ISO/IEC JTC1 SC27 WG2

Presentation slides for

CRYPTREC Cryptography Symposium

October 2000

by Michael Ward

ISO/IEC JTC1 SC27 WG2

Joint Technical Committee 1

- Information Technology

Sub Committee 27

- Security Techniques

Working Group 2

- Security Techniques and Mechanisms

Existing WG2 Standards

- Modes of operation for a 64-bit block cipher algorithm (8372)
- Modes of operation for an n-bit block cipher algorithm (10116)
- Entity authentication (9798)
- Message authentication codes (9797)
- Non-repudiation (13888)

Existing Standards (cont'd)

- Digital signature scheme giving message recovery (9796)
- Digital signatures with appendix (14888)
- Hash functions (10118)
- Key management (11770)

Upcoming Standards

- Cryptographic techniques based on elliptic curves (15946)
- Time stamping services and protocols (18014)
- Random number generation (18031)
- Prime number generation (18032)
- Encryption algorithms (18033)

Encryption Algorithms
18033

- Part 1: General
- Part 2: Asymmetric ciphers
- Part 3: Block ciphers
- Part 4: Stream ciphers

A restricted selection of evaluated algorithms rather than a single choice or an open registry.