Cryptographic Recommendations Smals

Creation date: 2025-10-28

WARNING: This document is generated in the context of experiments by Smals Research and has no authoritative value.

Symmetric Encryption

Recommended

Name	Type	Classical security	Quantum security	Conditions	Remarks	References
AES-128-GCM	authenticated encryption	128	1	[0, 1, 2, 3, 4]		[0, 1]
AES-192-GCM	authenticated encryption	192	3	[0, 1, 2, 3, 4]		[0, 1]
AES-256-GCM	authenticated encryption	256	5	[0, 1, 2, 3, 4]		[0, 1]
AES-128-GCM-SIV	authenticated encryption	128	1	[1, 5]		[2]
AES-256-GCM-SIV	authenticated encryption	256	5	[1, 5]		[2]

Secure

Name	Type	Classical security	Quantum security	Conditions	Remarks	References
AES-128-CCM	authenticated encryption	128	1	[6, 2, 4]		[0, 3]
AES-192-CCM	authenticated encryption	192	3	[6, 2, 4]		[0, 3]
AES-256-CCM	authenticated encryption	256	5	[6, 2, 4]		[0, 3]

Phase-out

Name	Type	Classical security	Quantum security	Conditions	Remarks	References
AES-128-CBC	symmetric encryption	128	1	[7, 8, 9]		[0, 4]
AES-192-CBC	symmetric encryption	192	3	[7, 8, 9]		[0, 4]
AES-256-CBC	symmetric encryption	256	5	[10, 11, 8, 9]		[0, 4]
AES-128-CTR	symmetric encryption	128	1	[12, 13]		[0, 4]
AES-192-CTR	symmetric encryption	192	3			[0, 4]
AES-256-CTR	symmetric encryption	256	5	[2, 4, 13]		[0, 4]

Insecure

Name	Type	Classical security	Quantum security	Conditions	Remarks	References
AES-128-ECB	symmetric encryption	0	0		[0]	
AES-192-ECB	symmetric encryption	0	0		[0]	
AES-256-ECB	symmetric encryption	0	0		[0]	

DES	blockcipher	0	0		[1]	
Blowfish	blockcipher	0	0		[2]	
TDAE	blockcipher	0	0		[3, 4]	

Padding schemes

Recommended

Name	Type	Conditions	Remarks	References
ISO-Padding	padding		[5]	[5, 6]
ESP-Padding	padding		[5]	[7]
RFC 5652	padding		[5]	[8]

Secure

Phase-out

Insecure

Conditions

[0] For initialization vectors, a bit length of 96 bits is recommended.

[1] A key change is required after at most 2^32 calls of the authenticated encryption function.

[2] Initialization vectors must not repeat within the lifetime of a key.

[3] Tags of at least 96 bits should be used.

[4] When encrypting a t block message, with IV = j, we never take a new nonce in the range [j , j+t-1].

[5] AES-GCM-SIV is defined for AES-128 and AES-256, so a key length of 192 bits should not be

used

[6] A tag length of > 96 bits is recommended.

[7] Only unpredictable initialization vectors are to be used. A single key should not be used to encrypt more than 2^64 blocks (key exhaustion).

[8] CBC mode only offers confidentiality, making it susceptible to malleability attacks. Use of CBC mode SHOULD be accompanied by a data authentication mechanism.

[9] Formatting by filling the last block to the required block size is also called padding. Only the CBC mode requires a padding step.

[10] Only unpredictable initialization vectors are to be used.

[11] A single key should not be used to encrypt more than 2^64 blocks (key exhaustion).

[12] Initialization vectors must not repeat within the lifetime of a key. When encrypting a t block message, with IV = j, we never take a new nonce in the range [j , j+t-1].

[13] CTR mode only offers confidentiality, making it susceptible to malleability attacks. Use of CTR mode SHOULD be accompanied by a data authentication mechanism.

Remarks

[0] Replicating the same plaintext block results in identical ciphertext blocks. That exposes a pattern in the encrypted data; hence, the application of ECB mode is only suitable when dealing with single-value encryption, for example, the transmission of a key.

[1] Its key length of 56 bits makes it insecure

[2] Its 64 block length makes it susceptible to birthday attacks

[3] Triple Data Encryption Algorithm, also known as Triple DES

[4] Insecure because of 1) Small block length of only 64 bits, 2) Reduced security against generic attacks on block ciphers, and 3) Various other undesirable properties

[5] In CBC mode of operation, care must be taken to ensure that an attacker cannot learn from error messages or other side-channels whether the padding of an introduced data packet was correct.

References

[0] FIPS PUB 197 (2001)

[1] NIST SP 800-38D (2007)

[2] RFC 8452 (2019)

[3] NIST SP 800-38C (2004)

[4] NIST SP 800-38A (2001)

[5] ISO/IEC 9797-1:2011, method 2

[6] NIST SP 800-38A, appendix A

[7] RFC 4303, section 2.4

[8] RFC 5652, section 6.3