

ISO/IEC 10118-2:2000-12 (E)

Information technology - Security techniques; Hash-functions - Part 2: Hash-functions using an n-bit block cipher

Contents		Page
Foreword		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Symbols and abbreviated terms	1
5	Use of the general model	2
6	Hash-function one	2
6.1	Parameter selection	2
6.2	Padding method	2
6.3	Initializing value	2
6.4	Round-function	2
6.5	Output transformation	3
7	Hash-function two	3
7.1	Parameter selection	3
7.2	Padding method	3
7.3	Initializing value	3
7.4	Round-function	4
7.5	Output transformation	5
8	Hash-function three	5
8.1	General	5
8.2	Parameter selection	5
8.3	Padding method	5
8.4	Initializing value	6
8.5	Round-function	6
8.6	Output transformation	8
9	Hash-function four	8
9.1	General	8
9.2	Parameter selection	8
9.3	Padding method	8
9.4	Initializing value	8
9.5	Round-function	8
9.6	Output transformation	10
Annex A (informative)	Use of DEA	11
Annex B (informative)	Examples	14
Bibliography		19