sur les caractéristiques de chaque mode.

La présente Norme internationale définit quatre modes opératoires tels que, dans le cadre d'applications d'un algorithme de chiffrement par blocs de *n*-bits (par ex. protection de transmission de données, stockage de données, authentification), la présente Norme internationale constitue une référence utile pour, par exemple, la spécification du mode opératoire et les valeurs des paramètres (selon le cas).

Pour certains modes, un remplissage peut être nécessaire pour assurer que toutes les variables du texte clair ont la longueur nécessaire. Les techniques de remplissage ne sont pas du domaine de la présente Norme internationale.

NOTE 2 Deux paramètres, *j* et *k*, sont définis pour le mode opératoire (voir article 6) par rebouclage du cryptogramme (CFB). Un seul paramètre, *j*, est défini pour le mode par rebouclage (voir article 7) de la sortie (OFB). Lorsqu'on utilise un de ces modes opératoires, la ou les valeurs des paramètres doivent être choisies et employées par toutes les parties qui communiquent.

2 Définitions

Pour les besoins de la présente Norme internationale, les définitions suivantes s'appliquent.

2.1 texte clair : Informations non chiffrées.

2.2 cryptogramme ou texte chiffré : Informations chiffrées.

2.3 algorithme de chiffrement par blocs de *n*-bits : Algorithme de chiffrement par blocs avec la particularité que les blocs de texte clair et les blocs de texte chiffrés ont une longueur de *n*-bits.

2.4 chaînage de blocs : Chiffrement d'information où chaque bloc de texte chiffré dépend du bloc de texte chiffré précédent.

2.5 valeur initiale (*IV*) : Valeur qui sert à définir le point de départ d'un processus de chiffrement.

2.6 variable de départ (*SV*) : Variable découlant de la valeur initiale et utilisée pour définir le point de départ des modes opératoires.

NOTE 3 La méthode permettant de calculer la variable de départ à partir de la valeur initiale n'est pas définie dans la présente Norme internationale. Elle doit être décrite dans toute application des modes opératoires.

2.7 synchronisation cryptographique : Coordination des processus de chiffrement et de déchiffrement.

3 Notation

Pour les besoins de la présente Norme internationale, la relation fonctionnelle définie par l'algorithme de chiffrement par blocs s'écrit

$$C = eK(P)$$

où

P est le bloc de texte clair ;

C est le bloc de texte chiffré ;

K est la clé.

L'expression eK est l'opération de chiffrement utilisant la clé K.

La fonction de déchiffrement correspondante s'écrit :

$$P = dK(C)$$

Une variable désignée par une lettre majuscule comme P et C ci-dessus, représente un vecteur de bits, par exemple,

$$A = (a_1, a_2, ..., a_m) \text{ et } B = (b_1, b_2, ..., b_m)$$

c'est-à-dire des vecteurs de m bits, numérotés de 1 à m. Dans tous les vecteurs de bits, le bit le plus significatif est à gauche.

L'opération d'addition, modulo 2, également appelée fonction «OU exclusif» est représentée par le symbole ⊕. Appliquée à des vecteurs comme A et B, l'opération se définit comme

$$A \oplus B = (a_1 \oplus b_1, a_2 \oplus b_2, ..., a_m \oplus b_m)$$

L'opération qui consiste à sélectionner les j bits les plus à gauche de A pour générer un vecteur de j bits s'écrit

$$A \sim j = (a_1, a_2, ..., a_j)$$

Cette opération est définie seulement quand $j \leq m$, m étant le nombre de bits de A.

Une «fonction de décalage» S_K se définit comme suit :

Considérant une variable X de m bits et une variable F de k bits avec $k \leq m$, l'effet d'une fonction de décalage $S_K(X|F)$ est de produire la variable de m bits :

$$S_k(X\,/\,F) = (x_{k+1}, x_{k+2}, ..., x_m, f_1, f_2, ..., f_k) \qquad (k < m)$$

L'effet résultant est de décaler de k positions vers la gauche les bits du vecteur X, supprimant $x_1 ... x_k$ et de placer le vecteur F dans les k positions les plus à droite de X. Lorsque $k = m$ l'effet est de remplacer totalement X par F.

