NORME INTERNATIONALE

ISO 8372

Première édition
1987-08-15

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
ORGANISATION INTERNATIONALE DE NORMALISATION
МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ

Traitement de l'information — Modes opératoires d'un algorithme de chiffrement par blocs de 64 bits

Information processing — Modes of operation for a 64-bit block cipher algorithm

Numéro de référence
ISO 8372 : 1987 (F)

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est normalement confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux.

Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour approbation, avant leur acceptation comme Normes internationales par le Conseil de l'ISO. Les Normes internationales sont approuvées conformément aux procédures de l'ISO qui requièrent l'approbation de 75 % au moins des comités membres votants.

La Norme internationale ISO 8372 a été élaborée par le comité technique ISO/TC 97, *Systèmes de traitement de l'information.*

L'attention des utilisateurs est attirée sur le fait que toutes les Normes internationales sont de temps en temps soumises à révision et que toute référence faite à une autre Norme internationale dans le présent document implique qu'il s'agit, sauf indication contraire, de la dernière édition.

Imprimé en Suisse

Traitement de l'information — Modes opératoires d'un algorithme de chiffrement par blocs de 64 bits

1 Objet et domaine d'application

La présente Norme internationale décrit quatre modes opératoires, d'un algorithme quelconque de chiffrement par blocs de 64 bits, utilisant une clé secrète.

NOTE — L'annexe, qui ne fait pas partie intégrante de la présente Norme internationale, contient des commentaires sur les caractéristiques de chaque mode.

La présente Norme internationale définit quatre modes opératoires tels que, dans le cadre d'une quelconque application de chiffrement par blocs de 64 bits (par exemple, transmission de données, stockage de données, authentification) cette norme constitue une référence utile pour la spécification des modes opératoires, la formation de la variable de départ et les valeurs des paramètres (selon le cas).

NOTE — Deux paramètres, j et k, sont définis pour le mode opératoire (voir chapitre 7) par rebouclage du cryptogramme (CFB). Un seul paramètre, j, est défini pour le mode par rebouclage (voir chapitre 8) de la sortie (OFB). Lorsqu'un de ces modes opératoires est utilisé, la ou les valeurs des paramètres doivent être choisies et employées par toutes les parties qui communiquent.

2 Référence

ANSI X3.92-1981, *Data Encryption Algorithm.*

3 Définitions

3.1 texte clair: Informations non chiffrés.

3.2 cryptogramme: Informations chiffrées.

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

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

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

NOTE — La méthode permettant de calculer la variable de départ à partir de la variable d'initialisation n'est pas définie dans la présente Norme internationale. Elle doit être décrite dans toutes les applications des modes opératoires.

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

4 Notation

Pour tout ce qui concerne la présente Norme internationale, la relation fonctionnelle définie par l'algorithme de chiffrement des blocs s'écrit

$$C = eK(P)$$

où

P est le bloc de texte clair;
C est le cryptogramme;
K est la clé.

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

La fonction de déchiffrement correspondante s'écrit

$$P = dK(C)$$

Une variable telle que P ou C ci-dessus, désignée par une majuscule représente un vecteur de bits, par exemple:

$$A = \{a_1, a_2, \ldots, a_m\} \qquad B = \{b_1, b_2, \ldots, b_m\}$$

c'est-à-dire des vecteurs de m bits, numérotés de 1 à m.

L'opération d'addition modulo 2 également appelée fonction «ou exclusif» est représentée par l'opération $\oplus$. Appliquée à des vecteurs comme A et B, l'opération se définit comme

$$A \oplus B = \{a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_m \oplus b_m\}$$

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

$$A \sim j = \{a_1, a_2, \ldots, a_j\}$$

Cette opération est définie seulement lorsque $j < m$, 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 $k \leqslant m$, la fonction de décalage $S_k(X \mid F)$ produit la variable de m bits

$$S_k(X \mid F) = \{x_{k+1}, x_{k+2}, \ldots, x_m, f_1, f_2, \ldots, f_k\}$$

L'effet résultant est de décaler de k positions vers la gauche les bits du vecteur X, en plaçant de côté $x_1 \ldots x_k$ et le vecteur F, dans les k positions de droite de X.

