CS 465

MAC: Message Authentication Code

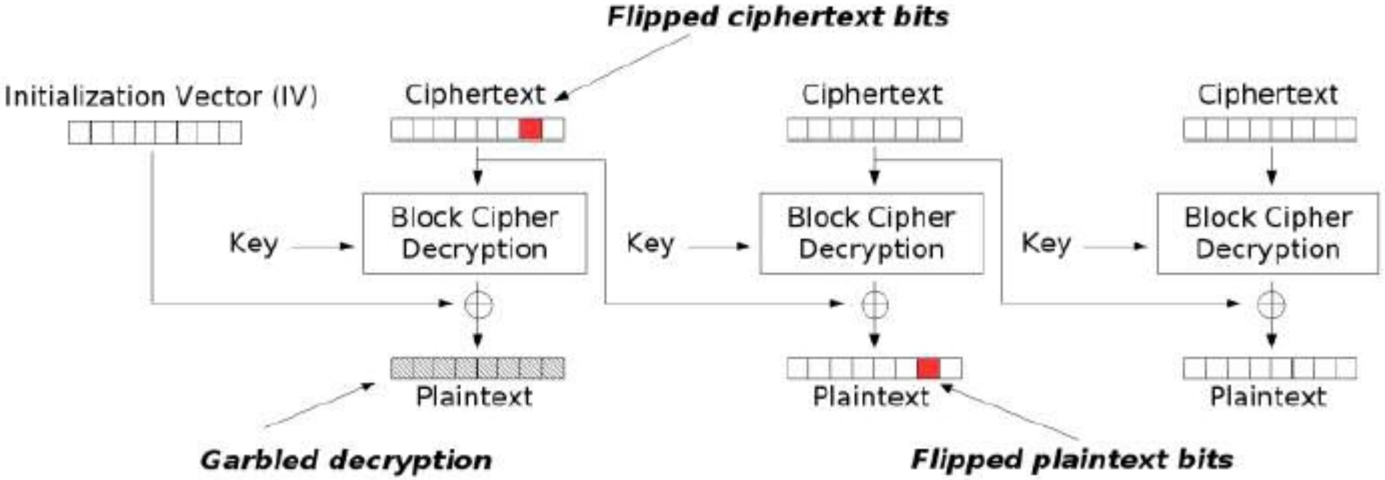
Last Updated: Aug 20, 2012

What Assurrances are Provided by Symmetric Encryption?

- Authentication?
- Confidentiality?
- Integrity?
- Non-repudiation?

Bit Flipping Attacks (Block Cipher)

Modification attacks on CBC



Modification attack on CBC

Bit Flipping Attacks (Stream Cipher)

- Plaintext: ACCT_NO:123-45-6789 ADD:100
- Ciphertext: 15b1206b7efa68b9 89 c87357507e3a27a138ca dc b2a1bb f8 eebee5