On utilise un cas particulier de cette fonction qui commence avec la variable de m bits $I(m)$ constituée de m bits «1» successifs et on décale la variable F de k bits dans la précédente, avec la relation $k \leq m$.

Le résultat est

$$S_k(I(m) \mid F) = (1, 1, ..., 1, f_1, f_2, ..., f_k) \qquad (k < m)$$

$$S_k(I(m) \mid F) = (f_1, f_2, ..., f_k) \qquad (k = m)$$

où les $m - k$ bits les plus à gauche sont égaux à «1».

4 Mode dictionnaire (ECB)

4.1 Les variables utilisées pour le mode de chiffrement ECB sont

a) Une suite de q blocs de texte clair $P_1, P_2, ..., P_q$, chacun de n bits.

b) Une clé K.

c) La suite résultante de q blocs de texte chiffré $C_1, C_2, ..., C_q$, chacun de n bits.

4.2 Le chiffrement en mode ECB se décrit comme suit :

$$C_i = eK(P_i) \text{ pour } i = 1, 2, ..., q \qquad ... (1)$$

4.3 Le mode ECB de déchiffrement se décrit comme suit :

$$P_i = dK(C_i) \text{ pour } i = 1, 2, ..., q \qquad ... (2)$$

5 Mode chaînage de blocs chiffrés (CBC)

5.1 Les variables utilisées avec le mode de chiffrement CBC sont

a) Une suite de q blocs de texte clair $P_1, P_2, ..., P_q$, chacun de n bits.

b) Une clé K.

c) Une variable de départ SV de n bits.

d) Une suite de q blocs de texte chiffré $C_1, C_2, ..., C_q$, chacun de n bits.

5.2 Description de la méthode de chiffrement en mode CBC :

Chiffrement du premier bloc de texte clair,

$$C_1 = eK(P_1 \oplus SV) \qquad ... (3)$$

ensuite,

$$C_i = eK(P_i \oplus C_{i-1}) \text{ pour } i = 2, 3, ..., q \qquad ... (4)$$

Cette procédure est illustrée en haut de la figure 1. La variable de départ SV est utilisée pour générer la sortie du premier cryptogramme. Ensuite, le cryptogramme est additionné, modulo 2, au texte clair suivant avant chiffrement.

5.3 Description de la méthode de déchiffrement en mode CBC :

Déchiffrement du premier bloc de texte chiffré,

$$P_1 = dK(C_1) \oplus SV \qquad ... (5)$$

ensuite,

$$P_i = dK(C_i) \oplus C_{i-1} \text{ pour } i = 2, 3, ..., q \qquad ... (6)$$

Cette procédure est illustrée dans le bas de la figure 1.

6 Mode rebouclage de texte chiffré (CFB)

6.1 Deux paramètres définissent un mode opératoire CFB :

— la taille de la variable de rebouclage, k, où $1 \leq k \leq n$

— la taille de la variable de texte clair, j, où $1 \leq j \leq k$

Les variables utilisées dans le mode opératoire CFB sont

a) Les variables d'entrée

1) Une suite de q variables de texte clair $P_1, P_2, ..., P_q$, chacune de j bits.

2) Une clé K.

3) Une variable de départ SV de n bits.

b) Les résultats intermédiaires

1) Une suite de q blocs d'entrée de l'algorithme $X_1, X_2, ..., X_q$, chacun de n bits.

2) Une suite de q blocs de sortie de l'algorithme $Y_1, Y_2, ..., Y_q$, chacun de n bits.

3) Une suite de q variables $E_1, E_2, ..., E_q$, chacune de j bits.

