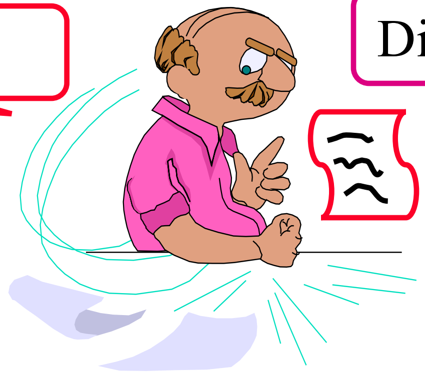
Message Authentication Codes

Was this message altered?



Did he really send this?

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-17/

1. Message Authentication
2. MACS based on Hash Functions: HMAC
3. MACs based on Block Ciphers: DAA and CMAC
4. Authenticated Encryption: CCM and GCM
5. Pseudorandom Number Generation Using Hash Functions and MACs

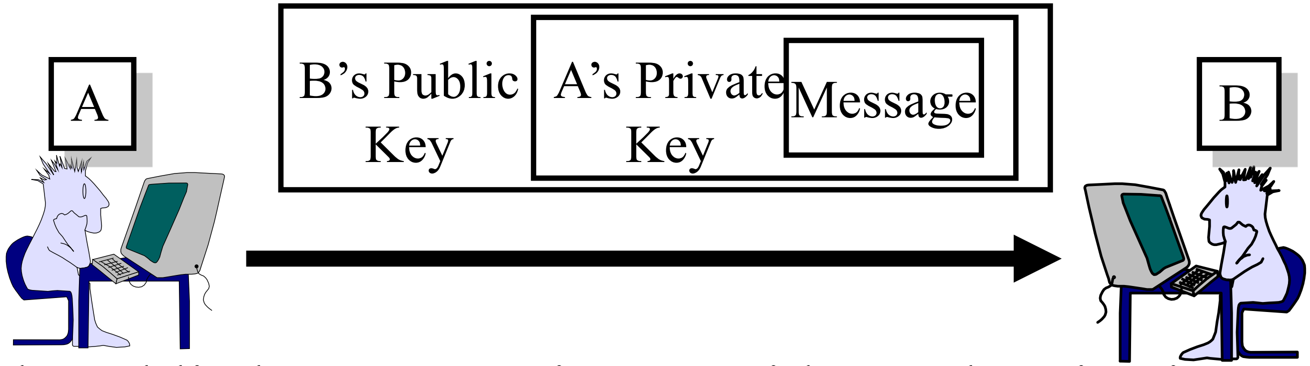
These slides are based partly on Lawrie Brown's slides supplied with William Stallings's book "Cryptography and Network Security: Principles and Practice," 7[h] Ed, 2017.

Message Security Requirements

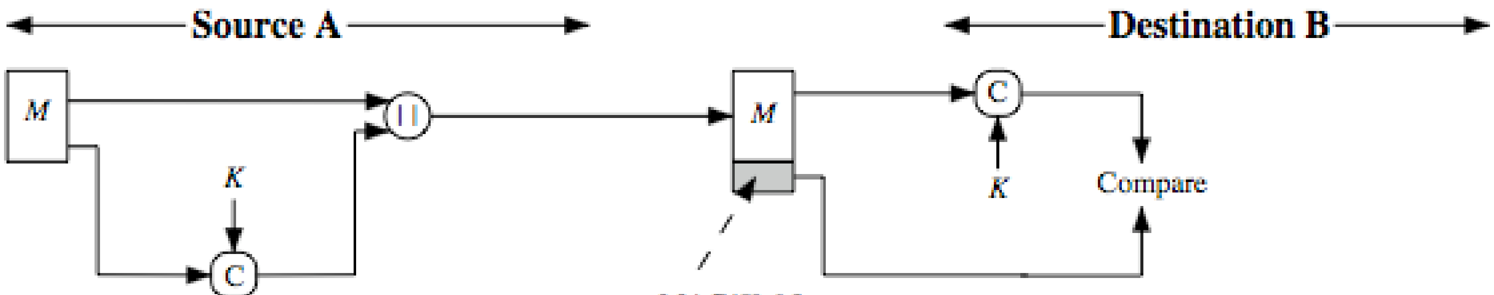
- Disclosure
- Traffic analysis
- Masquerade
- Content modification
- Sequence modification
- Timing modification
- Source repudiation
- Destination repudiation

Message Authentication = Integrity + Source Authentication

Public-Key Authentication and Secrecy



- Double public key encryption provides authentication and integrity. Double public key ⇒ Very compute intensive
- Crypto checksum (MAC) is better.
  Based on a secret key and the message.
  Can also encrypt with the same or different key.



