



Cryptographic Algorithm Validation Testing.



Table of Contents

FIPS APPROVED ALGORITHMS.....	3
TDES	3
AES	4
DSA	4
DSA-2.....	4
SHA	6
RNG.....	7
RSA	8
HMAC.....	10
CCM.....	10
ECDSA	10
CMAC	11
DRBG	11
KAS FFC.....	12
KAS ECC.....	13
CGM	14
NON FIPS APPROVED ALGORITHMS.....	15
DES	15
MAC.....	15
FIPS 171.....	15
RC4.....	15
Blowfish.....	15

FIPS Approved algorithms

For more information see: <http://csrc.nist.gov/groups/STM/cavp/index.html>

TDES: (FIPS 46-3 & FIPS 81)			
Support for testing: http://csrc.nist.gov/groups/STM/cavp/documents/des/tripledesval.html			
	ECB	with state options	<input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		with keying options	<input type="checkbox"/> K1, K2, K3 independent
			<input type="checkbox"/> K1 = K3, K2 independent
	CBC	with state options	<input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		with keying options	<input type="checkbox"/> K1, K2, K3 independent
			<input type="checkbox"/> K1 = K3, K2 independent
	CBC-1	with state options	<input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		with keying options	<input type="checkbox"/> K1, K2, K3 independent
			<input type="checkbox"/> K1 = K3, K2 independent
	CFB	with state options	1 Bit <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
			8 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
			64 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		with keying options	<input type="checkbox"/> K1, K2, K3 independent
			<input type="checkbox"/> K1 = K3, K2 independent
			<input type="checkbox"/> K1 = K2 = K3
	CFB-P	with state options	1 Bit <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
			8 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
			64 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		with keying options	<input type="checkbox"/> K1, K2, K3 independent
			<input type="checkbox"/> K1 = K3, K2 independent
			<input type="checkbox"/> K1 = K2 = K3
	OFB	with state options	<input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		with keying options	<input type="checkbox"/> K1, K2, K3 independent
			<input type="checkbox"/> K1 = K3, K2 independent
OFB-1	with state options	<input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt	
	with keying options	<input type="checkbox"/> K1, K2, K3 independent	
	with keying options	<input type="checkbox"/> K1 = K3, K2 independent	
	with keying options	<input type="checkbox"/> K1 = K2 = K3	
CTR	with state options	<input type="checkbox"/> Encrypt	
	with counter source options	<input type="checkbox"/> Internal, <input type="checkbox"/> External	

AES: FIPS 197		
Support for testing: http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html		
	ECB	128 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		192 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		256 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
	CBC	128 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		192 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		256 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
	OFB	128 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		192 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		256 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
	CFB 1	128 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		192 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		256 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
	CFB 8	128 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		192 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
		256 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
	CFB 128	128 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
192 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt		
256 Bits <input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt		
CTR	with state options 128 bits <input type="checkbox"/> Encrypt	
	with state options 192 bits <input type="checkbox"/> Encrypt	
	with state options 256 bits <input type="checkbox"/> Encrypt	
	with counter source options <input type="checkbox"/> Internal <input type="checkbox"/> External	

DSA: FIPS 186-2		
Support for testing: http://csrc.nist.gov/groups/STM/cavp/documents/dss/dsaval.htm		
	PQG Gen	1024
	PQG Ver	1024
	Key Pair Gen	1024
	Sig Gen	1024
	Sig Ver	1024

DSA-2: FIPS 186-2		
Support for testing: http://csrc.nist.gov/groups/STM/cavp/documents/dss/dsaval.htm		
	PQG Gen L=1024, N=160	SHA-1
		SHA-224
		SHA-256
		SHA-384
		SHA-512
	PQG Gen L=2048, N=224	SHA-224
		SHA-256

		SHA-384		
		SHA-512		
		PQG Gen L=2048, N=256	SHA-256	
			SHA-384	
			SHA-512	
		PQG Gen L=3072, N=256	SHA-256	
	SHA-384			
	SHA-512			
	PQG Ver L=1024, N=160	SHA-1		
		SHA-224		
		SHA-256		
		SHA-384		
		SHA-512		
	PQG Ver L=2048, N=224	SHA-224		
		SHA-256		
		SHA-384		
		SHA-512		
	PQG Ver L=2048, N=256	SHA-256		
		SHA-384		
		SHA-512		
PQG Ver L=3072, N=256	SHA-256			
	SHA-384			
	SHA-512			
	Key Pair L=1024, N=160	SHA-1		
		SHA-224		
		SHA-256		
		SHA-384		
		SHA-512		
	Key Pair L=2048, N=224	SHA-224		
		SHA-256		
		SHA-384		
		SHA-512		
	Key Pair L=2048, N=256	SHA-256		
		SHA-384		
		SHA-512		
	Key Pair L=3072, N=256	SHA-256		
		SHA-384		
		SHA-512		
	Sig Gen L=1024, N=160	SHA-1		
SHA-224				
SHA-256				
SHA-384				
SHA-512				

