Task Group 5

Progress on Recommendations Concerning the Data Protection Plan

Preliminary Recommendations

ACCRES

Recommendation

- Where a requirement for symmetric encryption exists the working group recommends CRS operators employ the Advanced Encryption Standard (AES) per NIST FIPS-197 unless a compelling rationale exists for employment of an alternative cipher.

Rationale

- The AES cipher is a heavily researched asymmetric cipher that is resistant to quantum threats
- A significant body of knowledge is available to users through NIST publications

Preliminary Recommendations

ACCRES

Recommendation

- When employing cryptographic techniques CRS operators should select algorithms which have a security strength of 256 bits or greater unless a compelling rationale otherwise exists.
  - Applies to symmetric (stream/block) ciphers and asymmetric (rekey) ciphers

Rationale

- Grover's algorithm may reduce the search space necessary to brute force AES from $O(N)$to $O(\sqrt{N})$
  - FROM 256 bits TO 128 bits
  - FROM 128 bits TO 64 bits (attack is now feasible)

Comparable Security Strengths

Shamelessly taken from a NIST slide deck…

Security Strength (Bits)	Symmetric Key Algorithms	FFC (DSA, D-H, MQV)	IFC (RSA)	ECC (ECDSA, ECDH, ECMQV)	Digital Signature, Hash Only	HMAC, Key Der., RNG[1]
128	AES-128	7,680	7,680	384 - 511	SHA-256	SHA-1
256	AES-256	15,360	15,360	512+	SHA-512	SHA-256

FFC = Finite Field Cryptography
IFC = Integer Factorization Cryptography
ECC = Elliptic Curve Cryptography

1. The security strength assumes that the random number generator has been provided with adequate entropy to support the desired security strength.

Preliminary Recommendations

ACCRES

Recommendation

- Where encryption is unnecessary provisions should be made for unencrypted communications.

Rationale

- In some cases encryption of command or data links is unnecessary, unauthorized or places an undue burden on available resources.
- Examples where encryption is unnecessary may include but are not limited to:
  - Cases where radio frequency bands are used wherein use of encryption is prohibited by a regulatory entity, for example by university or amateur radio programs using amateur radio bands
  - Cases where secrecy is deemed unnecessary, for example transmission of telemetry or mission data that is deemed non-sensitive

Preliminary Recommendations

Recommendation

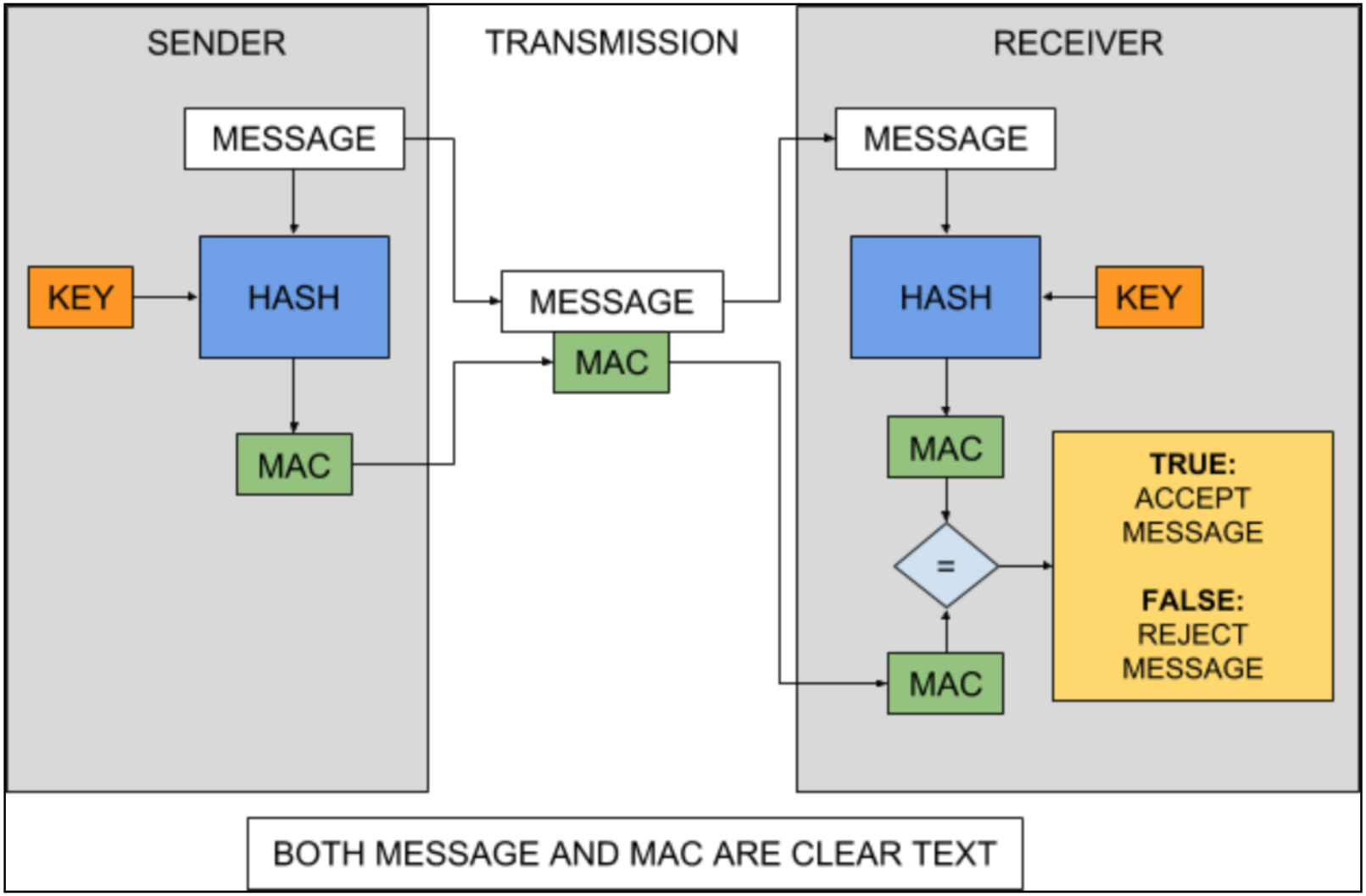
- Where provisions are made for unencrypted communications messages should be properly authenticated, or otherwise ignored, by the receiving system using encrypted authentication techniques.
  - Examples of encrypted authentication include:
    - Employment of a Keyed-Hash Message Authentication Code (HMAC) to produce a Message Authentication Code (MAC) (See: NIST FIPS PUB 198-1)
    - Employment of Additional Authenticated Data (AAD) when using the Galois Counter Module (GCM) mode of operation with the AES cipher (See: NIST Special Publication 800-38D)

