NORME INTERNATIONALE

ISO 10126-2

Première édition
1991-07-15

Banque — Procédures de chiffrement de messages (service aux entreprises) —

Partie 2: Algorithme DEA

Banking - Procedures for message encipherment (wholesale) —

Part 2: DEA algorithm

Numéro de référence
ISO 10126-2:1991(F)

Sommaire

Organisation internationale de normalisation
Case Postale 56 • CH-1211 Genève 20 • Suisse

Imprimé en Suisse

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 en général 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. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

La Norme internationale ISO 10126-2 a été élaborée par le comité technique ISO/TC 68, *Banque et services financiers liés aux opérations bancaires*.

L'ISO 10126 comprend les parties suivantes, présentées sous le titre général *Banque — Procédures de chiffrement de messages (service aux entreprises)*:

— *Partie 1: Principes généraux*

— *Partie 2: Algorithme DEA*

L'ISO 10126 est le fruit des travaux de l'ANSI et est un développement de l'ANSI X9.23 (1988), *Financial Institution: Encryption of Wholesale Financial Messages*, avec laquelle elle reste compatible.

Page blanche

Banque — Procédures de chiffrement de messages (service aux entreprises) —

Partie 2:
Algorithme DEA

1 Domaine d'application

L'ISO 10126-1 prescrit une méthode de chiffrement et de déchiffrement des messages financiers entiers (ou partiels) grâce à l'utilisation du chiffrement niveau ou application, dans un but de confidentialité.

DEA est un algorithme approprié pour mettre en œuvre l'ISO 10126-1. Il est spécifié dans l'ANSI X3.92. Les clés doivent être gérées conformément à l'ISO 8732.

2 Références normatives

Les normes suivantes contiennent des dispositions qui, par suite de la référence qui en est faite, constituent des dispositions valables pour la présente partie de l'ISO 10126. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute norme est sujette à révision et les parties prenantes des accords fondés sur la présente partie de l'ISO 10126 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des normes indiquées ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur à un moment donné.

ISO 8372:1987, *Traitement de l'information — Modes opératoires d'un algorithme de chiffrement par blocs de 64 bits.*

ISO 8732:1988, *Banque — Gestion de clés.*

ISO 10126-1:1991[1], *Banque — Procédures de chiffrement de messages (service aux entreprises) — Partie 1: Principes généraux.*

ANSI X3.92:1981, *American National Standard for information Systems — Data Encryption Algorithm.*

3 Modes opératoires

Les modes opératoires qui doivent être utilisés sont le chiffrement par blocs chaînés (CBC), le chiffrement à rebouclage par le chiffré bit par bit (CFB-1) ou le chiffrement à rebouclage par le chiffré octet par octet (CFB-8) comme défini dans l'ISO 8732.

4 Vecteurs d'initialisation (IV)

Un IV est utilisé comme point de départ pour le chiffrement et le déchiffrement d'une séquence de données afin d'accroître la sécurité en introduisant une variation cryptographique supplémentaire (c'est-à-dire que la répétition d'une séquence de texte clair ne se traduira pas par la répétition d'une séquence de texte chiffré) et de synchroniser le matériel de chiffrement.

4.1 Chiffrement par blocs chaînés (CBC)

Un nouveau IV à 64 bits aléatoire, pseudo-aléatoire ou non répétitif doit être utilisé pour chaque période de validité. Le même IV peut servir dans la période de validité de la clé associée.

4.2 Chiffrement à rebouclage par le chiffré (CFB)

Un nouveau IV à 48 ou 64 bits aléatoire, pseudo-aléatoire ou non répétitif doit être utilisé pour chaque message.

1) À publier.

5 Séquence de texte initiale (ITS)

Dans le cas de CBC, si le IV n'est pas changé d'un message à l'autre, une nouvelle séquence de texte initial (ITS) à 64 bits aléatoire, pseudo-aléatoire ou non répétitive doit immédiatement précéder les données de message à protéger. Si un nouveau IV aléatoire, pseudo-aléatoire ou non répétitif est utilisé d'un message à l'autre, aucune ITS n'est nécessaire.

6 Zone de remplissage (mode CBC uniquement)

Le remplissage doit être présent dans tout message CBC. Le texte clair doit être complété jusqu'à obtenir un multiple de 64 bits avant le chiffrement en mode CBC. Le chiffrement doit être effectué à l'aide de bits ou d'octets en ajoutant une zone de remplissage à la fin du texte clair (comme indiqué en grisé sur la figure 1). Après déchiffrement, la zone de remplissage doit être rejetée.