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

Le résultat est

$$S_j(I(k) \mid C) = \{1, 1, \ldots, 1, c_1, c_2, \ldots, c_j\}$$

où il y a $k - j$ «uns» sur la gauche du vecteur résultant.

5 Mode dictionnaire (ECB)

À partir d'un bloc P de 64 bits de texte clair, l'algorithme de chiffrement donne un bloc C de 64 bits de cryptogramme, c'est-à-dire:

$$C = eK(P)$$

L'algorithme de déchiffrement donne

$$P = dK(C)$$

Ce mode d'utilisation de l'algorithme de chiffrement est appelé mode «dictionnaire».

6 Mode chaînage de blocs chiffres (CBC)

Les variables utilisées avec le mode de chiffrement CBC sont

a) une séquence de n blocs de texte clair $P_1, P_2, \ldots, P_n$, contenant chacun 64 bits;

b) une clé K;

c) une variable de départ SV de 64 bits;

d) la séquence résultante de n blocs de texte chiffré $C_1, C_2, \ldots, C_n$, de 64 bits chacun.

NOTE — La méthode de formation de SV n'est pas décrite dans la présente Norme internationale.

Description de la méthode de chiffrement en mode CBC:

Chiffrement de la première variable texte clair:

$$C_1 = eK(P_1 \oplus SV) \qquad \ldots (1)$$

ensuite,

$$C_i = eK(P_i \oplus C_{i-1}) \quad \text{pour } i = 2, 3, \ldots, n \qquad \ldots (2)$$

Cette procédure est illustrée en haut de la figure 1. La variable de départ SV est utilisée pour engendrer la sortie du premier cryptogramme.

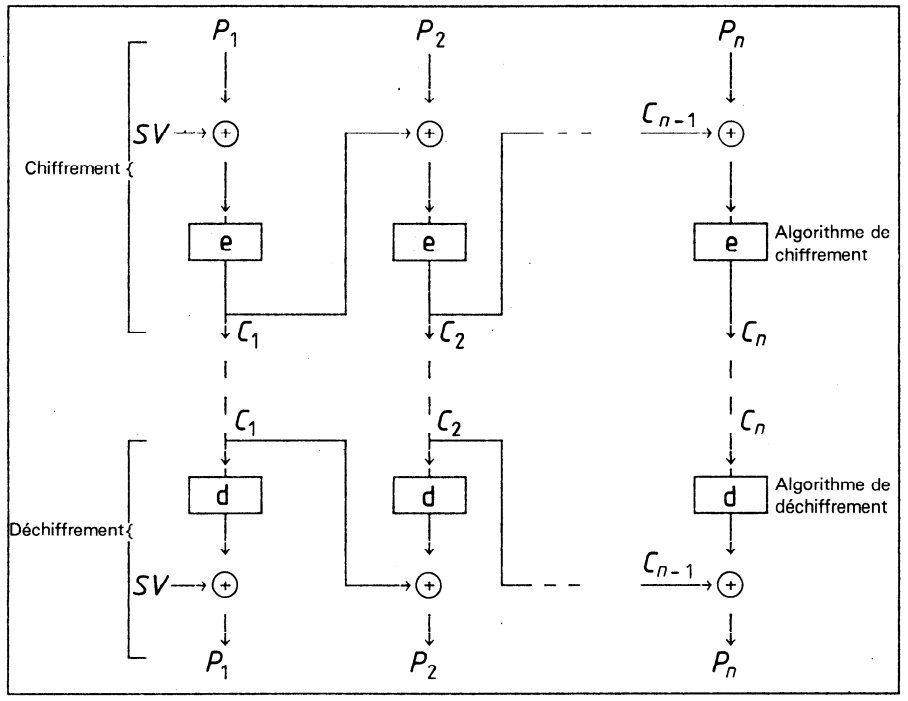

Figure 1 — Mode opératoire du chaînage de bloc (CBC)

Ultérieurement, le cryptogramme obtenu est additionné modulo 2 au prochain texte clair, avant chiffrement.

