NORME INTERNATIONALE

ISO 8731-1

Première édition
1987-06-01

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

Banque — Algorithmes approuvés pour l'authentification des messages —

Partie 1 : DEA

Banking — Approved algorithms for message authentication —

Partie 1 : DEA

Numéro de référence
ISO 8731-1 : 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 8731-1 a été élaborée par le comité technique ISO/TC 68, *Banque.*

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

Banque — Algorithmes approuvés pour l'authentification des messages —

Partie 1 : DEA

0 Introduction

L'ISO 8731 spécifie dans des parties séparées les algorithmes d'authentification approuvés. Chaque algorithme a été approuvé s'il répond aux exigences en matière d'authentification spécifiées dans l'ISO 8730.

1 Objet et domaine d'application

La présente partie de l'ISO 8731 traite de l'Algorithme de chiffrage des données [DEA (Data Encryption Algorithm)] en tant que méthode à utiliser pour le calcul du Code d'authentification des messages [MAC (Message Authentification Code)].

Bien que le DEA puisse être mis en œuvre en logiciel, ses mises en œuvre en matériel se font à des vitesses nettement plus élevées.

2 Références

ISO 8730, *Opérations bancaires — Spécifications liées à la normalisation de l'authentification des messages.*

ANSI X3.92-1981, *Norme nationale américaine pour les systèmes d'information — Algorithme de chiffrage des données.*

ANSI X3.106-1983, *Norme nationale américaine pour les systèmes d'information — Algorithme de chiffrage des données — Mode de fonctionnement.*

ANSI X9.9-1982, *Authentification des messages des institutions financières (commerce de gros).*

3 Source de l'algorithme DEA

Le DEA est publié en tant que ANSI X3.92.

ANSI X3.92 spécifie que les clés binaires 8, 16, 24, 32, 40, 48, 56 et 64 seront utilisées comme bits impairs de priorité pour les octets sur lesquels ils apparaissent. L'objet de la présente Norme internationale n'est pas de spécifier l'utilisation de ces éléments binaires.

4 Spécification de l'algorithme

4.1 Clé cryptographique DEA

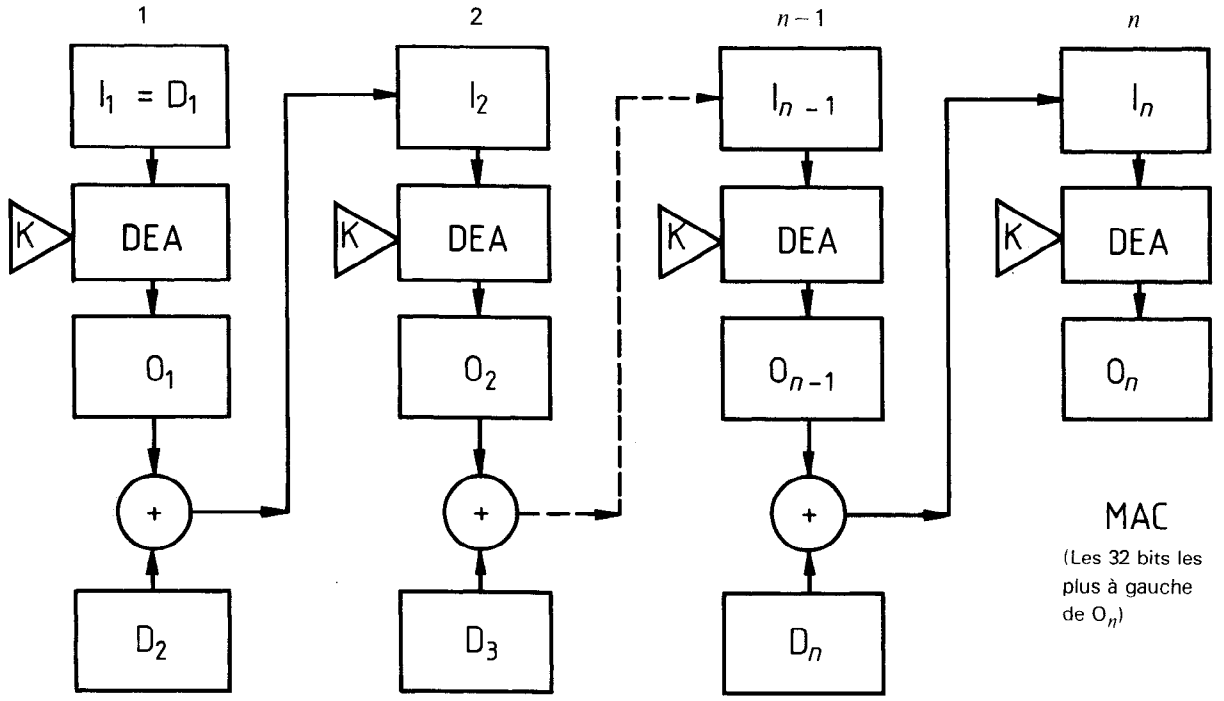
La clé cryptographique DEA est constituée de 64 éléments binaires dont 56 sont utilisés par l'algorithme d'authentification (constituant la clé active) et dont 8 sont disponibles pour détecter les erreurs à l'intérieur de la clé. Si les 64 éléments binaires sont numérotés de gauche à droite (1, 2, ..., 64), les éléments binaires 8, 16, 24, ..., 64 servent au contrôle de la parité.

Lorsqu'on écrit une clé DEA, on doit la représenter par 8 paires de caractères hexadécimaux, les paires étant séparées par un espace (hh hh hh hh hh hh hh hh).

La clé active doit être générée de façon aléatoire ou pseudo-aléatoire. Toute la clé de 64 éléments binaires doit être protégée pendant toute sa vie active contre tous tiers non autorisés. Les clés doivent être changées de temps en temps.

4.2 Génération du code d'authentification de message (MAC) en utilisant le DEA

Le MAC est généré tel qu'indiqué à la figure. Le DEA doit être utilisé par enchaînement des blocs (cipher block chaining) avec le vecteur d'initialisation à zéro, tel que spécifié dans l'ANSI X3.106-1983. Le Registre d'Entrée (I_1) (voir la figure) est initialisé avec les 64 premiers éléments binaires de données (D_1) qui doivent être authentifiés. Cette entrée passe par le DEA qui utilise une clé d'authentification (K) pour générer 64 éléments binaires dans le registre de sortie (O_1). Les 64 éléments binaires de données suivants (D_2) qui doivent être authentifiés sont soumis à une opération addition modulo 2 avec les 64 éléments binaires du registre de sortie et le résultat est chargé dans le registre d'entrée (I_2). Ce processus se poursuit jusqu'à ce qu'il ne reste que 64 éléments binaires à authentifier. Ces éléments binaires restants doivent être cadrés à gauche et l'on doit ajouter des zéros pour former un bloc de données de 64 éléments binaires (D_n). Ce bloc est alors soumis à une opération addition modulo 2 avec les 64 éléments binaires dans le registre de sortie. Le résultat (I_n) passe par le DEA, ce qui génère le bloc final de sortie de 64 éléments binaires (O_n). Les 32 éléments binaires à l'extrême gauche de la sortie finale (O_n) constituent le MAC. L'ANSI X9.9.1982 donne un exemple du calcul du MAC.



Légende

I : Entrée
DEA : Algorithme de chiffrage des données (mode chiffrage)
O : Sortie
K : Clé DEA
D : Bloc de données
+ : addition modulo 2

Figure — Algorithme d'authentification

CDU 681.3.04 : 336.717

Descripteurs : banque, document bancaire, message, traitement de l'information, authentification.

Prix basé sur 2 pages