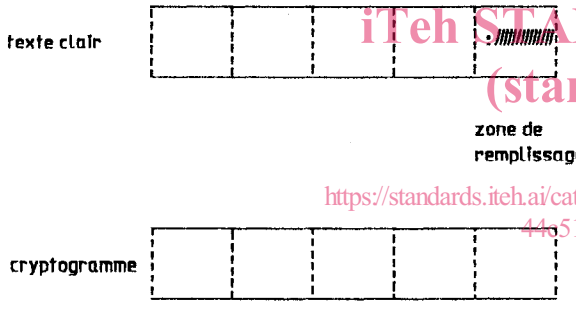
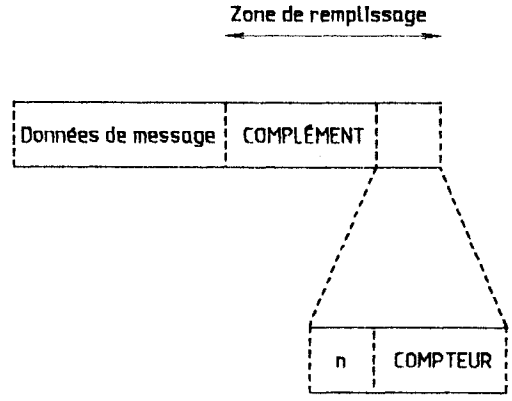


Figure 1 — Remplissage d'un message

Lorsqu'on complète avec des bits, la zone de remplissage doit comprendre entre 8 et 71 bits divisés en deux sous-zones (voir figure 2). La première sous-zone (complément) doit comprendre entre 0 et 63 bits avec un contenu arbitraire. La deuxième sous-zone (comptage) doit contenir sur 8 bits le nombre de bits dans la zone de remplissage, entre 8 et 71. Le bit le plus à gauche du compteur doit indiquer que le compteur est donné en bits (valeur exprimée 1). Les bits restants du compteur doivent contenir un nombre binaire non signé. Ce nombre doit être le nombre total de bits dans la zone de remplissage. Voir le tableau 1 pour de plus amples informations sur le remplissage à l'aide de bits (mode CBC uniquement).



NOTE — Lorsque n = 1, le comptage est exprimé en bits; lorsque n = 0, le comptage est exprimé en octets.

Figure 2 — Format de zone de remplissage

Lorsqu'on complète avec des octets, la zone de remplissage doit comprendre 1 à 8 octets divisés en deux sous-zones (voir figure 2). La première sous-zone (complément) doit comprendre 0 à 7 octets avec un contenu arbitraire. La deuxième sous-zone (comptage) doit contenir sur un octet le nombre d'octets de la zone de remplissage entre 1 et 8. Le bit le plus à gauche du comptage doit indiquer que le comptage est en octets (valeur exprimée 0). Les bits restants du compteur doivent contenir un nombre binaire non signé. Ce nombre doit être le nombre total d'octets de remplissage dans la zone de remplissage. Voir le tableau 2 pour de plus amples informations sur le remplissage à l'aide d'octets (mode CBC uniquement).

Tableau 1 — Remplissage à l'aide de bits (mode CBC uniquement)

Nombre de bits dans le dernier bloc de texte clair	Nombre de bits de complément	Nombre de bits dans la zone de remplissage	Compteur (8 bits)
64	56	64	11000000
63	57	65	11000001
62	58	66	11000010
.	.	.	.
.	.	.	.
.	.	.	.
58	62	70	11000110
57	63	71	11000111
56	0	8	10001000
55	1	9	10001001
54	2	10	10001010
.	.	.	.
.	.	.	.
.	.	.	.
2	54	62	10111110
1	55	63	10111111

Tableau 2 — Remplissage à l'aide d'octets (mode CBC uniquement)

Nombre d'octets dans le dernier bloc de texte clair	Nombre d'octets de complément	Nombre d'octets dans la zone de remplissage	Compteur (8 bits)
8	7	8	00001000
7	0	1	00000001
6	1	2	00000010
5	2	3	00000011
4	3	4	00000100
3	4	5	00000101
2	5	6	00000110
1	6	7	00000111

7 Chiffrement et déchiffrement indépendants des éléments de chiffrement

Voir ISO 10126-1:1991, 5.3, méthode 1.

Le IV utilisé pour chiffrer le $n^{ième}$ élément de chiffrement doit être formé en ajoutant modulo-2 le IV et la valeur de n en binaire non signé justifiée à droite: IVn = IV + n. Pour le premier chiffrement, l'élément n doit avoir la valeur 1.

Dans le cas de CBC, si le IV n'est pas modifié d'un message à l'autre, une nouvelle ITS aléatoire, pseudo-aléatoire ou non répétitive doit apparaître au début de chaque élément de chiffrement.

Dans le cas de CBC, chaque élément de chiffrement doit être rempli avant chiffrement conformément à l'article 6.

CDU 336.719.2:355.405.2:681.3.04

Descripteurs: banque, message, protection de l'information, combinaison de code, algorithme.

Prix basé sur 3 pages