Description de la méthode de chiffrement en mode CBC:

Déchiffrement du premier cryptogramme:

$$P_1 = dK(C_1) \oplus SV \qquad \ldots (3)$$

ensuite,

$$P_i = dK(C_i) \oplus C_{i-1} \quad \text{pour } i = 2, 3, \ldots, n \qquad \ldots (4)$$

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

7 Mode autoclave sur le cryptogramme (CFB)

7.1 Deux paramètres définissent le mode opératoire CFB

a) la taille de la variable de rebouclage k, pour laquelle $1 \leqslant k \leqslant 64$;

b) la taille de la variable de texte clair, j, pour laquelle $1 \leqslant j \leqslant k$.

Les variables utilisées dans ce mode opératoire sont

a) Les variables d'entrée:

1) une séquence de n variables de texte clair $P_1, P_2, \ldots, P_n$, contenant chacune j bits;

2) une clé K;

3) une variable SV de départ de 64 bits.

b) Les résultats intermédiaires:

1) une séquence de n variables d'entrée de l'algorithme $X_1, X_2, \ldots, X_n$, de 64 bits chacune;

2) une séquence de n variables de sortie de l'algorithme $Y_1, Y_2, \ldots, Y_n$, de 64 bits chacune;

3) une séquence de n variables $E_1, E_2, \ldots, E_n$, de j bits chacune;

4) une séquence de n variables de rebouclage $F_1, F_2, \ldots, F_n$, de k bits chacune.

c) Les variables de sortie sont constituées par une série de n variables de cryptogrammes $C_1, C_2, \ldots, C_n$, de j bits chacune.

NOTE — La méthode de formation de SV n'est pas décrite dans la présente Norme internationale.

La variable X est mise à sa valeur initiale

$$X_1 = SV \qquad \ldots (5)$$

7.2 Le chiffrement de chaque bloc de texte clair se compose des cinq étapes suivantes:

a) utilisation de l'algorithme de chiffrement, $Y_i = eK(X_i)$; ... (6)

b) sélection des j bits de gauche, $E_i = Y_i \sim j$; ... (7)

c) production du bloc de texte chiffré, $C_i = P_i \oplus E_i$; ... (8)

d) production du bloc de retour, $F_i = S_j(I(k)|C_i)$; ... (9)

e) fonction de décalage sur X, $X_{i+1} = S_k(X_i|F_i)$. ... (10)

Ces étapes sont répétées pour $i = 1, 2, \ldots, n$, et se terminent par l'équation (8) pour le dernier cycle. La procédure est illustrée sur le côté gauche de la figure 2. Les j bits de gauche de la sortie Y de l'algorithme de chiffrement sont utilisés pour chiffrer, par une addition modulo 2, le bloc de texte clair de j bits. Les bits restants de Y sont rejetés. Les bits des blocs du texte clair et du texte chiffré sont numérotés de 1 à j.

Le cryptogramme est étendu en mettant $k - j$ «uns» dans les positions binaires les plus à gauche pour obtenir F, un vecteur de k bits; ensuite, les bits du vecteur X sont décalés à gauche de k positions et le vecteur F est mis dans les k positions de droite, pour donner la nouvelle valeur de X. Dans cette opération de décalage, les k bits de gauche de X sont rejetés. La valeur initiale du vecteur X est la variable de départ (SV).

7.3 Les variables utilisées pour le déchiffrement sont les mêmes que celles utilisées pour le chiffrement. La variable X est mise à sa valeur initiale $X_1 = SV$.

Le déchiffrement de chaque bloc de cryptogramme se compose des cinq étapes suivantes:

a) utilisation de l'algorithme de chiffrement, $Y_i = eK(X_i)$; ... (11)

b) sélection des j bits de gauche, $E_i = Y_i \sim j$; ... (12)

c) production du bloc de texte clair, $P_i = C_i \oplus E_i$; ... (13)

d) production du bloc de rebouclage, $F_i = S_j(I(k)|C_i)$; ... (14)

e) fonction de décalage sur X, $X_{i+1} = S_k(X_i|F_i)$. ... (15)

Ces étapes sont répétées pour $i = 1, 2, \ldots, n$, et se terminent par l'équation (13) pour le dernier cycle. La procédure est illustrée sur la partie droite de la figure 2. Les j bits de gauche de la sortie Y de l'algorithme de chiffrement sont utilisés pour chiffrer le cryptogramme de même couleur par une addition modulo 2. Les bits restants de Y sont rejetés. Les bits des blocs «clair» et de cryptogramme sont numérotés de 1 à j.