(a) Message authentication

MAC Properties

- A MAC is a cryptographic checksum

  $MAC = C_K(M)$

  - Condenses a variable-length message M using a secret key
  - To a fixed-sized authenticator
- Is a many-to-one function
  - Potentially many messages have same MAC
  - But finding these needs to be very difficult
- Properties:
  1. It is infeasible to find another message with same MAC
  2. MACs should be uniformly distributed
  3. MAC should depend equally on all bits of the message
- Public key MACs provide non-repudiation.
  Secret key MACs do not.

Security of MACs

- **Brute-force** attacks exploiting
  - Strong collision resistant hash have cost min(2^k, 2^n), k=size of key, n=size of the hash
  - MACs with known message-MAC pairs
    - Can either attack keyspace (cf key search) or hash
    - 128-bit hash looks vulnerable, 160-bits better

HMAC Design Objectives

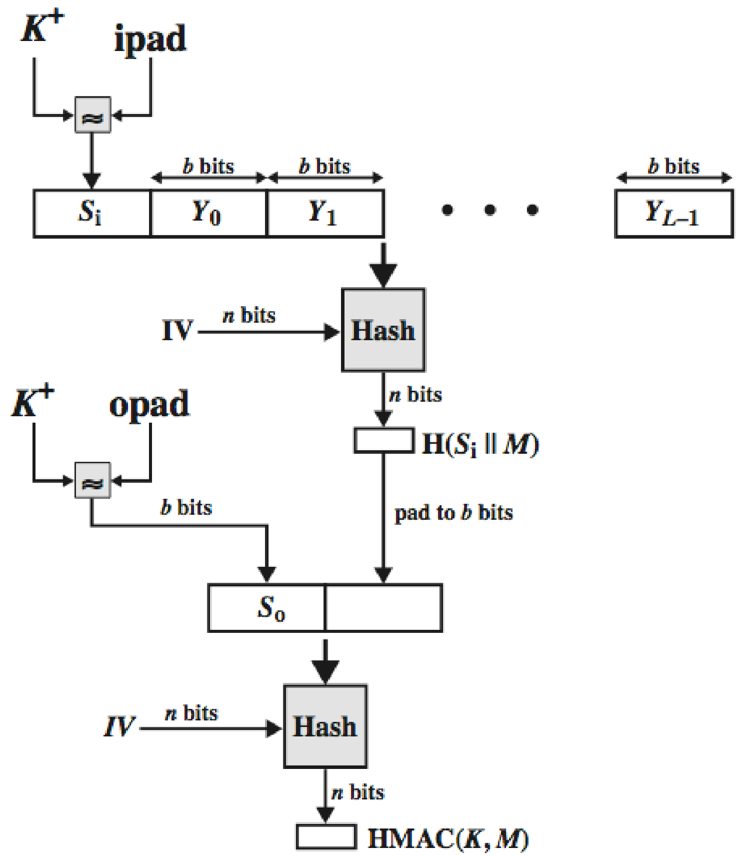
- Keyed Hash ⇒ includes a key along with message
- HMAC is a general design. Can use any hash function ⇒ HMAC-MD5, HMAC-AES
- Uses hash functions without modifications
- Allow for easy replace-ability of embedded hash function
- Preserve original performance of hash function without significant degradation
- Uses and handles keys in a simple way.
- Has well understood cryptographic analysis of authentication mechanism strength

HMAC

- RFC2104
- Uses hash function on the message:

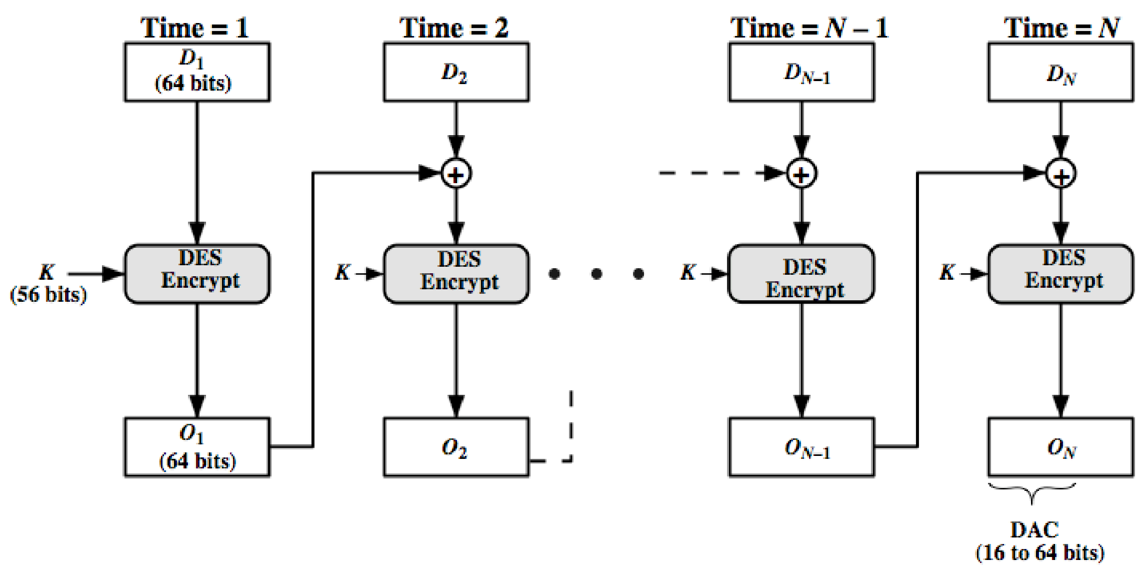
  $HMAC_K(M) = H[(K^+ \oplus opad) || H[(K^+ \oplus i$

