Security Operations for CC℠

Data Security

Kevin Henry

CISM CISSP CCSP

kevin@kmhenrymanagement.com

CC℠ Certification Examination

Domains	Weights
1. Security Principles	26%
2. Business Continuity (BC), Disaster Recovery (DR), & Incident Response	10%
3. Access Control Concepts	22%
4. Network Security	24%
5. Security Operations	18%

Security Operations for CC℠ Certification

Agenda:

Data Security

Security Operations and Administration

Security Awareness Training

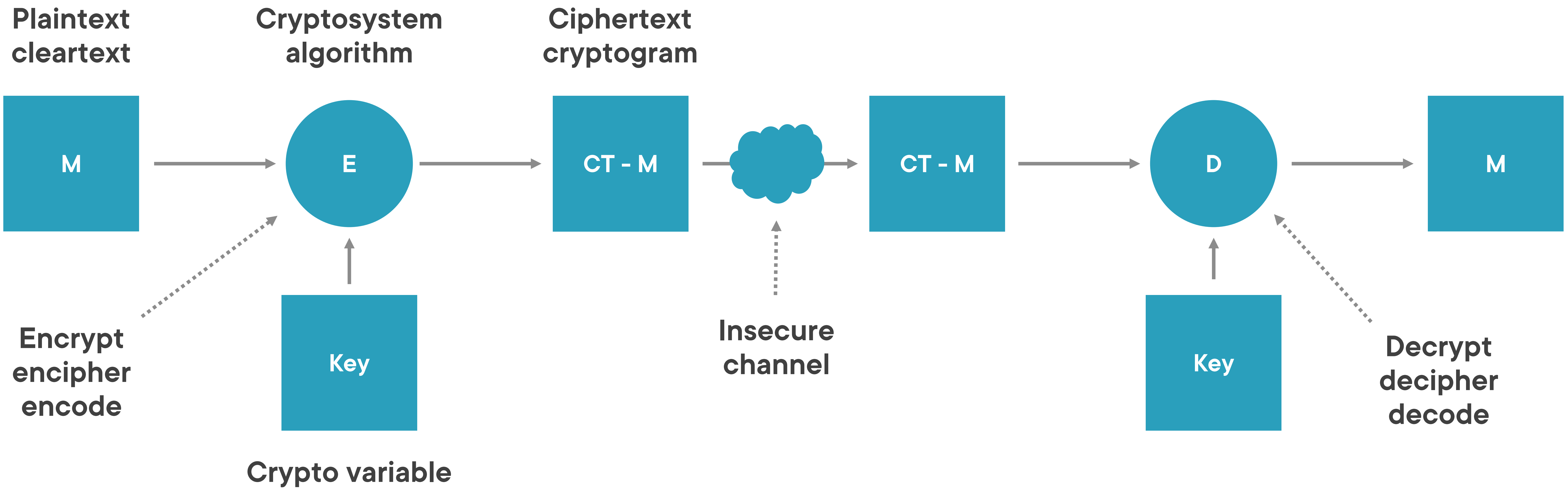
Exam review Tips and Techniques

Data Protection

Data protection requires:

- Ownership
- Classification
- Labels
- Retention policy
- Secure destruction

Cryptography Terminology



Symmetric Algorithms

=

An algorithm that uses the same key in both the encryption and decryption process

Characteristics:

- **Good for confidentiality**
- **Relatively fast**
- **Good for encrypting streaming content**