Le cryptogramme est étendu en insérant $k - j$ «uns» dans ses positions binaires de gauche pour obtenir F, un vecteur de k bits; ensuite, les bits du vecteur X sont décalés à gauche de k positions et le vecteur F est mis dans les k positions de droite, pour donner la nouvelle valeur de X. Dans cette opération de décalage, les k bits de gauche de X sont rejetés. La valeur initiale du vecteur X est la variable de départ (SV).

7.4 Lorsqu'on utilise le mode CFB, il est recommandé de choisir des valeurs égales pour j et k.

Dans cette forme recommandée ($j = k$), les équations (9) et (14) peuvent s'écrire

$$F_i = C_i \qquad (\text{cas } j = k)$$

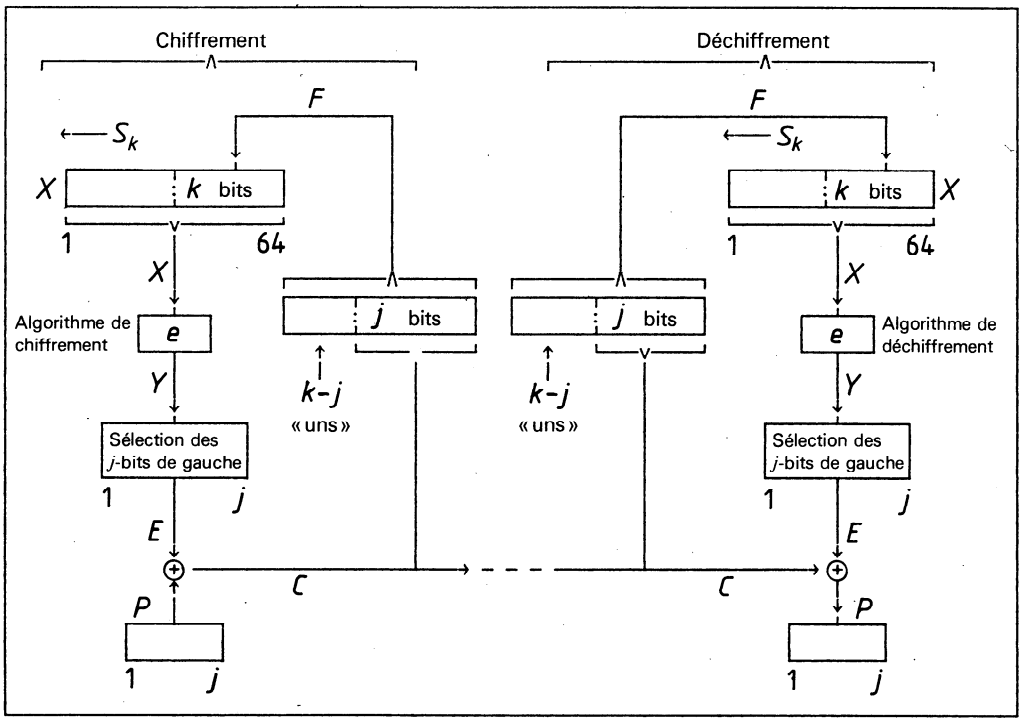

Figure 2 — Mode autoclave sur le cryptogramme (CFB)

8 Mode autoclave sur la sortie (OFB)

8.1 Un seul paramètre définit le mode opératoire OFB; il s'agit de la taille de la variable j du texte clair, où $1 \leqslant j \leqslant 64$.

Les variables utilisées pour le mode opératoire OFB sont

a) Les variables d'entrée

1) une séquence de n blocs de texte clair $P_1, P_2, \ldots, P_n$, contenant chacun j bits;

2) une clé K;

3) une variable SV de départ de 64 bits.

b) Les résultats intermédiaires:

1) une séquence de n variables d'entrée de l'algorithme $X_1, X_2, \ldots, X_n$, de 64 bits chacune;

2) une séquence de n variables de sortie de l'algorithme $Y_1, Y_2, \ldots, Y_n$, de 64 bits chacune;

3) une séquence de n variables $E_1, E_2, \ldots, E_n$, de j bits chacune.

c) Les variables de sortie, c'est-à-dire une séquence de n variables de cryptogramme $C_1, C_2, \ldots, C_n$, de j bits chacune.

