

BS ISO/IEC 10118-2:2010

Incorporating corrigendum December 2011



BSI Standards Publication

Information technology

— Security techniques

— Hash-functions

Part 2: Hash-functions using an
n-bit block cipher

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO/IEC 10118-2:2010, incorporating corrigendum December 2011.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2012

ISBN 978 0 580 76008 2

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2010.

Amendments/corrigenda issued since publication

Date	Text affected
31 January 2012	Implementation of ISO/IEC corrigendum December 2011: Amended Annex B.3 Padding methods 1 and 2