4) Une suite de $q - 1$ variables de rebouclage $F_1, F_2, ..., F_{q-1}$, chacune de k bits.

c) Les variables de sortie, soit une suite de q variables de cryptogramme $C_1, C_2, ..., C_q$, chacune de j bits.

6.2 Le bloc d'entrée X est mis à sa valeur initiale

$X_1 = SV$ ... (7)

Le chiffrement de chaque variable de texte clair se fait en cinq étapes comme suit :

a) Application de l'algorithme de chiffrement,

$Y_i = eK(X_i)$ ... (8)

b) Sélection des j bits les plus à gauche,

$E_i = Y_i \sim j$ ... (9)

c) Production de la variable de cryptogramme,

$C_i = P_i \oplus E_i$ ... (10)

d) Production de la variable de rebouclage,

$F_i = S_j(I(k) \mid C_i)$ ... (11)

e) Fonction de décalage,

$X_{i+1} = S_k(X_i \mid F_i)$ ... (12)

Ces étapes sont répétées pour $i = 1, 2, ..., q$, et se terminent par l'équation (12) lors du dernier cycle. La procédure est illustrée sur le côté gauche de la figure 2. Les j bits de gauche du bloc de sortie Y de l'algorithme de chiffrement sont utilisés pour chiffrer, par une addition modulo 2, la variable de texte clair de j bits. Les bits restants de Y sont rejetés. Les bits des variables de texte clair et de cryptogramme sont numérotés de 1 à j.

La variable de cryptogramme est étendue en mettant $k - j$ bits à «1» dans les positions binaires les plus à gauche pour devenir la variable de rebouclage F de k bits. Ensuite les bits du bloc d'entrée X sont décalés à gauche de k positions et F est inséré dans les k positions les plus à droite pour donner la nouvelle valeur de X. Dans cette opération de décalage, les k bits les plus à gauche de X sont rejetés.

6.3 Les variables utilisées pour le déchiffrement sont les mêmes que celles utilisées pour le chiffrement. Le bloc d'entrée X est mis à sa valeur initiale $X_1 = SV$.

Le déchiffrement de chaque variable de cryptogramme se fait en cinq étapes comme suit :

a) Utilisation de l'algorithme de chiffrement,

$Y_i = eK(X_i)$ ... (13)

b) Sélection des j bits de gauche,

$E_i = Y_i \sim j$ ... (14)

c) Production de la variable de texte clair,

$P_i = C_i \oplus E_i$ ... (15)

d) Production de la variable de rebouclage,

$F_i = S_j(I(k) \mid C_i)$ ... (16)

e) Fonction de décalage,

$X_{i+1} = S_k(X_i \mid F_i)$ ... (17)

Ces étapes sont répétées pour $i = 1, 2, ..., q$, et se terminent par l'équation (17) lors du dernier cycle. La procédure est illustrée sur le côté droit de la figure 2. Les j bits de gauche du bloc de sortie Y de l'algorithme de chiffrement sont utilisés pour déchiffrer, par une addition modulo 2, la variable de cryptogramme de j bits. Les bits restants de Y sont rejetés. Les bits des variables de texte clair et de cryptogramme sont numérotés de 1 à j.

La variable de cryptogramme est étendue en mettant $k - j$ bits à «1» dans les positions binaires les plus à gauche pour devenir la variable de rebouclage F de k bits. Ensuite les bits du bloc d'entrée X sont décalés à gauche de k positions et F est inséré dans les k positions les plus à droite pour donner la nouvelle valeur de X. Dans cette opération de décalage, les k bits de gauche de X sont rejetés.

6.4 Lorsqu'on utilise le mode CFB, il est recommandé de choisir des valeurs égales pour j et k. Sous cette forme recommandée ($j = k$), les équations (11) et (16) peuvent s'écrire

$F_i = C_i$ (cas $j = k$)

7 Mode rebouclage de la sortie (OFB)

7.1 Un paramètre définit un mode opératoire OFB, il s'agit de la taille de la variable j du texte clair où $1 \leq j \leq n$.