NOTE — La méthode de formation de SV n'est pas décrite dans la présente Norme internationale.

La variable X est mise à sa valeur initiale

$$X_1 = SV \qquad \ldots (16)$$

8.2 Le chiffrement de chaque bloc de texte clair se compose des quatres étapes suivantes:

a) utilisation de l'algorithme de chiffrement, $Y_i = eK(X_i)$; ... (17)

b) sélection des j bits de gauche, $E_i = Y_i \sim j$; ... (18)

c) production du cryptogramme, $C_i = P_i \oplus E_i$; ... (19)

d) opération de rebouclage, $X_{i+1} = Y_i$. ... (20)

Ces étapes sont répétées pour $i = 1, 2, \ldots, n$, et se terminent par l'équation (19) pour le dernier cycle. La procédure est illustrée sur le côté gauche de la figure 3. Chaque résultat Y_i obtenu par l'algorithme de chiffrement est rebouclé et devient la prochaine valeur de X, à savoir X_{i+1}. Les j bits de gauche de Y_i sont utilisés pour chiffrer le bloc d'entrée.

8.3 Les variables utilisées pour le déchiffrement sont les mêmes que celles utilisées pour le chiffrement. La variable X est mise à sa valeur initiale $X_1 = SV$.

Le déchiffrement de chaque bloc de cryptogramme se compose des quatre étapes suivantes:

a) utilisation de l'algorithme de chiffrement, $Y_i = eK(X_i)$; ... (21)

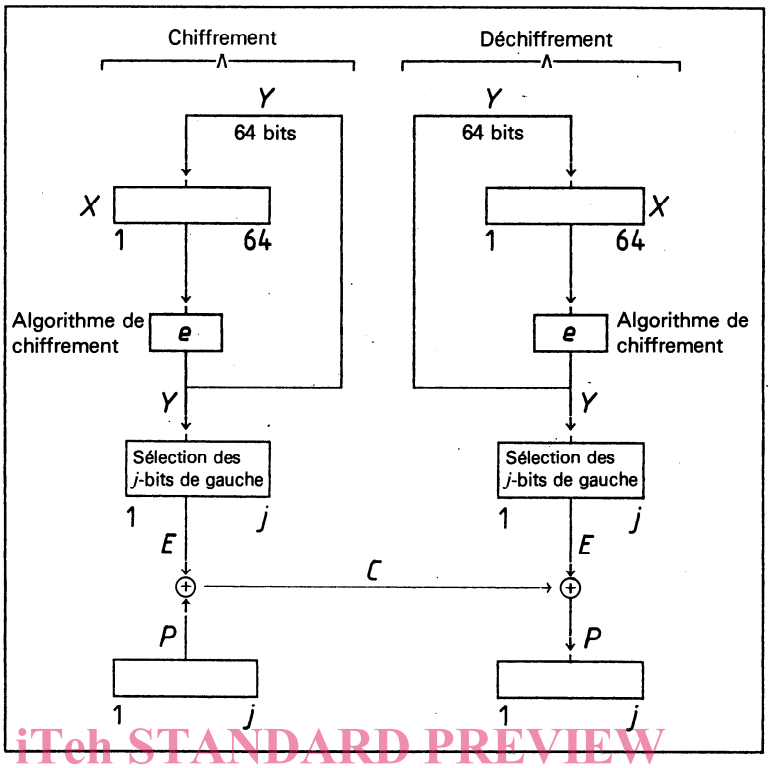

Figure 3 — Mode opératoire par rebouclage de la sortie (OFB)

b) sélection des j bits de gauche, $E_i = Y_i \sim j$; . . . (22)

c) production du bloc de texte clair, $P_i = C_i \oplus E_i$; . . . (23)

d) opération de rebouclage, $X_{i+1} = Y_i$. . . . (24)

Ces étapes sont répétées pour $i = 1, 2, \ldots, n$, et se terminent par l'équation (23) pour le dernier cycle. La procédure est illustrée sur la partie droite de la figure 3. Les valeurs des variables X_i et Y_i sont les mêmes que celles utilisées pour le chiffrement; seule l'équation (23) est différente.

Annexe

Propriétés des modes opératoires

(Cette annexe contient des commentaires sur les propriétés des quatres modes opératoires décrits dans la présente Norme internationale et ne fait pas partie intégrante de la norme.)