  - Where K^+ = key padded to b-bits or hashed to b-bits if |k|>b
  - b = block size for the hash
  - opad, ipad are constants
  - ipad = 36 repeated b/8 times
    opad = 5C repeated b/8 times
- Any hash function can be used
  - E.g., MD5, SHA-1, RIPEMD-160, W
- Proved that security of HMAC relates to
  algorithm



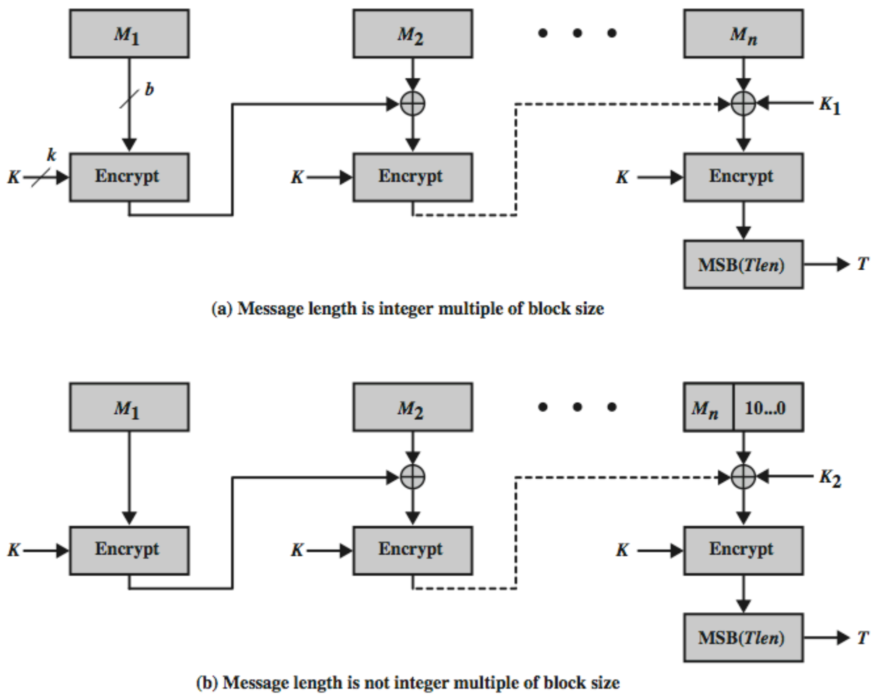
Using Symmetric Ciphers for MACs

- Can use any block cipher chaining mode and use final block as a MAC
- **Data Authentication Algorithm (DAA)** = DES-CBC
  - Using IV=0 and zero-pad of final block
- For single block message X, T=MAC(K, X)
  Weakness: T is also MAC of 2-block message X||(X⊕T)



Cipher-based Message Authentication Code (CMAC)

- Black and Rogaway fixed DAA problem by using 3 keys. Iwata updated by generating 3 keys from a single key.
- Adopted by NIST SP800-38B
- Two n-bit keys from a k-bit encryption key
- $L=E(K,0^n)$
- $K_1=L\cdot x$
- $K_2=L\cdot x^2$
- $\cdot$=Multiplication in $GF(2^n)$
- Using a irreducible polynomial with min 1's
  - $x^{64}+x^4+x^3+x+1$ for 64 bits
  - $x^{128}+x^7+x^2+x+1$ for 128 bits



