NORME INTERNATIONALE

ISO/CEI 9797

Première édition
1989-12-01

Techniques cryptographiques — Mécanisme d'intégrité de données utilisant une fonction de contrôle cryptographique employant un algorithme de chiffrement par bloc

Data cryptographic techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm

Numéro de référence
ISO/CEI 9797:1989(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 de l'ISO ou de la CEI participent au développement de Normes internationaeles 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 et 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 9797 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*.

L'annexe A de la présente Norme internationale est donnée uniquement à titre d'information.

ISO/CEI Copyright Office • Case postale 56 • CH-1211 Genève 20 • Suisse
Version française tirée en 1990
Imprimé en Suisse

Introduction

Le calcul décrit dans la présente Norme internationale est semblable à celui utilisé dans l'ISO 8731-1 et dans la norme américaine ANSI X9.9, sauf qu'il est défini en termes d'algorithme utilisant des blocs de données de *n-bits* et une valeur de contrôle de *m-bits*. C'est pourquoi les calculs des valeurs de contrôle cryptographiques décrites dans l'ISO 8731 et l'ANSI X9.9 sont des sous-ensembles de la présente Norme internationale pour $n = 64$ et $m = 32$, en utilisant DEA (voir ANSI X3:1981).

Techniques cryptographiques — Mécanisme d'intégrité de données utilisant une fonction de contrôle cryptographique employant un algorithme de chiffrement par bloc

1 Domaine d'application

La présente Norme internationale spécifie une méthode d'utilisation d'une clé et des algorithmes de *n-bits* en mode de chiffrement par bloc pour calculer une valeur de contrôle cryptographique de *m-bits* que l'on peut utiliser comme mécanisme d'intégrité de données pour détecter si les données ont été modifiées de façon non autorisée. Le degré d'intégrité des données dépend de la longueur de la clé et de son caractère secret, de la nature de l'algorithme cryptographique et de m, la longueur de la valeur de contrôle.

La présente Norme internationale peut s'appliquer aux services de sécurité de toute architecture, de tout processus ou de toute application de sécurité.

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 Norme internationale. 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 Norme internationale 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 8731-1:1987, *Banque — Algorithmes approuvés pour l'authentification de messages — Partie 1: DEA.*

ANSI X3.92:1981, *Algorithme de chiffrement de données.*

ANSI X9.9:1986, *Authentification de messages des institutions financières.*

3 Terminologie

La valeur de contrôle cryptographique est indifféremment désignée par les termes:

code d'authentification de message (MAC);

code d'intégrité de message (MIC); ou

code de détection de modification (MDC).

La présente Norme internationale désigne la valeur de contrôle par le terme MAC.

4 Prescriptions

La valeur m sera inférieure ou égale à la taille de bloc n. Le résultat du calcul et de tout processus optionnel sera un bloc d'information de taille n. La valeur de contrôle cryptographique est constituée des m-bits de gauche du bloc final de n-bits. Si l'on suppose que l'algorithme a une solidité adéquate, plus la valeur de m sera grande, plus la protection sera grande.

5 Calcul du MAC

5.1 Algorithme cryptographique de *n-bits*

Le MAC est calculé comme le montre la figure 1. Les bits de données de D, pour lesquels la valeur de contrôle cryptographique doit être calculée, sont divisés en blocs de *n-bits*, $D_1, D_2 \ldots, D_{q-1}$ suivis par un bloc éventuellement incomplet D_q.

5.2 Clé cryptographique

Il convient que la clé soit générée de façon aléatoire ou pseudo-aléatoire. Il convient de changer la clé périodiquement. Si le même algorithme est utilisé pour le chiffrement du message, la clé utilisée pour

le calcul du MAC devrait être différente de celle utilisée pour le chiffrement.

5.3 Étape initiale

Le registre d'entrée I_1 est initialisé avec les n premiers bits des données D_1. Cette entrée I_1 passe dans l'algorithme qui utilise la clé K pour produire n bits dans le registre de sortie O_1.

