Lecture 8

KEYED HASHING AND HMAC

R. Rhouma

UTAS
Sultanate of Oman

September 2022

CSSY2201 : Introduction to Cryptography

Plan

1. Problems and countermeasure of security problems
2. Message authentication techniques
    - MAC
    - HMAC
    - CMAC
    - Authenticated Encryption
3. Pseduo-Random number generators

جامعة التقنية
والعلوم التطبيقية
University of Technology
and Applied Sciences
Salalah صلالة

Different types of attacks/problems in a network

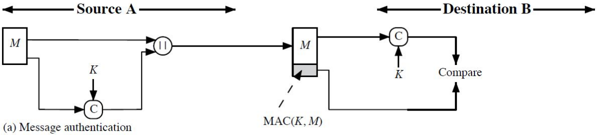
- Disclosure of messages $\Longrightarrow$ Sol : encryption
- Traffic analysis $\Longrightarrow$ Sol : encryption
- Masquerade : message insertion from fraudulent source $\Longrightarrow$ Sol : Message authentication
- content modification : insertion, deletion, transposition and modification $\Longrightarrow$ Sol : Message authentication
- modification in time : message delay or replay $\Longrightarrow$ Sol : Message authentication
- Repudiation of source : Denial of transmission of message by source $\Longrightarrow$ Sol : Digital signature
- Destination repudiation : Denial of receipt of message by recipient $\Longrightarrow$ Sol : Digital signature

Message authentication techniques

1. Hash functions : a function that accepts n variable-length messages as input and outputs a fixed-length digest. The digest is the authenticator of the message (already seen)
2. The encryption of the message : the ciphertext of the message constitutes its authenticator : Authenticated encryption
3. The MAC (Message authentication code) : a function of the message and a secret key that produce a fixed length output MAC which constitutes the authenticator of the message
4. HMAC
5. CMAC

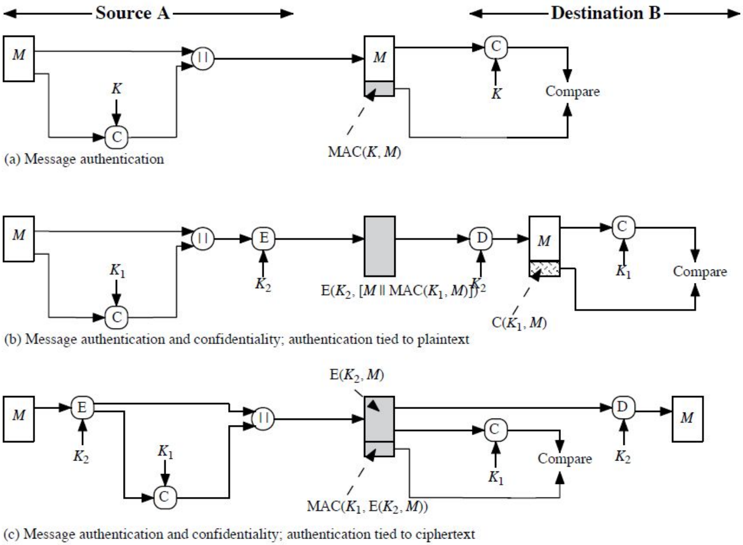
MAC

- Also known as keyed hash function
- used when two entities sharing the same key to authenticate the information exchanged between them
- Takes as input a secret key K and a block of data M and produces a MAC=C(K,M)
- the MAC is associated with the message when it is sent
- If the integrity of the message needs to be checked, the MAC function is applied to the message and the result is compared to the associated MAC (received)
- a hacker who wants to modify the message will be unable to modify the MAC without knowing the secret key.
- MAC is not a digital signature

