Information technology — Security techniques — Encryption algorithms —

Part 2: Asymmetric ciphers

Technologies de l’information — Techniques de sécurité — Algorithmes de chiffrement —

Partie 2: Chiffres asymétriques
## Contents

1. Scope ...................................................... 1
2. Normative references ...................................... 1
3. Definitions ................................................... 2
4. Symbols and notation ....................................... 7
5. Mathematical conventions .................................... 8
   5.1 Functions and algorithms ................................. 8
   5.2 Bit strings and octet strings ............................ 9
   5.3 Finite Fields ........................................... 10
   5.4 Elliptic curves ........................................ 12
6. Cryptographic transformations .............................. 14
   6.1 Cryptographic hash functions ........................... 14
   6.2 Key derivation functions ............................... 15
   6.3 MAC algorithms ........................................ 16
   6.4 Block ciphers .......................................... 16
   6.5 Symmetric ciphers ...................................... 17
7. Asymmetric ciphers .......................................... 19
   7.1 Plaintext length ........................................ 20
   7.2 The use of labels ....................................... 21
   7.3 Ciphertext format ...................................... 21
   7.4 Encryption options ..................................... 21
   7.5 Method of operation of an asymmetric cipher .......... 22
   7.6 Allowable asymmetric ciphers ......................... 22
8. Generic hybrid ciphers ...................................... 22
   8.1 Key encapsulation mechanisms ......................... 23
   8.2 Data encapsulation mechanisms ....................... 24
   8.3 HC ...................................................... 25
9. Constructions of data encapsulation mechanisms ........ 26
   9.1 DEM1 .................................................. 26
   9.2 DEM2 .................................................. 27
   9.3 DEM3 .................................................. 28
10. ElGamal-based key encapsulation mechanisms ............ 30
   10.1 Concrete groups ....................................... 30
   10.2 ECIES-KEM ............................................ 32
   10.3 PSEC-KEM ............................................ 34
   10.4 ACE-KEM ............................................. 36
11. RSA-based asymmetric ciphers and key encapsulation mechanisms ........ 39
   11.1 RSA key generation algorithms ....................... 39
   11.2 RSA Transform ....................................... 40
   11.3 RSA encoding mechanisms ............................. 40
   11.4 RSAES ................................................. 42
   11.5 RSA-KEM ............................................. 44
12. Ciphers based on modular squaring ........................ 45
Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

ISO/IEC 18033-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.

ISO/IEC 18033 consists of the following parts, under the general title Information technology — Security techniques — Encryption algorithms:

— Part 1: General
— Part 2: Asymmetric ciphers
— Part 3: Block ciphers
— Part 4: Stream ciphers
Introduction

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this International Standard may involve the use of patents.

The ISO and IEC take no position concerning the evidence, validity and scope of this patent right. The holder of this patent right has assured the ISO and IEC that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with the ISO and IEC. Information may be obtained from:

ISO/IEC JTC 1/SC 27 Standing Document 8 (SD8) "Patent Information"

Standing Document 8 (SD8) is publicly available at: http://www.ni.din.de/sc27

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.
Information technology — Security techniques — Encryption algorithms —

Part 2:
Asymmetric ciphers

1 Scope

This part of ISO/IEC 18033 specifies several asymmetric ciphers. These specifications prescribe the functional interfaces and correct methods of use of such ciphers in general, as well as the precise functionality and cipher text format for several specific asymmetric ciphers (although conforming systems may choose to use alternative formats for storing and transmitting cipher-texts).

A normative annex (Annex A) gives ASN.1 syntax for object identifiers, public keys, and parameter structures to be associated with the algorithms specified in this part of ISO/IEC 18033.

However, these specifications do not prescribe protocols for reliably obtaining a public key, for proof of possession of a private key, or for validation of either public or private keys; see ISO/IEC 11770-3 for guidance on such key management issues.

The asymmetric ciphers that are specified in this part of ISO/IEC 18033 are indicated in Clause 7.6.

NOTE Briefly, the asymmetric ciphers are:
— ECIES-HC; PSEC-HC; ACE-HC: generic hybrid ciphers based on ElGamal encryption;
— RSA-HC: a generic hybrid cipher based on the RSA transform;
— RSAES: the OAEP padding scheme applied to the RSA transform;
— HIME(R): a scheme based on the hardness of factoring.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.