Goals of Message Authentication

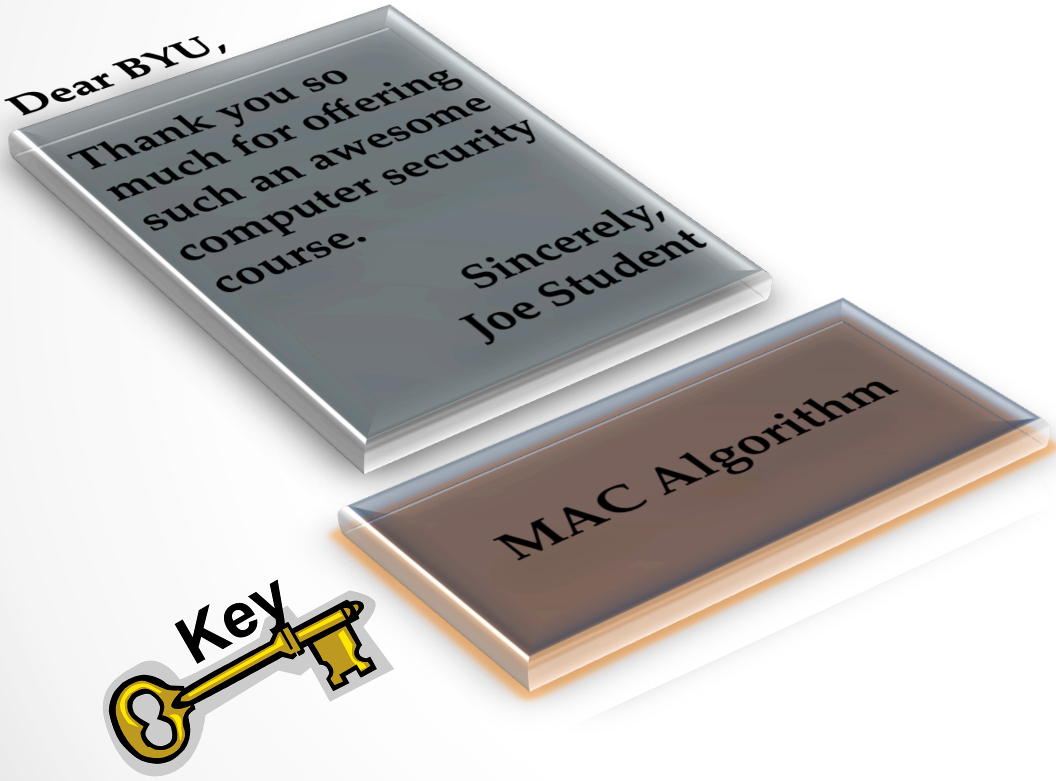
- Assure that the message has not been altered
- Assure the source of the message is authentic
- Optional – Timeliness of the message

Message Authentication: Ciphertext vs. Plaintext

- Authentication of encrypted messages
  - Include an error-detection code in plaintext message

- Authentication of plaintext messages
  - Authentication without confidentiality
  - Attach a key-based error-detection code to plaintext message

Message Authentication Code (MAC)



Dear BYU,

Thank you so
much for offering
such an awesome
computer security
course.

Sincerely,
Joe Student

Message Authentication Code (MAC)