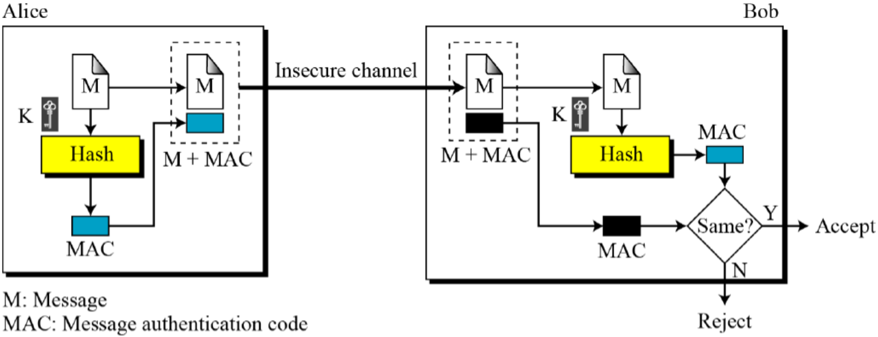


(a) Message authentication

basic use of MAC

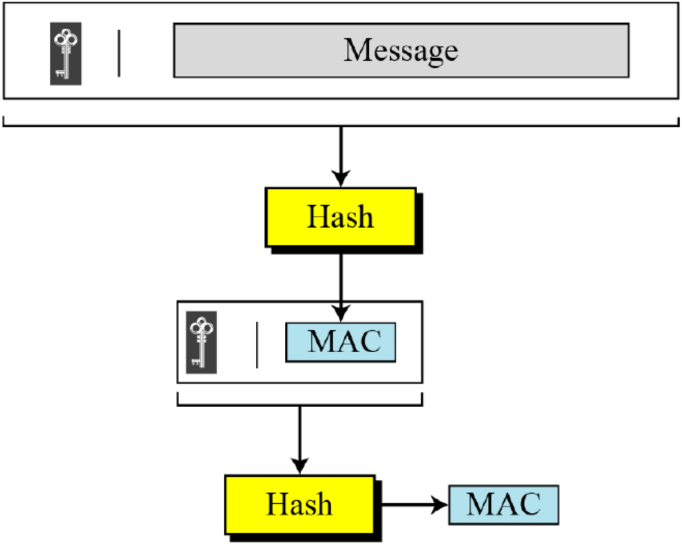

Source A
Destination B
M
K
C
||
M
C
K
Compare
MAC(K, M)
(a) Message authentication
M
K_1
C
||
E
K_2
$E(K_2, [M \| MAC(K_1, M)])$
D
K_2
M
C
K_1
Compare
$C(K_1, M)$
(b) Message authentication and confidentiality; authentication tied to plaintext
M
E
K_2
K_1
C
||
$E(K_2, M)$
D
M
K_2
C
K_1
Compare
$MAC(K_1, E(K_2, M))$
(c) Message authentication and confidentiality; authentication tied to ciphertext

Keyed hash= MAC



M: Message
MAC: Message authentication code
K: A shared secret key

Nested MAC



HMAC

- keyed-hash message authentication codeÂ
- use, without modifications, hash functions
- allow for easy replacement of embedded hash function
- preserve original performance of hash function without significant degradation
- use and handle keys in a simple way.
- have well understood cryptographic analysis of authentication mechanism strength

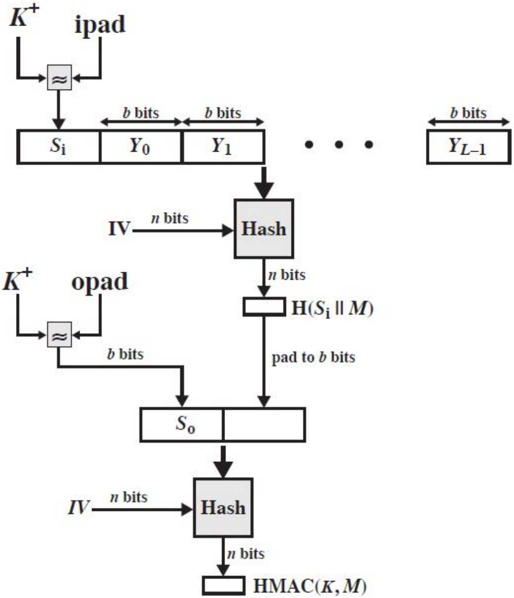
HMAC

- specified as Internet standard RFC2104
- uses hash function on the message :

$$HMACK(M) = Hash[(K^{+} \oplus opad)||Hash[(K^{+} \oplus ipad)||M)]]$$

  - where K+ is the key padded out to block size
  - opad, ipad are specified padding constants
- any hash function can be used eg. MD5, SHA-1, SHA-2, RIPEMD-160, Whirlpool