Les variables utilisées pour le mode opératoire OFB sont

a) Les variables d'entrée

1) Une suite de q variables de texte clair $P_1, P_2, ..., P_q$, chacune de j bits.

2) Une clé K.

3) Une variable de départ SV de n bits.

b) Les résultats intermédiaires

1) Une suite de q blocs d'entrée de l'algorithme $X_1, X_2, ..., X_q$, chacun de n bits.

2) Une suite de q blocs de sortie de l'algorithme $Y_1, Y_2, ..., Y_q$, chacun de n bits.

3) Une suite de q variables $E_1, E_2, ..., E_q$, chacune de j bits.

c) Les variables de sortie, soit une suite de q variables de cryptogramme $C_1, C_2, ..., C_q$, chacune de j bits.

7.2 Le bloc d'entrée X est mis à sa valeur initiale

$$X_1 = SV \quad ...(18)$$

Le chiffrement de chaque variable de texte clair se fait en quatre étapes comme suit :

a) Utilisation de l'algorithme de chiffrement,

$$Y_i = eK(X_i) \quad ...(19)$$

b) Sélection des j bits de gauche,

$$E_i = Y_i \sim j \quad ...(20)$$

c) Production de la variable de cryptogramme,

$$C_i = P_i \oplus E_i \quad ...(21)$$

d) Opération de rebouclage,

$$X_{i+1} = Y_i \quad ...(22)$$

Ces étapes sont répétées pour $i = 1, 2, ..., q$, et se terminent par l'équation (21) lors du dernier cycle. La procédure est illustrée sur le côté gauche de la figure 3. Le résultat de chaque utilisation de l'algorithme de chiffrement Y_i est rebouclé et devient la valeur suivante de X, à savoir X_{i+1}. Les j bits les plus à gauche de Y_i sont utilisés pour chiffrer la variable d'entrée.

7.3 Les variables utilisées pour le déchiffrement sont les mêmes que celles utilisées pour le chiffrement. Le bloc d'entrée X est mis à sa valeur initiale $X_1 = SV$.

Le déchiffrement de chaque variable de cryptogramme se fait en quatre étapes comme suit :

a) Utilisation de l'algorithme de chiffrement,

$$Y_i = eK(X_i) \quad ...(23)$$

b) Sélection des j bits de gauche,

$$E_i = Y_i \sim j \quad ...(24)$$

c) Production de la variable de texte clair,

$$P_i = C_i \oplus E_i \quad ...(25)$$

d) Opération de rebouclage,

$$X_{i+1} = Y_i \quad ...(26)$$

Ces étapes sont répétées pour $i = 1, 2, ..., q$, et se terminent par l'équation (25) lors du dernier cycle. La procédure est illustrée sur le côté droit de la figure 3. Les valeurs X_i et Y_i sont les mêmes que celles utilisées pour le chiffrement ; seule l'équation (25) est différente.