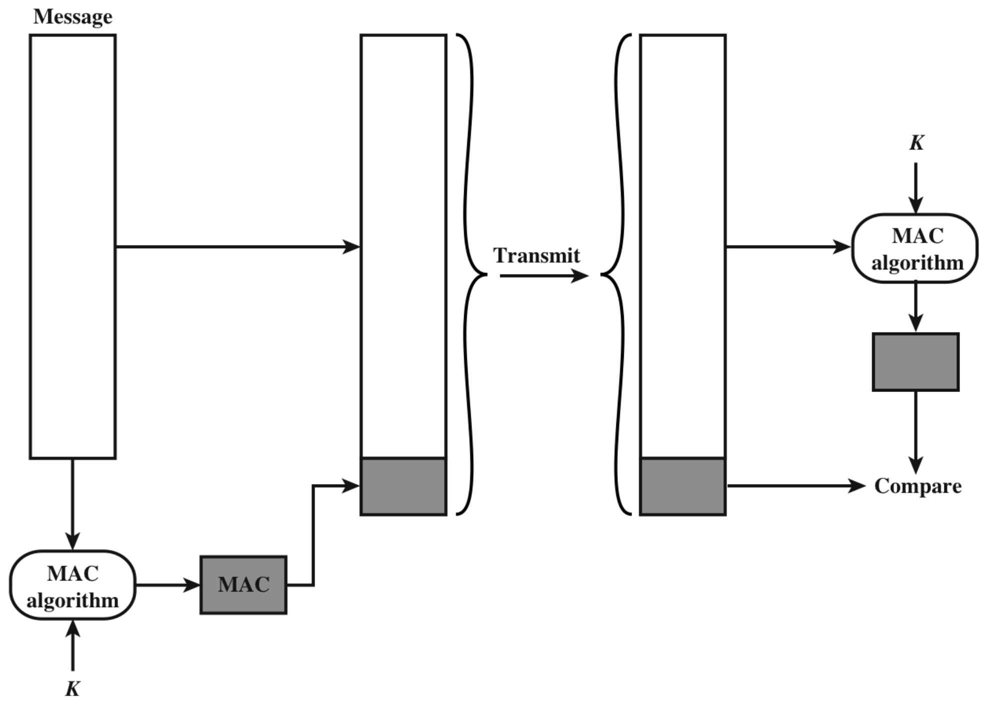
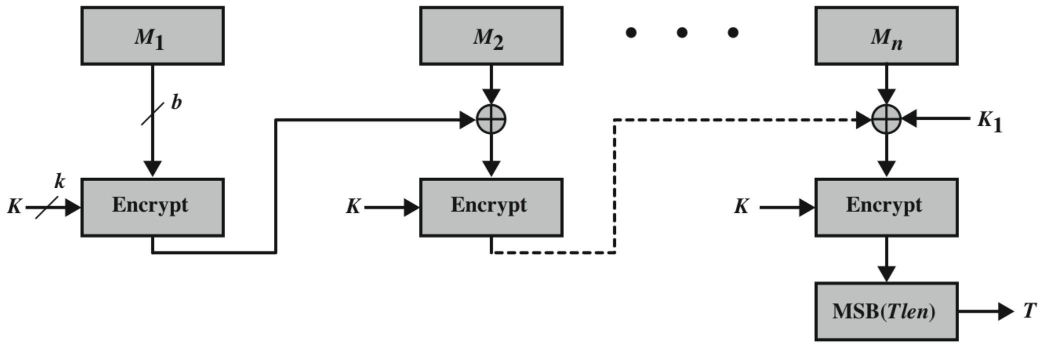


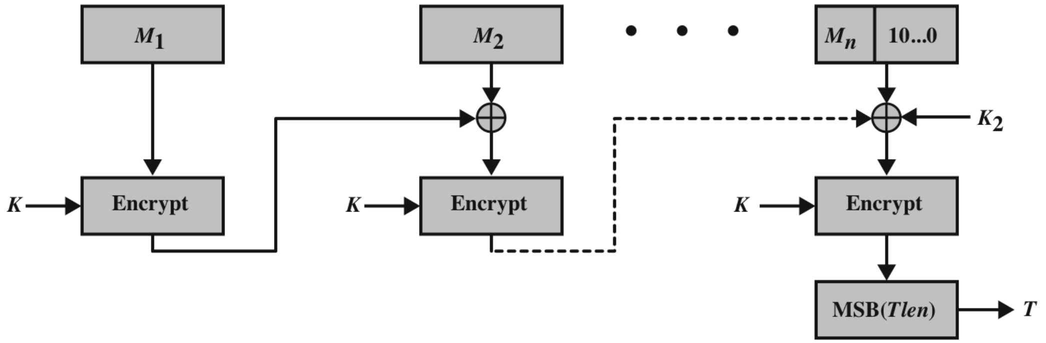
Figure 3.1 Message Authentication Using a Message Authentication Code (MAC)

Source: Network Security Essentials (Stallings)