A.1 Propriétés du mode opératoire ECB

Les messages transportant des informations entre des ordinateurs, ou entre des correspndantes, peuvent contenir des répétitions ou des séquences utilisées fréquémment. En mode ECB, deux textes clair identiques donnent (avec la même clé) des cryptogrammes identiques. À cause de cette caractéristique, le mode ECB ne convient pas pour l'usage général. L'utilisation du mode ECB pourra être spécifiée dans des normes ultérieures, à des fins particulières, lorsque la caractéristique de répétition est acceptable.

Si des limites de blocs sont perdues entre le chiffrement et le déchiffrement (par exemple 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.

A.2 Propriétés du mode CBC

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 valeur d'initialisation. Les utilisateurs qui sont gênés par cette particularité doivent adopter une stratégie modifiant le début du texte clair, la clé ou la variable de départ. Une des possibilités consiste à inclure un identificateur unique (par exemple un compteur incrémenté) au début de chaque message CBC. Une autre possibilité réservée pour le chiffrement d'enregistrements dont la taille ne doit pas être augmentée, consiste à employer comme valeur d'identification une valeur qui peut être calculée à partir de l'enregistrement, sans connaître son contenu (par exemple, le numéro du bloc dans lequel il se trouve en mémoire à accès aléatoire).

Puisque le mode CBC est une méthode de chiffrement bloc par bloc, on doit opérer sur des blocs de données complets de 64 bits. Les blocs contenant moins de 64 bits exigent un traitement spécial.

En mode CBC, une ou plusieurs erreurs binaires intervenant dans un même bloc de cryptogramme affecte(nt) le déchiffrement de deux blocs (le bloc dans lequel se trouve l'erreur et le bloc suivant). Si les erreurs sont dans le i^e bloc du cryptogramme, chaque bit du i^e bloc de texte clair comportera un taux moyen d'erreur de 50 %. Dans le $(i + 1)^e$ bloc de texte clair, les seuls bits erronés seront ceux qui correspondent directement aux bits erronés du crypotgramme.

Si des limites de blocs sont perdues entre le chiffrement et le déchiffrement (par exemple 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.

A.3 Propriétés du mode CFB

En mode CFB, toute erreur dans un bloc de cryptogramme de longueur j affecte son déchiffrement ainsi que celui des blocs de cryptogramme suivants et ce, jusqu'au moment où les bits erronés seront extraits du bloc d'entrée par décalage. La première unité de longueur j bits de texte clair déchiffrée sera erronée exactement au endroits où le cryptogramme est erroné. Les textes déchiffrés ultérieurs contiendront un taux moyen d'erreur de 50 % jusqu'au moment où toutes les erreurs auront été sorties du bloc d'entrée. Si on suppose qu'aucune autre erreur additionnelle n'est détectée pendant ce temps, le texte clair correct est alors obtenu. Cette caractéristique est parfois appelée «limitation de la propagation d'erreurs».

Si des limites des j bits sont perdues pendant le déchiffrement, la synchronisation cryptographique est perdue jusqu'à l'exécution d'une initialisation cryptographique ou jusqu'à 64 bits après le rétablissement des limites des j bits.

Les opérations de chiffrement et de déchiffrement du mode CFB utilisent toutes deux la forme de chiffrement de l'algorithme.

A.4 Propriétés du mode par rebouclage de la sortie (OFB)

La mode opératoire OFB ne propage pas les erreurs du cryptogramme dans le texte déchiffré. Lorsqu'un bit du cryptogramme est erroné, il provoque seulement l'apparition d'un bit erroné dans le texte clair au même endroit. Il n'y a pas d'autosynchronisation. Si les deux opérations, chiffrement et déchiffrement, se trouvent désynchronisées, le système doit être ré-initialisé. Cette perte de synchronisation peut être due à une perte des limites correctes des blocs de j bits (à cause d'un glissement de bit) ou à une erreur de la valeur de la variable X, à une extrémité où à l'autre, ce qui a pour effet de différencier les valeurs X aux deux extrémités jusqu'au moment où la ré-initialisation intervient.

Chaque ré-initialisation devrait utiliser pour SV une valeur différente des valeurs SV utilisées auparavant avec la même clé.

Page blanche