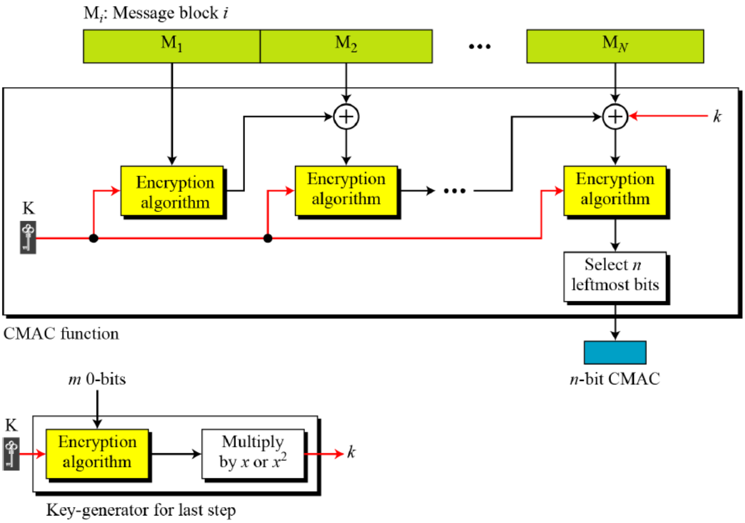
HMAC


K^+
ipad
≈
b bits
b bits
b bits
S_i
Y_0
Y_1
• • •
Y_{L-1}
IV
n bits
Hash
n bits
K^+
opad
≈
$H(S_i \| M)$
b bits
pad to b bits
S_o
IV
n bits
Hash
n bits
HMAC(K, M)

HMAC Security

- proved security of HMAC relates to that of the underlying hash algorithm
- attacking HMAC requires either :
  - brute force attack on key used
  - birthday attack (but since keyed would need to observe a very large number of messages)
- choose hash function used based on speed verses security constraints

CMAC


M_i: Message block i
M_1
M_2
•••
M_N
k
K
Encryption algorithm
Encryption algorithm
•••
Encryption algorithm
Select n leftmost bits
CMAC function
n-bit CMAC
m 0-bits
K
Encryption algorithm
Multiply by x or x^2
k
Key-generator for last step

Authenticated encryption

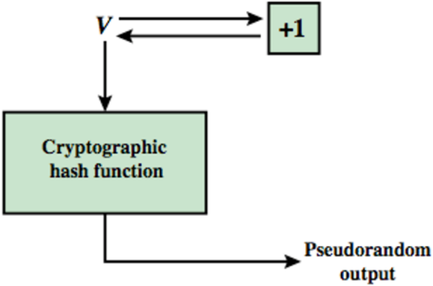
- Protect privacy and provide authentication at the same time
- Different approaches :
  - Hash-then-encrypt : $E(K, (M||H(M))$
  - MAC-then-encrypt : $E(K2, (M||MAC(K1, M))$
  - Encrypt-then-MAC : $C = E(K2, M), T = MAC(K1, C)$
  - Encrypt-and-MAC : $C = E(K2, M), T = MAC(K1, M)$
- decryption and verification is easy

PRNG

- essential elements of PRNG are
  - seed value
  - deterministic algorithm
- seed must be known only as needed
- can base PRNG on
  - encryption algorithm,
  - hash function or
  - MAC (NIST SP 800-90)

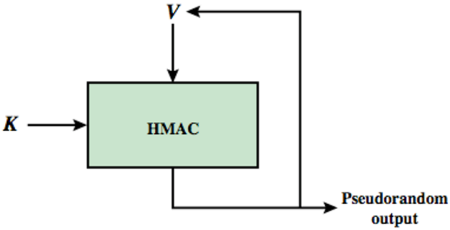
PRNG from Hash function

- hash PRNG from SP800-90 and ISO18031
  - take seed V
  - repeatedly add 1
  - hash V
  - use n-bits of hash as random value
- secure if good hash used



PRNG using a MAC

- MAC PRNGs in SP800-90, IEEE 802.11i, TLS
  - use key
  - input based on last hash in various ways


V
K
HMAC
Pseudorandom output