MAC Creation with Block Cipher



(a) Message length is integer multiple of block size

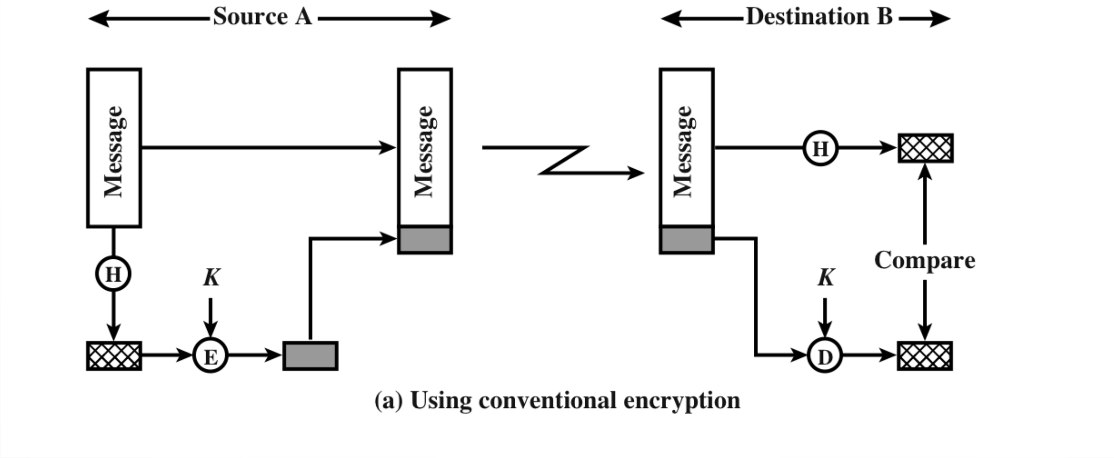


(b) Message length is not integer multiple of block size

Figure 12.12 Cipher-Based Message Authentication Code (CMAC)

Three Ways to Implement a MAC

1. CBC-MAC
   - Use CBC mode and a block cipher
   - Expensive
2. Hash the message and encrypt the digest

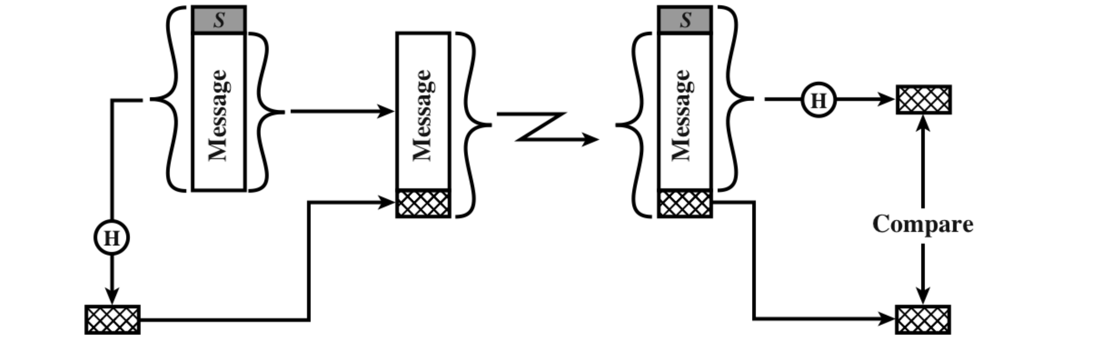


(a) Using conventional encryption

Source: Network Security Essentials (Stallings)

Three Ways to Implement a MAC

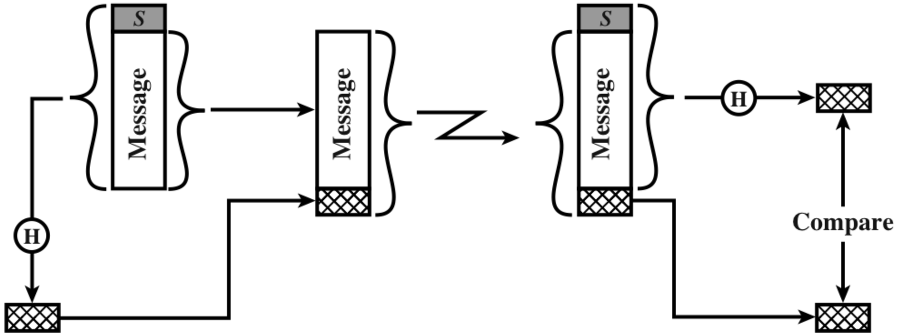
1. CBC-MAC
2. Hash the message and encrypt the digest
3. Hash the message along with a shared key
   - MAC generated using hashing is known as an HMAC



(c) Using secret value

Source: Network Security Essentials (Stallings)

Design Flaw!



