

MeshCore Encryption Overview

This page summarizes MeshCore's encryption as verified from the official source code. The key facts: AES-128 symmetric encryption, ECDH key exchange using Ed25519 keys transposed to X25519, and a 2-byte truncated MAC (derived from HMAC-SHA256) for message authentication.

Verified Encryption Summary

Component	Algorithm	Notes
Symmetric cipher	AES-128 ECB	16-byte key (CIPHER_KEY_SIZE=16); zero-padding on final block
Message authentication	2-byte truncated MAC (from HMAC-SHA256)	CIPHER_MAC_SIZE=2; encrypt-then-MAC, MAC prepended before the ciphertext
Key exchange	ECDH via X25519	Ed25519 keys converted to X25519 for DH; AES-128 uses 16 bytes of the 32-byte shared secret, the MAC is keyed with the full 32
Identity keys	Ed25519	32-byte public key, 64-byte private key
Advertisement signing	Ed25519 signature	Prevents node identity spoofing

Security Caveats

- **ECB mode leaks structure:** ECB encrypts each 16-byte block independently, so identical plaintext blocks produce identical ciphertext blocks. A passive listener can detect repeated content, message patterns, and known headers without the key. Do not assume ECB hides patterns in templated or repetitive traffic. (MeshCore embeds a timestamp in each message to partially mitigate this.)
- **The 2-byte (16-bit) MAC is weak:** A truncated 16-bit MAC is an integrity check, not strong authentication. An active attacker can forge it by brute force in roughly 32,000 attempts. Channel "authentication" is also group-level only: any holder of the channel key

can forge messages as any sender.

- **No forward secrecy:** Identity keys are static, so a single leaked private key decrypts all past and future recorded traffic for that node. There is no key revocation.
- **The public/default channel key is publicly documented** (`8b3387e9c5cdea6ac9e5edbaa115cd72`). Traffic on the public channel is readable by anyone; it is not private or secure against observers.

Common Misconceptions

- **Not AES-256:** MeshCore uses AES-128, not AES-256. Key length (128-bit) is adequate; the real cryptographic limitations of MeshCore are the ECB cipher mode and the 2-byte (16-bit) truncated MAC described in the Security Caveats above — not the key size.
- **Not CTR mode:** The implementation uses ECB mode with zero-padding, not CTR or GCM mode.
- **The official MeshCore website** states "AES-128 encryption" - this matches the source code.

Source: Official MeshCore repository source code. Verified 2026-05-03.

Revision #4

Created 2026-05-03 06:20:53 UTC by Mesh America Admin

Updated 2026-06-09 14:17:19 UTC by Mesh America Admin