Examples of Symmetric Algorithms

DES – 3DES – withdrawn

AES

Rijndael

MARS, SERPENT,
RC 4,5,6, Blowfish

Asymmetric Algorithms

Based on use of a key pair

Private key
Must be kept secret

Public key
Computed from the private key
One-way function
Can be shared freely

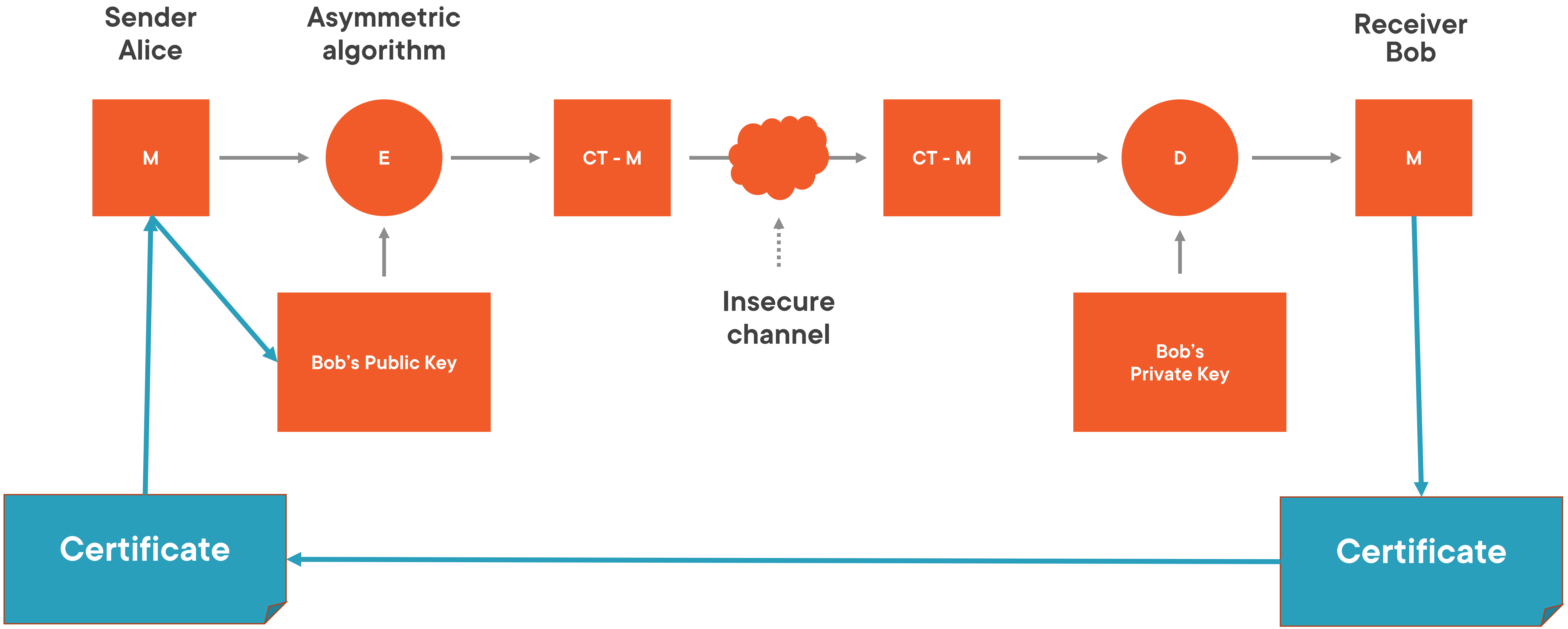
Examples of Asymmetric Algorithms

Diffie-Hellman

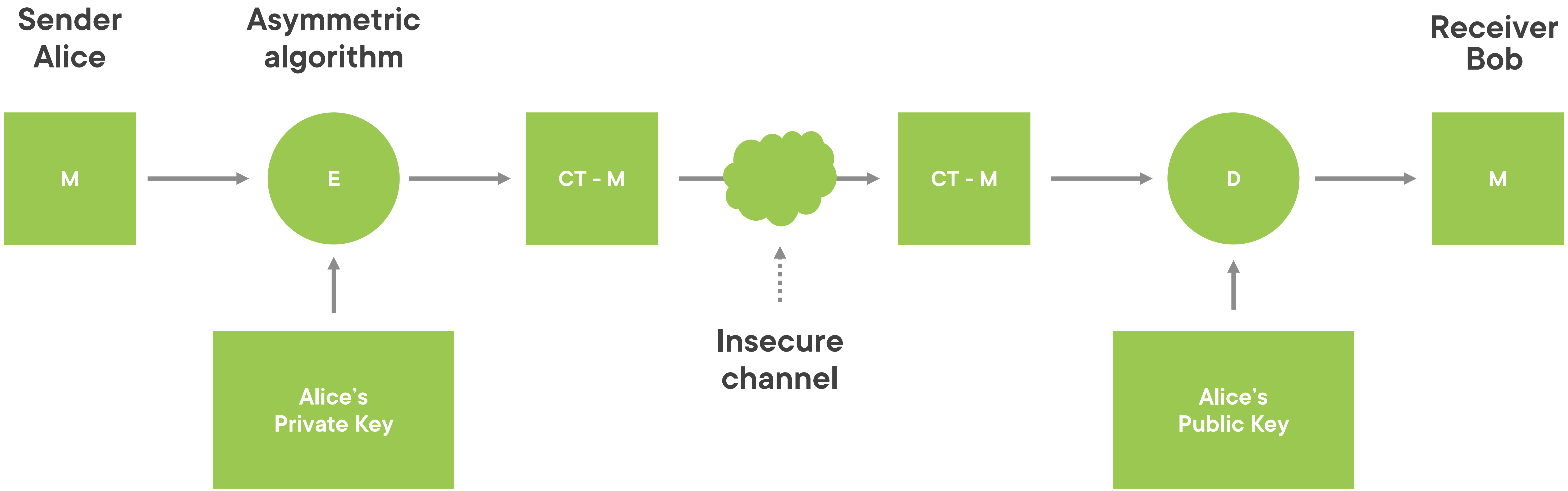
Rivest Shamir Adelman (RSA)