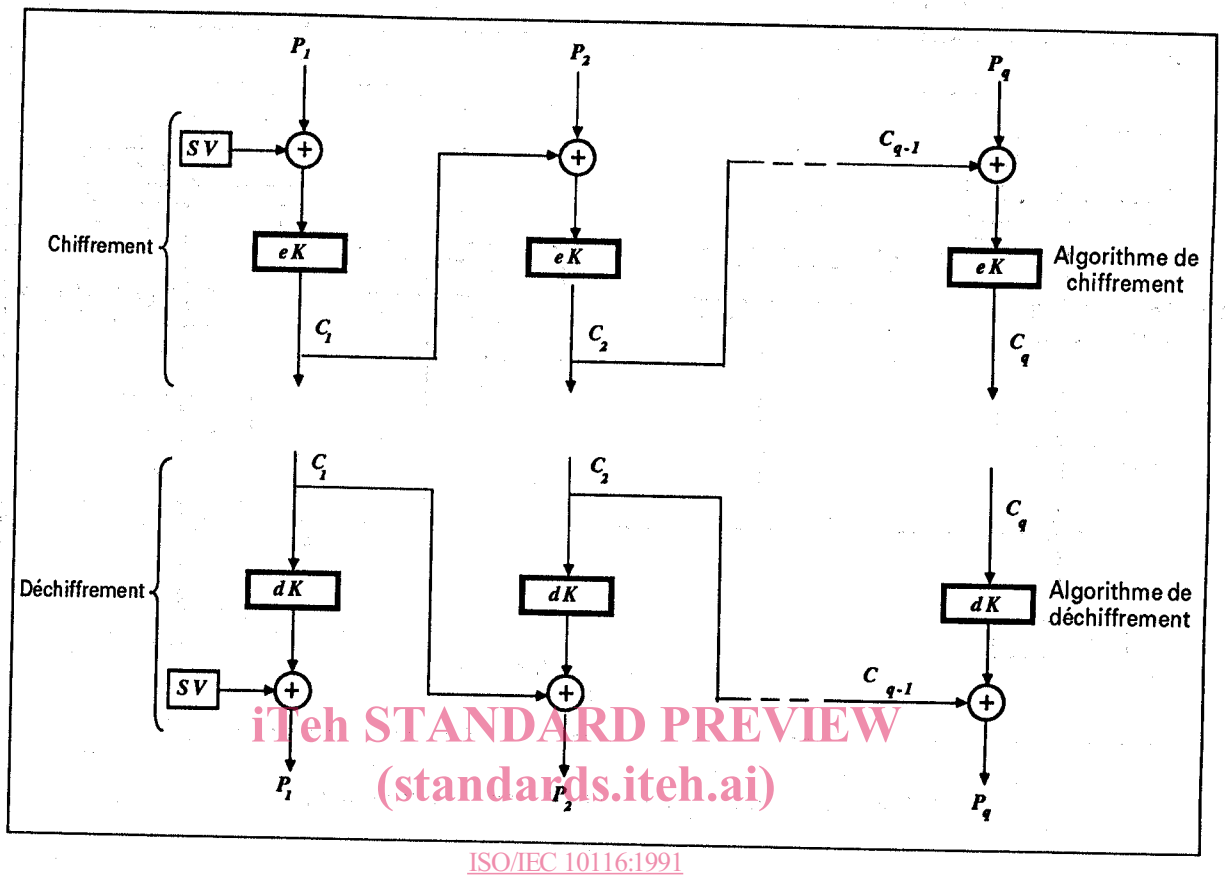

Figure 1 — Mode opératoire «chaînage de blocs chiffrés» (CBC)

