

Security Mechanisms

Thorsten Fischer
<t.fischer@rhul.ac.uk>
Revision : 1.1

March 22, 2004

One

foo

The Register of Cryptographic Algorithms, ISO/IEC 9979 [4], is a result of the ISO's tries to standardize cryptographic algorithms. The standardisation of DES failed due to political reasons after it was made a FIPS standard [5] and also an ANSI standard [1]. Since then, ISO is not standardising algorithms, but merely providing a register for them. The register's purpose is that, in its own words, *it serves as a common reference point for the identification of cryptographic algorithms by a unique name*. So it is basically a database using an algorithm name as a unique key to point to a number of characteristics of this algorithm. Communicating entities can then use these entries to define what they actually mean when they talk about an algorithm.

An entry in the register must first of all consist of a formal unique name and a number of proprietary names for it. The intended range of application has to be specified, along with cryptographic interface parameters and a set of test values to make it possible to test an implementation. Also, the organisation requesting the registration of an algorithm must be identified. The dates of registration and modification of the entry are recorded, along with the fact whether the algorithm is a national standard and any patent information regarding the algorithm.

Optional entry information are a list of references to associated algorithms and a description of it, thus making it possible to actually implement the algo-

rithm, a list of modes of operation the algorithm might be used with, and any other additional arbitrary information that the requesting organisation feels the need to submit.

IEEE 1363 [2] covers public key encryption techniques, including encryption, signatures and key establishment.

- differences to IEEE1363 and ISO 18033 [3]

Two

foo

The usage of hybrid cipher systems is heavily endorsed by the ISO/IEC 18033 standard. A hybrid cipher uses symmetric and asymmetric techniques in encrypting messages: first, the message is encrypted using a symmetric cipher. Then, the key used for this encryption process is encrypted using an asymmetric technique. Decrypting the message works by decrypting the key first and then using it to decrypt the actual message.

In ISO/IEC 18033, hybrid algorithms are built on two blocks, a KEM (key encapsulation mechanism) to produce a symmetric key and its encipherment from a private asymmetric key, and a DEM (data encapsulation mechanism) to use that symmetric key to produce an encipherment of the message.

The main advantage of a hybrid cipher is that

- advantages and disadvantages of hybrid algorithms

Three

foo.

- describe two of the modes in ISO 10116 - why would ECB not always be used?

Four

foo.

Five

foo.

Six

foo.

References

- [1] ANSI-X3.92. *American National Standard for Data Encryption Algorithm (DEA)*. American National Standards Institute, 1981.
- [2] IEEE 1363. *FXMPE: Standard Specifications for Public Key Cryptography*. IEEE New York, 2000.
- [3] ISO/IEC 18033. *International Encryption Standard*. International Organisation for Standardization.
- [4] ISO/IEC 9979. *Register of Cryptographic Algorithms*. International Organisation for Standardization.
- [5] National Bureau of Standards, NBS FIPS PUB 46. *Data Encryption Standard*. US Department of Commerce, January 1977.