Specifications of e-Government Recommended Ciphers

The "CRYPTREC Ciphers List" has been published on March, 2013. The list is the revision of the previous "e-Government Recommended Ciphers List" (*1). The CRYPTREC Ciphers List consists of three lists: "e-Government Recommended Ciphers List", "Candidate Recommended Ciphers List" and "Monitored Ciphers List".
The specifications of the ciphers in these lists are shown in the following tables. Please note that the ciphers listed in the "CRYPTREC Ciphers List" are limited to those in the following tables.

For the specifications of the ciphers in the previous "e-Government Recommended Ciphers List", please refer to "Specifications of e-Government Recommended Ciphers".

Specifications of ciphers in the e-Government Recommended Ciphers List

Classification		Cipher	Specification
Public key ciphers	Signature	DSA	NIST FIPS PUB 186-4
		ECDSA	SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) (*2) or ANS X9.62-2005 (*1)
		RSA-PSS	Public-Key Cryptography Standards (PKCS)#1 v2.2
		RSASSA-PKCS1-v1_5	Public-Key Cryptography Standards (PKCS)#1 v2.2
	Confidentiality	RSA-OAEP	Public-Key Cryptography Standards (PKCS)#1 v2.2
	Key exchange	DH	ANS X9.42-2003 (*1) or Specified as FFC DH primitive in NIST SP 800-56A Revision 2 (May 2013)
		ECDH	SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) (*2) or Specified as C(2e, 0s, ECC CDH) in NIST SP 800-56A Revision 2 (May 2013)
Symmetric key ciphers	64-bit block ciphers	3-key Triple DES	NIST SP 800-67 Revision 1 (January 2012)
	128-bit block ciphers	AES	NIST FIPS PUB 197
		Camellia	Algorithm specifications of 128-bits block cipher Camelia (2nd version: September 26, 2001)
	Stream ciphers	KCipher-2	Stream Cipher KCipher-2 (March 31, 2017 Version1.2)
Hash functions		SHA-256	NIST FIPS PUB 180-4
		SHA-384	NIST FIPS PUB 180-4

		SHA-512	NIST FIPS PUB 180-4
Modes of operation	Encryption modes	CBC	NIST SP 800-38A
		CFB	NIST SP 800-38A
		CTR	NIST SP 800-38A
		OFB	NIST SP 800-38A
	Authenticated encryption modes	CCM	NIST SP 800-38C
		GCM	NIST SP 800-38D
Message authentication codes		CMAC	NIST SP 800-38B
		HMAC	NIST FIPS PUB 198-1
Entity authentication		ISO/IEC 9798-2	ISO/IEC 9798-2:2008 (*1), ISO/IEC 9798-2:2008/Cor 1:2010, ISO/IEC 9798-2:2008/Cor 2:2012, ISO/IEC 9798-2:2008/Cor 3:2013
		ISO/IEC 9798-3	ISO/IEC 9798-3:1998(*1), ISO/IEC 9798-3:1998/Amd 1:2010 (*1), ISO/IEC 9798-3:1998/Cor 1:2009, ISO/IEC 9798-3:1998/Cor 2:2012

(*1) Specifications can be purchased from Japanese Standards Association.
(*2) A newer version has been published. CRYPTREC is considering the change of reference.

When a specification is linked to outside of this domain, the specification is managed by the linked organization.
If you find a broken link, please inform it to CRYPTREC Secretariat.

Specifications of ciphers in the Candidate Recommended Ciphers List

Classification		Cipher	Specification
Public key ciphers	Signature	NA	
	Confidentiality	NA	
	Key exchange	PSEC-KEM	PSEC-KEM specification (April 14, 2008)
Symmetric key ciphers	64-bit block ciphers	CIPHERUNICORN-E	Cryptographic specifications CIPHERUNICORN-E (May 8, 2002)
		Hierocrypt-L1	Cryptographic specifications: Hierocrypt-L1 (May 2002)
		MISTY1	Cryptographic specifications MISTY1 (updated May 13, 2002)
	128-bit block ciphers	CIPHERUNICORN-A	Cryptographic specifications CIPHERUNICORN-A (May 8, 2002)
		CLEFIA	The 128-bit Blockcipher CLEFIA Specification Version 1.0 (January 29, 2010)
		Hierocrypt-3	Specification on a Block Cipher : Hierocrypt-3 (May 2002)
		SC2000	The Block Cipher SC2000 Cryptographic Techniques Specifications (September 26, 2001)

	Stream ciphers	MUGI	Pseudo random number generator MUGI specifications, version 1.3 (May 14, 2002)
		Enocoro-128v2	Pseudorandom Number Generator Enocoro, Specification Ver. 2.0 (2 February 2010)
		MULTI-S01	Specifications MULTI-S01; Ciphers, Version 1.2 (May 14, 2002)
Hash functions		SHA-512/256	NIST FIPS PUB 180-4
		SHA3-256	NIST FIPS PUB 202
		SHA3-384	NIST FIPS PUB 202
		SHA3-512	NIST FIPS PUB 202
		SHAKE128	NIST FIPS PUB 202
		SHAKE256	NIST FIPS PUB 202
Modes of operation	Encryption modes	NA	
	Authenticated encryption modes	NA	
Message authentication codes		PC-MAC-AES	Specification of Cryptographic Technique PC-MAC-AES (February 3, 2010)
Entity authentication		ISO/IEC 9798-4	ISO/IEC 9798-4:1999 (*1), ISO/IEC 9798-4:1999/Cor 1:2009, ISO/IEC 9798-4:1999/Cor 2:2012

(*1) Specifications can be purchased from Japanese Standards Association.

When a specification is linked to outside of this domain, the specification is managed by the linked organization.
If you find a broken link, please inform it to CRYPTREC Secretariat.

Specifications of ciphers in the Monitored Ciphers List

Classification		Cipher	Specification
Public key ciphers	Signature	NA	
	Confidentiality	RSAES-PKCS1-v1_5	Public-Key Cryptography Standards (PKCS)#1 v2.2
	Key exchange	NA	
Symmetric key ciphers	64-bit block ciphers	NA	
	128-bit block ciphers	NA	
	Stream ciphers	128-bit RC4 (*2) (Arcfour)	It is assumed that the use of 128-bit RC4 is limited to SSL3.0/TLS1.0 or higher Refer to the following literature for technical information related to the specifications. Fluhrer Scott, Itsik Mantin, and Adi Shamir, “Attacks On RC4 and WEP”, CryptoBytes, Vol.5, No.2, pp.26-34, Summer/Fall 2002

Hash functions		RIPEMD-160	The hash function RIPEMD-160
		SHA-1	NIST FIPS PUB 180-4
Modes of operation	Encryption modes	NA	
	Authenticated encryption modes	NA	
Message authentication codes		CBC-MAC	ISO/IEC 9797-1:2011 (*1)
Entity authentication		NA	

(*1) Specifications can be purchased from Japanese Standards Association.
(*2) RC4 is trademarked by EMC Corporation.

When a specification is linked to outside of this domain, the specification is managed by the linked organization.
If you find a broken link, please inform it to CRYPTREC Secretariat.

Contact: CRYPTREC Secretariat info@cryptrec.go.jp