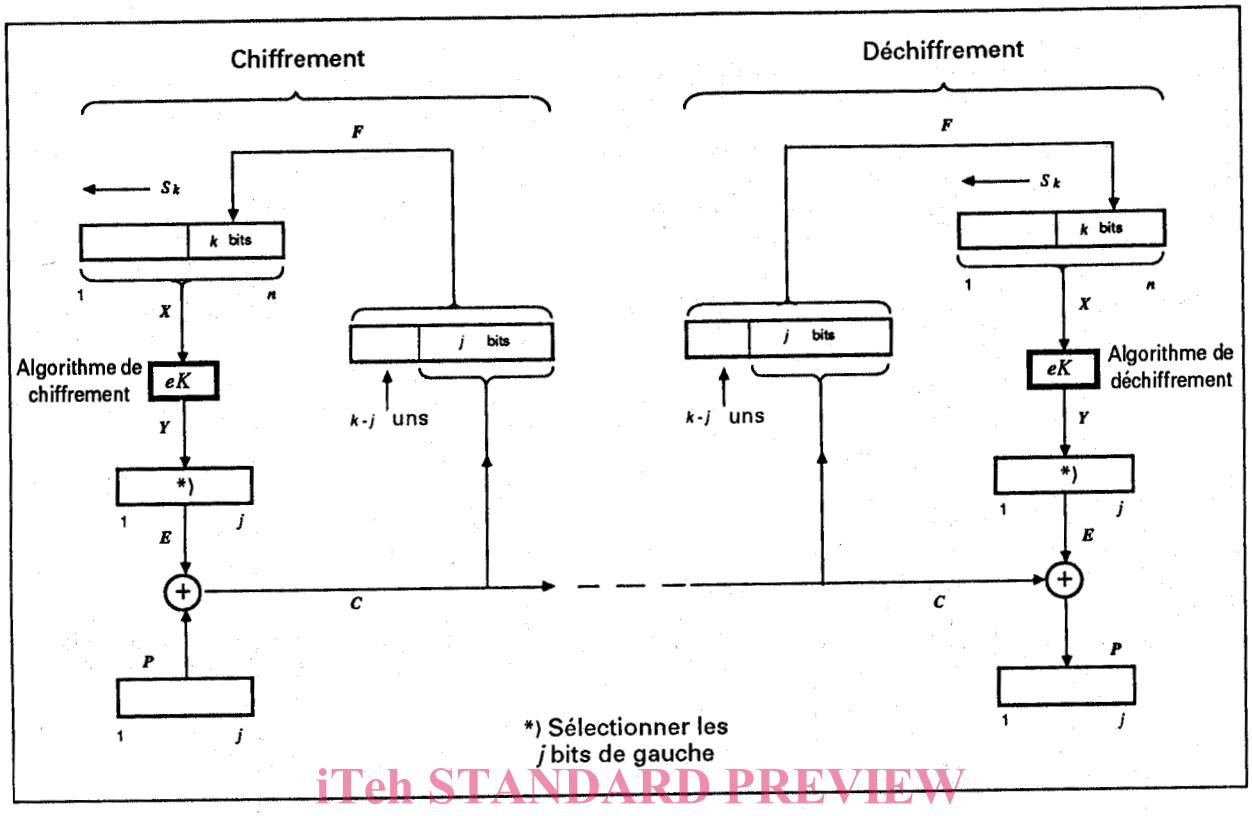

Figure 2 — Mode «rebouclage du texte chiffré» (CFB)

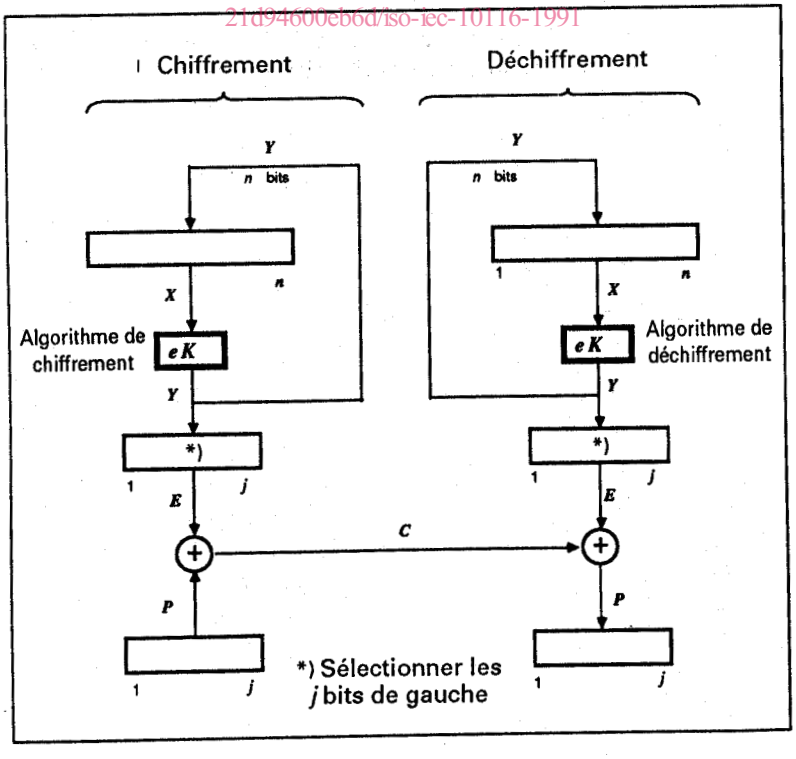

Figure 3 — Mode opératoire «rebouclage de la sortie» (OFB)