(c) Using secret value

- Cryptographers recommend against this kind of HMAC using modern hash functions
- Vulnerable to a message extension attack
- An example of an implementation weaknesses in the algorithm

Iterative Hash Function

- Popular hash functions (MD5, SHA-1) use an iterative implementation technique known as the Merkle-Damgård construction

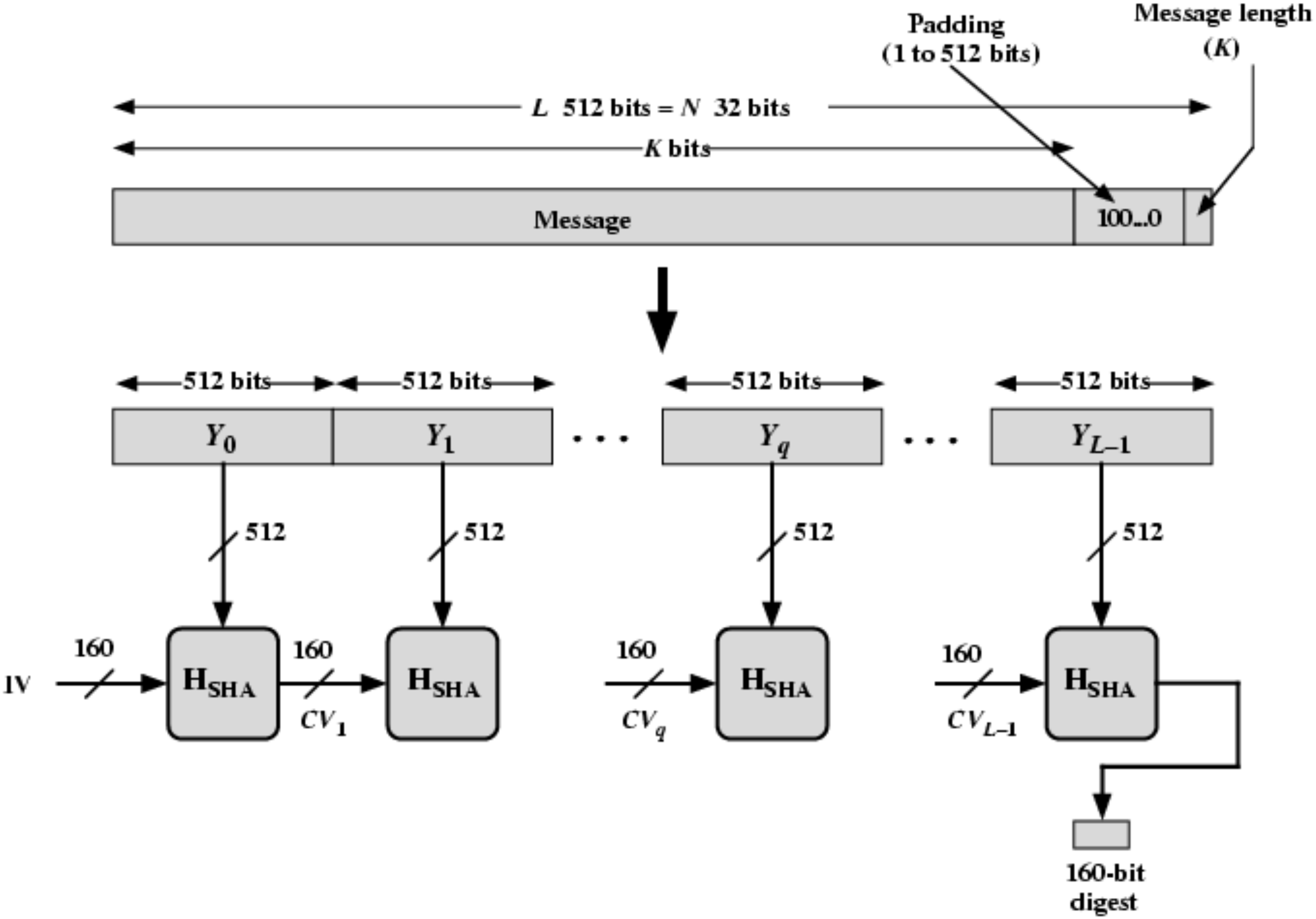


Figure 3.4 Message Digest Generation Using SHA-1

Alice and Bob

- Alice and Bob share a key K