5.4 Étapes suivantes jusqu'à l'étape finale

Le second bloc de n bits des données D_2 sont additionnés, par un ou exclusif bit à bit, aux n bits du registre de sortie O_1 et le résultat I_2 est chargé dans le registre d'entrée. Ce processus se poursuit jusqu'à ce qu'il reste n bits ou moins dans les données pour lesquelles il reste à calculer la valeur de contrôle cryptographique.

5.5 Étape finale

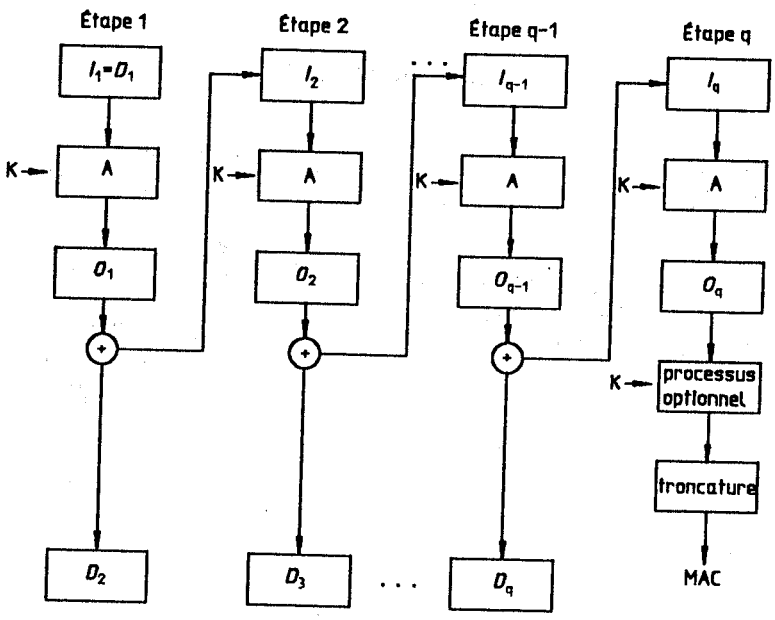
Les bits restants sont cadrés à gauche et le bloc final D_q de n bits est obtenu en ajoutant un «1» et autant de bits zéro que nécessaire. Ce bloc est ensuite additionné, par un ou exclusif bit à bit, au contenu du registre de sortie O_{q-1}. Le résultat I_q passe dans l'algorithme pour produire le bloc final de sortie de n bits O_q. Si des bits zéro sont ajoutés, le receveur doit soit connaître le nombre nécessaire auparavant soit recevoir ce nombre d'une façon qui assure son intégrité.

5.6 Processus optionnel

À ce stade, O_q peut être soumis à un traitement supplémentaire optionnel. Par exemple, l'ANSI X9.19, qui utilise le même algorithme, déchiffre O_q avec une clé secrète différente et chiffre ensuite le résultat avec la clé d'origine.

5.7 Troncature pour $m \leqslant n$

La valeur de contrôle cryptographique est calculée en prenant les m bits de gauche du bloc final de n bits.



Légende :

I entrée
A algorithme de chiffrement de *n* bits
O sortie
K clé
D bloc de données
⊕ ou exclusif

Figure 1 — Calcul du MAC

Annexe A
(informative)

Bibliographie

[1] ISO 2382-9:1984, *Traitement des données — Vocabulaire — Partie 09: Communication des données.*

[2] ISO 7498:1984, *Systèmes de traitement de l'information — Interconnexion des systèmes ouverts — Modèle de Référence de base.*

[3] ISO 7498-2:1989, *Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Modèle de référence de base — Partie 2: Architecture de sécurité (Publiée actuellement en anglais seulement).*

[4] ISO 9979:1989[1)], *Techniques cryptographiques — Procédures pour l'enregistrement des algorithmes cryptographiques.*

1) À publier.

CDU 681.3.04:003.26

Descripteurs: message, traitement de l'information, transmission de données, authentification, code détecteur d'erreur, fonction de contrôle algorithme.

Prix basé sur 3 pages