Elliptic Curve Cryptography

Confidentiality Using Asymmetric



Proof of Origin Using Asymmetric



Message Integrity

Message Authentication Codes (MAC)

Used to verify integrity of a message

Storage

Transmission

Examples of MAC

Parity bits

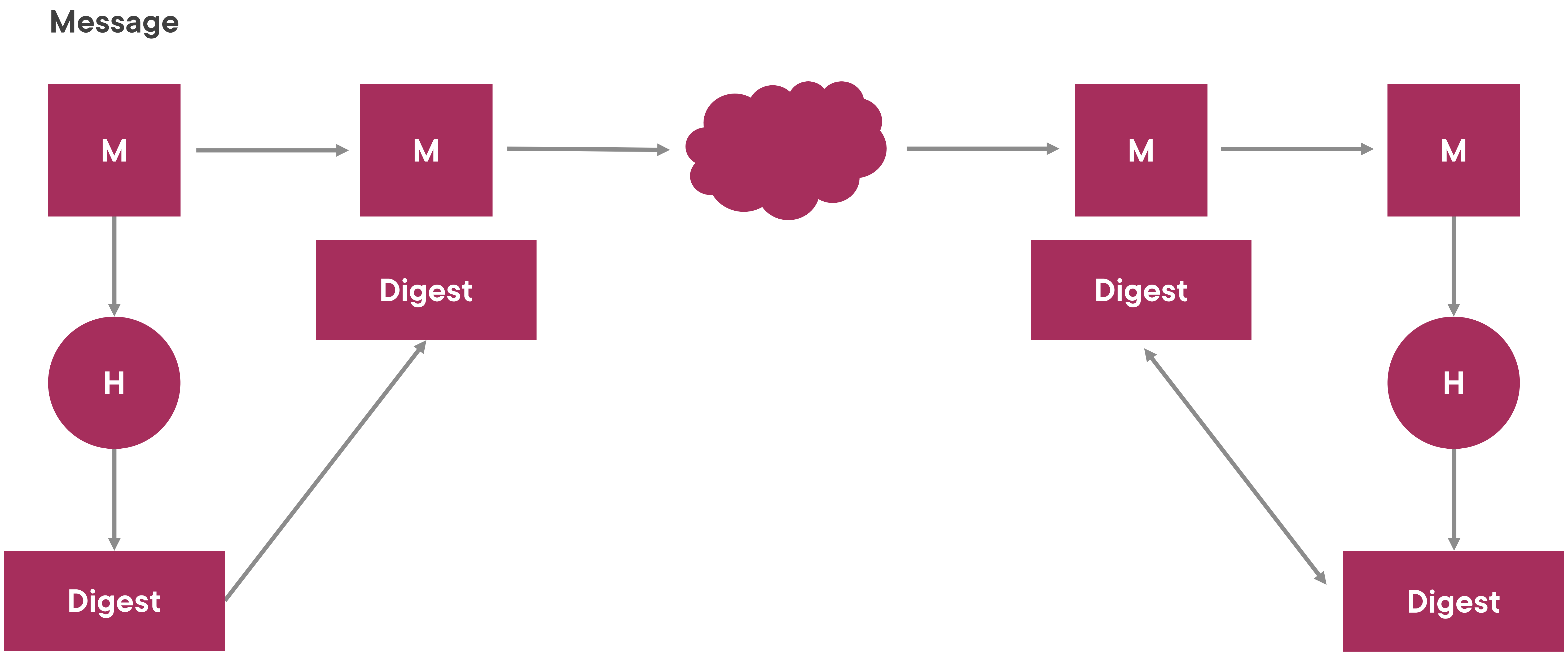
Checksums

Cyclic Redundancy Checks (CRC)