- Alice sends message M_1 to Bob such that Bob knows it came from Alice
  - Alice computes $H(K \mid\mid M_1) = d_1$
  - Alice send M_1 , d_1 Bob
- Bob verifies the message
  - Bob computes $H(K \mid\mid M_1) = d_2$ and compares d_1 to d_2. If they match, the message came from Alice.
  - Or did it????

HMAC

- Because of the message extension attack vulnerability, the government standard HMAC algorithm guards against this threat
    - FIPS 198
    - RFC 2104

HMAC

- H(K || H(K || M))

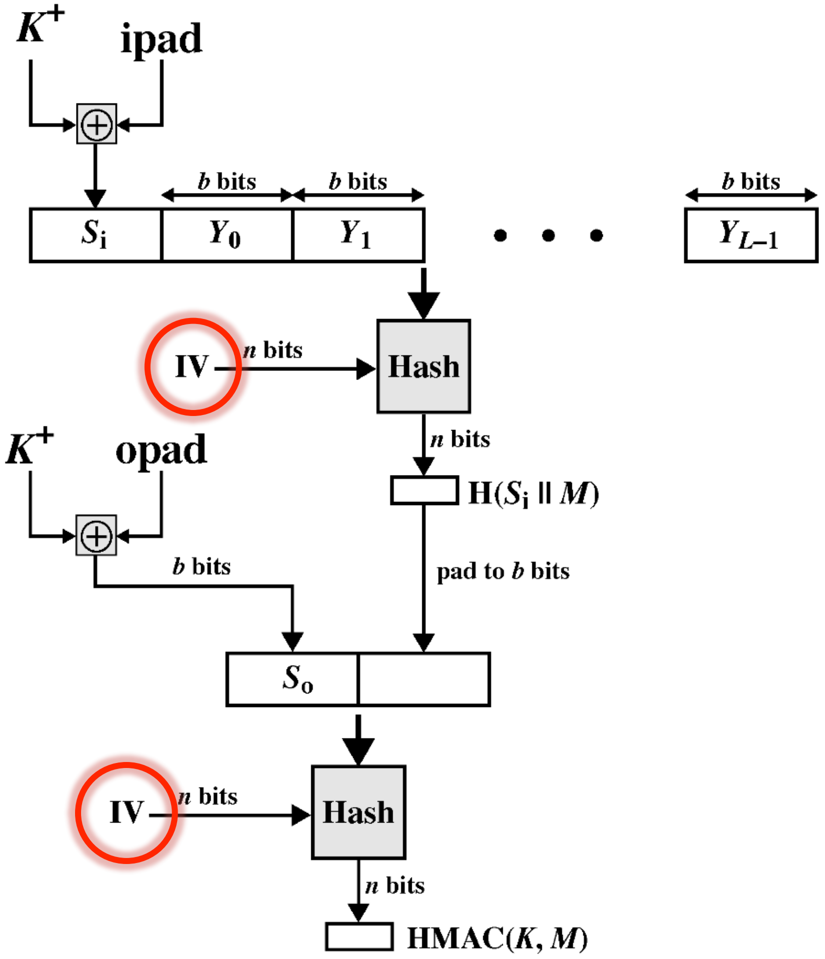


Figure 3.6 HMAC Structure