Rationale

- Encrypted authentication, for example the use of a MAC to ensure data integrity and authenticity, provides a cryptographically secure means of unencrypted communications where secrecy is unnecessary but positive control and/or authenticity are required.

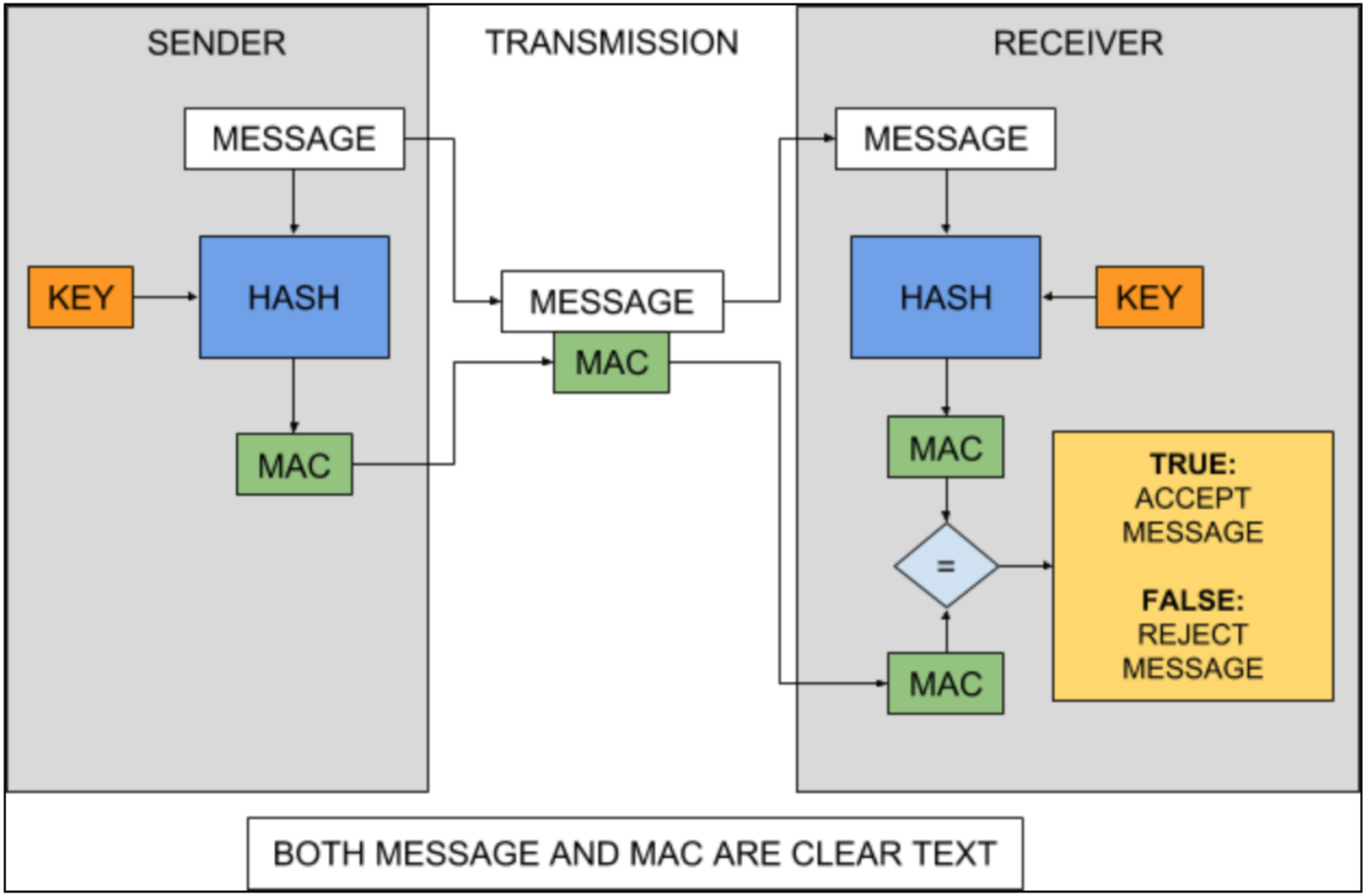
Example of Encrypted Authentication

ACCRES



Practical Authentication with GMAC

ACCRES



Preliminary Recommendations

ACCRES

Recommendation

- CRS operators should re-key systems with sufficient frequency to maintain cryptographic security

Rationale

- For many ciphers practical limits exist for throughput using a single key before security is degraded

Preliminary Recommendations

ACCRES

Recommendation

- CRS operators should pay particular attention to cipher mode of operation, implementation and key management.

Rationale

- Practical attacks will likely exploit weaknesses in implementation or key management rather than mathematical weaknesses in the underlying cipher