	Sig Gen L=2048, N=224	SHA-1	
		SHA-224	
		SHA-256	
		SHA-384	
		SHA-512	
	Sig Gen L=2048, N=256	SHA-1	
		SHA-224	
		SHA-256	
		SHA-384	
		SHA-512	
	Sig Gen L=3072, N=256	SHA-1	
		SHA-224	
		SHA-256	
		SHA-384	
		SHA-512	
Sig Ver	L=1024, N=160	SHA-1	
		SHA-224	
		SHA-256	
		SHA-384	
		SHA-512	
	L=2048, N=224	SHA-1	
		SHA-224	
		SHA-256	
		SHA-384	
		SHA-512	
	L=2048, N=256	SHA-1	
		SHA-224	
		SHA-256	
		SHA-384	
		SHA-512	
	L=3072, N=256	SHA-1	
		SHA-224	
		SHA-256	
		SHA-384	
		SHA-512	

SHA: FIPS 180-2

Support for testing: <http://csrc.nist.gov/groups/STM/cavp/documents/shs/shaval.htm>

	SHA-1 Byte Only Option	
	SHA-224 Byte Only Option	
	SHA-256 Byte Only Option	
	SHA-384 Byte Only Option	
	SHA-512 Byte Only Option	

RNG: FIPS 186, ANSI 9.62, ANSI 9.31			
Support for testing: http://csrc.nist.gov/groups/STM/cavp/documents/rng/rngval.html			
	FIPS 186	RNG Test: General Purpose RNG	
	FIPS 186	RNG Test: Regular 186 RNG	
	FIPS 186	RNG Generator: X - Original	
	FIPS 186	RNG Generator: X – Change Notice	
	FIPS 186	RNG Generator: K - Original	
	FIPS 186	RNG Generator: X – Change Notice	
	FIPS 186	RNG G Function SHA-1	
	FIPS 186	RNG G Function DES	
	FIPS 186	RNG Seed-Key Byte Size min length range 20-64	
	FIPS 186	RNG Seed-Key Byte Size min length range 20-64	
	ANSI 9.62	curve P-192	
		curve P-224	
		curve P-256	
		curve P-384	
		curve P-521	
		curve K-163	
		curve P-233	
		curve P-283	
		curve P-409	
		curve P-571	
		curve B-163	
		curve B-233	
		curve B-283	
		curve B-409	
	curve B-571		
	ANSI 9.62	G function SHA-1	
		G function DES	
	ANSI 9.62	Seed-Key Byte Size Min Length in the range of [20, 64]	
		Seed-Key Byte Size Max Length in the range of [20, 64]	
	ANSI 9.31	2 Key Triple DES	
		3 Key Triple DES	
		AES with Key Size 128	
		AES with Key Size 192	
		AES with Key Size 256	

RSA: FIPS 186-2				
Support for testing: http://csrc.nist.gov/groups/STM/cavp/documents/dss/rsaval.html				
	GenKey9.31	1024		
		1536		
		2048		
		3072		
		4096		
	Public Key Value:	3		
		17		
		65537		
	SigGen9.31 Modulus size	1024		
		1536		
		2048		
		3072		
		4096		
	SigGen9.31 Algorithm	SHA-1		
		SHA 256		
		SHA 384		
		SHA 512		
	SigGenPKCS1.5 Modulus Sizes	1024		
		1536		
		2048		
		3072		
		4096		
	SigGenPKCS1.5 Algorithms	SHA-1		
		SHA-224		
		SHA-256		
		SHA-384		
		SHA-512		
	SigGenPSS Modulus Sizes	1024		
		1536		
		2048		
		3072		
		4096		
SigGenPSS Algorithms	SHA-1			
	SHA-224			
	SHA-256			
	SHA-384			
	SHA-512			
SigVer9.31 Modulus Sizes	1024			
	1536			
	2048			

		3072 4096	
	SigVer9.31 Supported Algorithms	SHA-1 SHA-256 SHA-384 SHA-512	
	SigVerPKCS1.5 Modulus Sizes	1024 1536 2048 3072 4096	
	SigVerPKCS1.5 Supported Algorithms	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	
	SigVerPSS Modulus Sizes	1024 1536 2048 3072 4096	
	SigVerPSS Supported Algorithms	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	

HMAC: FIPS 198		
Support for testing: http://csrc.nist.gov/groups/STM/cavp/documents/mac/hmacval.html		
	SHA-1	
	SHA-224	
	SHA-256	
	SHA-384	
	SHA-512	

CCM: SP 800-38C			
Support for testing: http://csrc.nist.gov/groups/STM/cavp/documents/mac/ccmval.html			
	AES Key size	128	
		192	
		256	
	Associated Data Length Range [0, 32]		
	Payload Length [0, 32]		
	Nonce Length	7	
		8	
		9	
		10	
		11	
		12	
		13	
	Tag Length	4	
		6	
		8	
		10	
		12	
		14	
	16		

ECDSA: FIPS 186-2		
Support for testing: http://csrc.nist.gov/groups/STM/cavp/documents/dss/ecdsaval.html		
	KeyPair	
	PKV	
	SigGen	
	SigVer	