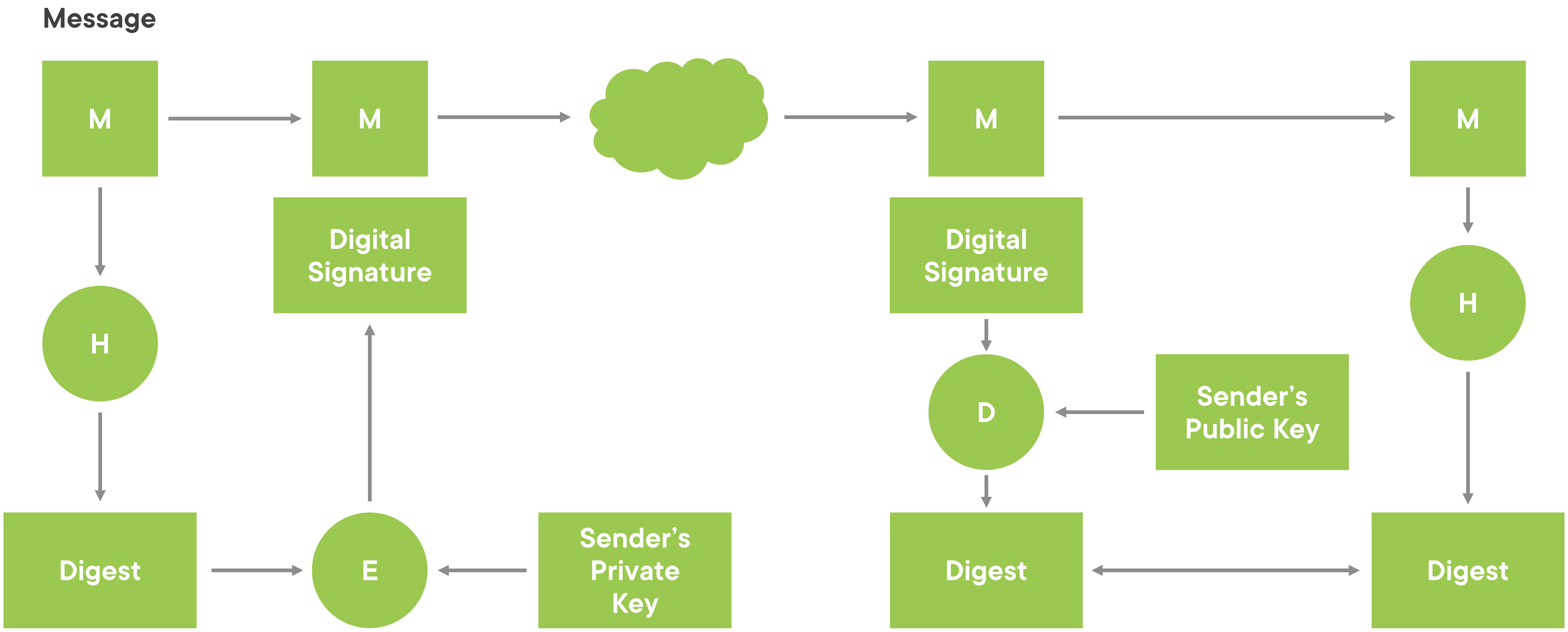
Hash Functions

- **MD5, SHA-1, SHA-2, SHA-3, RIPEMD-160**
- **HMAC**
- **Digital Signatures**

Simple Hash Function Operations



Digital Signatures



Key Points Review

Hashing is primarily used to ensure the integrity of data

- It is a one-way function - computationally infeasible to be reversed
- Very accurate to even the smallest changes to the original message

Security Monitoring

Continuous Monitoring

Automated

Tools

SIEM

Traditional Monitoring

Log analysis

Challenges:
Time
Tools
Skills
Volume

Threat Intelligence

Commercial feeds

Open Source Intelligence (OSINT) feeds

Blogs

Key Points Review

Controls can fail – fail to be effective – not be suitable for new threats

Therefore, monitoring is necessary to ensure that risk is identified and managed adequately