Annexe A

(informative)

Propriétés des modes opératoires

A.1 Propriétés du mode opératoire dictionnaire (ECB)

A.1.1 Environnement

Les messages qui transportent des informations entre les ordinateurs, ou entre des correspondants, peuvent contenir des répétitions ou des séquences utilisées fréquemment. En mode ECB, des textes clairs identiques donnent (pour la même clé) des cryptogrammes identiques.

A.1.2 Propriétés

Les propriétés du mode ECB sont les suivantes :

a) le chiffrement ou le déchiffrement d'un bloc peut être effectué indépendamment des autres blocs ;

b) le réarrangement des blocs de texte chiffré entraînera le réarrangement correspondant des blocs de texte clair ;

c) le même bloc de texte clair produit toujours le même bloc de texte chiffré (pour la même clé), ce qui le rend vulnérable aux «attaques dictionnaire».

Le mode ECB n'est en général pas recommandé pour les messages de plus d'un bloc. L'utilisation du mode ECB peut être spécifiée dans les Normes internationales ultérieures à des fins particulières lorsque la caractéristique de répétition est acceptable ou si les blocs ne peuvent être accédés qu'individuellement.

A.1.3 Prescriptions de remplissage

Seuls les multiples de n bits peuvent être chiffrés ou déchiffrés. Les autres longueurs nécessitent un remplissage pour arriver à une limite de n bits.

A.1.4 Propagation d'erreur

En mode ECB, un ou plusieurs bits erronés dans le même bloc de cryptogramme affectent uniquement le déchiffrement du bloc dans lequel ils se trouvent. En supposant que le chiffre ait la propriété que le fait de changer un bit de texte clair entraîne un changement moyen de 50 % du cryptogramme, chaque bit de la version en texte clair récupérée de ce bloc aura un taux moyen d'erreur de 50 %.

A.1.5 Limites de bloc

Si des limites de bloc sont perdues entre le chiffrement et le déchiffrement (par ex. à cause d'un glissement de bit), la synchronisation entre les opérations de chiffrement et de déchiffrement est perdue et ce, jusqu'au rétablissement des limites correctes des blocs. Les résultats de tous les déchiffrements seront incorrects tant que les limites de bloc seront perdues.

A.2 Propriétés du mode opératoire par «chaînage de blocs chiffrés» (CBC)

A.2.1 Environnement

Le mode CBC donne toujours le même cryptogramme dès lors que le même texte clair est chiffré à l'aide de la même clé et de la même variable de départ. Les utilisateurs qui sont gênés par cette particularité doivent adopter une stratégie pour modifier le début du texte clair, la clé ou la variable de départ. Une possibilité est d'incorporer un identificateur unique (par ex. un compteur incrémenté) au début de chaque message CBC. Une autre possibilité, qui peut être utilisée pour le chiffrement d'enregistrements dont la taille ne devrait pas augmenter, consiste à employer une valeur, variable de départ par exemple, qui peut être calculée à partir de l'enregistrement sans connaître son contenu (par ex. son adresse dans une mémoire à accès aléatoire).

A.2.2 Propriétés

Les propriétés du mode CBC sont

a) l'opération de chaînage rend les blocs de cryptogramme dépendants du bloc courant et de tous les blocs de texte clair précédents et par conséquent les blocs ne peuvent être réarrangés ;

b) l'utilisation de valeurs de *SV* différentes empêche que le chiffrement du même texte clair donne le même cryptogramme.