CMAC: SP 800-38B.			
Support for testing:			
	Generate with AES	AES 128	
		AES 192	
		AES 256	
	Verify with AES	AES 128	
		AES 192	
		AES 256	
	Generate with TDES	2-Key TDES	
		3-Key TDES	
	Verify with TDES	2-Key TDES	
		3-Key TDES	

DRBG: SP 800-90			
Support for testing: http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgval.html			
	Hash DRBG	SHA-1	
		SHA-224	
		SHA-256	
		SHA-384	
		SHA-512	
		Prediction Resistance Supported	
		Reseed not implemented	
	HMAC DRBG	SHA-1	
		SHA-224	
		SHA-256	
		SHA-384	
		SHA-512	
		Prediction Resistance Supported	
		Reseed not implemented	
	CTR DRBG	3 key TDEA	
		AES 128	
		AES 192	
		AES 256	
		Derivation function	
		No derivation function	
		Prediction Resistance Supported	
		Reseed not implemented	
	Dual EC DRBG	P256: SHA-1	
		P256: SHA-224	
		P256: SHA-256	
		P256: SHA-384	
		P256: SHA-512	

		P384: SHA-224	
		P384: SHA-256	
		P384: SHA-384	
		P384: SHA-512	
		P521: SHA-256	
		P521: SHA-384	
		P521: SHA-512	
		Prediction Resistance Supported	
		Reseed not implemented	

KAS FFC: SP			
Support for testing: http://csrc.nist.gov/groups/STM/cavp/#06			
	dhHybrid1	initiator	
		responder	
		Key confirmation: provider	
		Key confirmation: recipient	
		Key confirmation: unilateral	
		Key confirmation: bilateral	
	MVQ1	initiator	
		responder	
		Key confirmation: provider	
		Key confirmation: recipient	
		Key confirmation: unilateral	
		Key confirmation: bilateral	
	MVQ2	initiator	
		responder	
		Key confirmation: provider	
		Key confirmation: recipient	
		Key confirmation: unilateral	
		Key confirmation: bilateral	
	dhStatic	initiator	
		responder	
		Key confirmation: provider	
		Key confirmation: recipient	
		Key confirmation: unilateral	
		Key confirmation: bilateral	
	dhEphem	initiator	
		responder	
	dhOneflow	initiator	
		responder	
	dhHybridOneflow	initiator	
		responder	
		Key confirmation: provider	

		Key confirmation: recipient	
		Key confirmation: unilateral	
		Key confirmation: bilateral	

KAS ECC: SP			
Support for testing: http://csrc.nist.gov/groups/STM/cavp/#06			
	Full Unified	initiator	
		responder	
		Key confirmation: provider	
		Key confirmation: recipient	
		Key confirmation: unilateral	
		Key confirmation: bilateral	
	Ephemeral Unified	initiator	
		responder	
	Full MVQ	initiator	
		responder	
		Key confirmation: provider	
		Key confirmation: recipient	
		Key confirmation: unilateral	
		Key confirmation: bilateral	
	One Pass Unified	initiator	
		responder	
		Key confirmation: provider	
		Key confirmation: recipient	
		Key confirmation: unilateral	
		Key confirmation: bilateral	
	One Pass MVQ	initiator	
		responder	
		Key confirmation: provider	
		Key confirmation: recipient	
		Key confirmation: unilateral	
		Key confirmation: bilateral	
		responder	
	One Pass DH	initiator	
		responder	
		Key confirmation	
	Static Unified	initiator	
		responder	
		Key confirmation: provider	
		Key confirmation: recipient	
		Key confirmation: unilateral	
		Key confirmation: bilateral	

CGM: SP 800-38D		
Support for testing: http://csrc.nist.gov/groups/STM/cavp/#07		
	Mode	Encrypt
		Decrypt
	Key size	128
		192
		256
	Tag length	128
		120
		112
		104
		96
		64
		32
		96 bit IV supported
		Other IV

Non FIPS Approved algorithms

atsec can also test the following algorithms, but these are **not** validated or certified by NIST

DES		
Support for testing: http://csrc.nist.gov/groups/STM/cavp/documents/des/desval.html		
	ECB	<input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
	CBC	<input type="checkbox"/> Encrypt, <input type="checkbox"/> Decrypt
	CFB	1 Bit <input type="checkbox"/> Encrypt <input type="checkbox"/> Decrypt
		8 Bits <input type="checkbox"/> Encrypt <input type="checkbox"/> Decrypt
		64 Bits <input type="checkbox"/> Encrypt <input type="checkbox"/> Decrypt
	OFB	<input type="checkbox"/> Encrypt <input type="checkbox"/> Decrypt

MAC		
Support for testing: http://csrc.nist.gov/groups/STM/cavp/documents/des/desval.html		
MAC		Contact atsec for details

FIPS 171 (ANSI X9.17 Key management)		
http://csrc.nist.gov/groups/STM/cavp/documents/des/kmvsval.htm		
FIPS 171		Contact atsec for details

RC4		Contact atsec for details
------------	--	----------------------------------

Blowfish		Contact atsec for details
-----------------	--	----------------------------------