INTERNATIONAL STANDARD ISO/IEC 19772:2009
TECHNICAL CORRIGENDUM 1

Published 2014-09-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Security techniques — Authenticated encryption

TECHNICAL CORRIGENDUM 1

Technologies de l'information — Techniques de sécurité — Chiffrage authentifié

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum ## to ISO/IEC 19772:2009 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology.*

A) Page 15, Clause 10.2

Replace the definition of δ with the following text:
The decryption function, i.e. a function which takes as input a block cipher key K_1, a Starting Variable S, and an encrypted data string C' and, using the selected mode of operation, outputs a decrypted data string: the output is written $\delta_{K_1,S}(C')$.

Replace the definition of ε with the following text:
The encryption function, i.e. a function which takes as input a block cipher key K_1, a Starting Variable S, and a data string D and, using the selected mode of operation, outputs an encrypted data string: the output is written $\varepsilon_{K_1,S}(D)$.

B) Page 16, Clause 10.4

Replace steps a), b) and c) with the following:
a) A Starting Variable S appropriate for use with the selected block cipher mode of operation shall be selected. This variable shall be statistically distinct for every message to be protected under a given key, and must be made available to the recipient of the message. Further possible requirements for S are as described in the appropriate clauses of ISO/IEC 10116, and further guidance is provided in A.7.

ICS 35.040 **Ref. No. ISO/IEC 19772:2009/Cor.1:2014(E)**

© ISO/IEC 2014 – All rights reserved

Published in Switzerland

NOTE If the Starting Variable is chosen uniformly at random from the space of all possible Starting Variables (as is strongly recommended – see Annex A.7), and the number of messages encrypted using a single key is bounded appropriately, then the use of distinct Starting Variables is overwhelmingly likely, i.e. the Starting Variables can be regarded as statistically distinct.

b) Let C' = $\varepsilon_{K_1,S}(D)$, using the Starting Variable S.

c) Let T = $f_{K_2}(S \,||\, C')$.

Replace the last line of 10.4 with the following:

$C = C' \,||\, T$, together with the Starting Variable S.

C) Page 16, Clause 10.5

In the first line, replace 'string C' with:

string C, with accompanying Starting Variable S
Replace step c) with the following:
c) Let T' = $f_{K_2}(S \,||\, C')$

Replace step e) with the following:

e) Let D = $\delta_{K_1,S}(C')$, using the Starting Variable S.

D) Page 17, Clause 11.2

In the definition of G, replace '11.4' with '11.5'.

E) Page 19, Clause 11.6

Replace step h) with the following:

h) Let $T = (G(H, A, C_1||C_2||...||C_m) \oplus e_K(Y_0)|_t$.

F) Page 19, Clause 11.7

Replace step e) with the following:

e) Let $T' = (G(H, A, C_1||C_2||...||C_m) \oplus e_K(Y_0)|_t$.

G) Page 22, Annex A.7

Add the following two paragraphs after the existing text:

Regardless of the mode of encryption chosen, use of a Starting Variable chosen uniformly at random from the set of possible Starting Variables is strongly recommended. If this recommendation is not followed then the result of Bellare and Namprempre (referred to in the note in 10.1) will not apply. Moreover, in some circumstances attacks may be possible. In this connection note that, for CBC mode, Annex B.2.1 of ISO/IEC 10116 states that 'A randomly chosen statistically unique Starting Variable is recommended'.

© ISO/IEC 2014 – All rights reserved

The choice of MAC technique should take into account the context of use of the authenticated encryption technique, and the advice provided in ISO/IEC 9797 should be carefully followed. In particular, if a block cipher based MAC from ISO/IEC 9797-1 is chosen, then: (a) MAC algorithm 1 should only be used if the message length is fixed, and (b) Padding Method 1 should only be used if the message length is fixed.

© ISO/IEC 2014 – All rights reserved