Authenticated Encryption

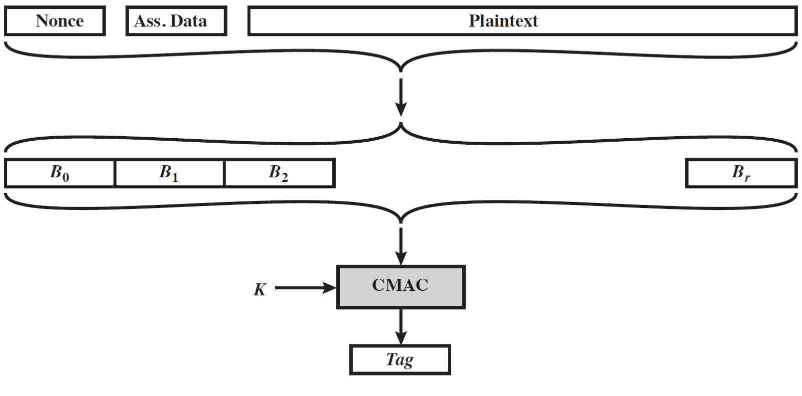
- Confidentiality + Integrity:

1. Hash-then-encrypt: E(K, (M || H(M))
2. MAC-then-encrypt: $E(K_2, (M \| MAC(K_1, M))$
   Used in SSL/TLS
3. Encrypt-then-MAC: $(C=E(K_2, M), T=MAC(K_1, C)$
   Used in IPsec
4. Encrypt-and-MAC: $(C=E(K_2, M), T=MAC(K_1, M)$
   Used in SSH

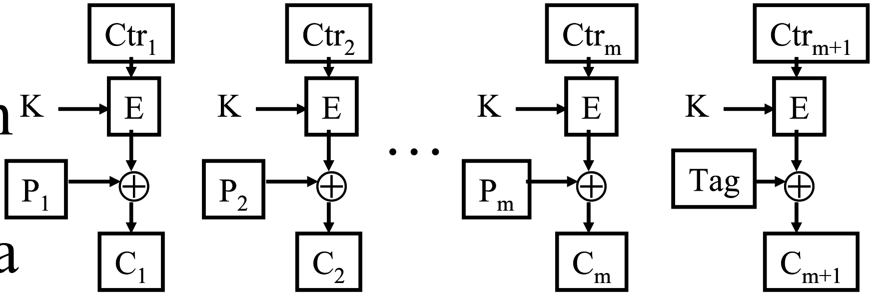
- But security vulnerabilities with all these
- NIST fixed these vulnerabilities with CCM and GCM

CCM

- Counter with Cipher Block Chaining-MAC
- NIST SP 800-38C for WiFi
- Algorithmic ingredients
  - AES encryption algorithm
  - CTR mode of operation
  - CMAC authentication algorithm
- Single key for both encryption & MAC
- Counters are generated using a counter generation function
- 2 passes over plaintext: MAC+E
- Associate data = headers in clear

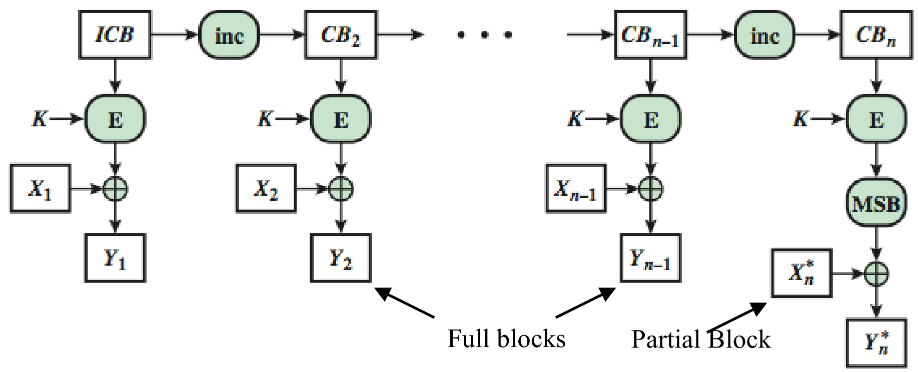


(a) Authentication



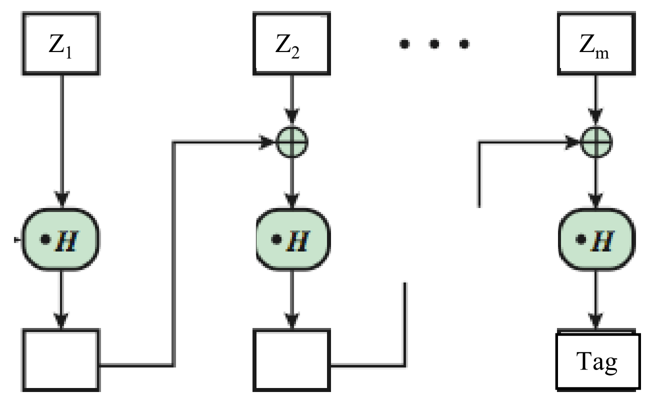
Galois/Counter Mode (GCM)

- NIST standard SP 800-38D, pa
- Uses two functions:
  - GCTR - CTR mode with in
  - GHASH - a keyed hash fun
- GHASH: plaintext xor'ed with key H in GF(2^{128}) to generate a H=E[K,0^{128}]



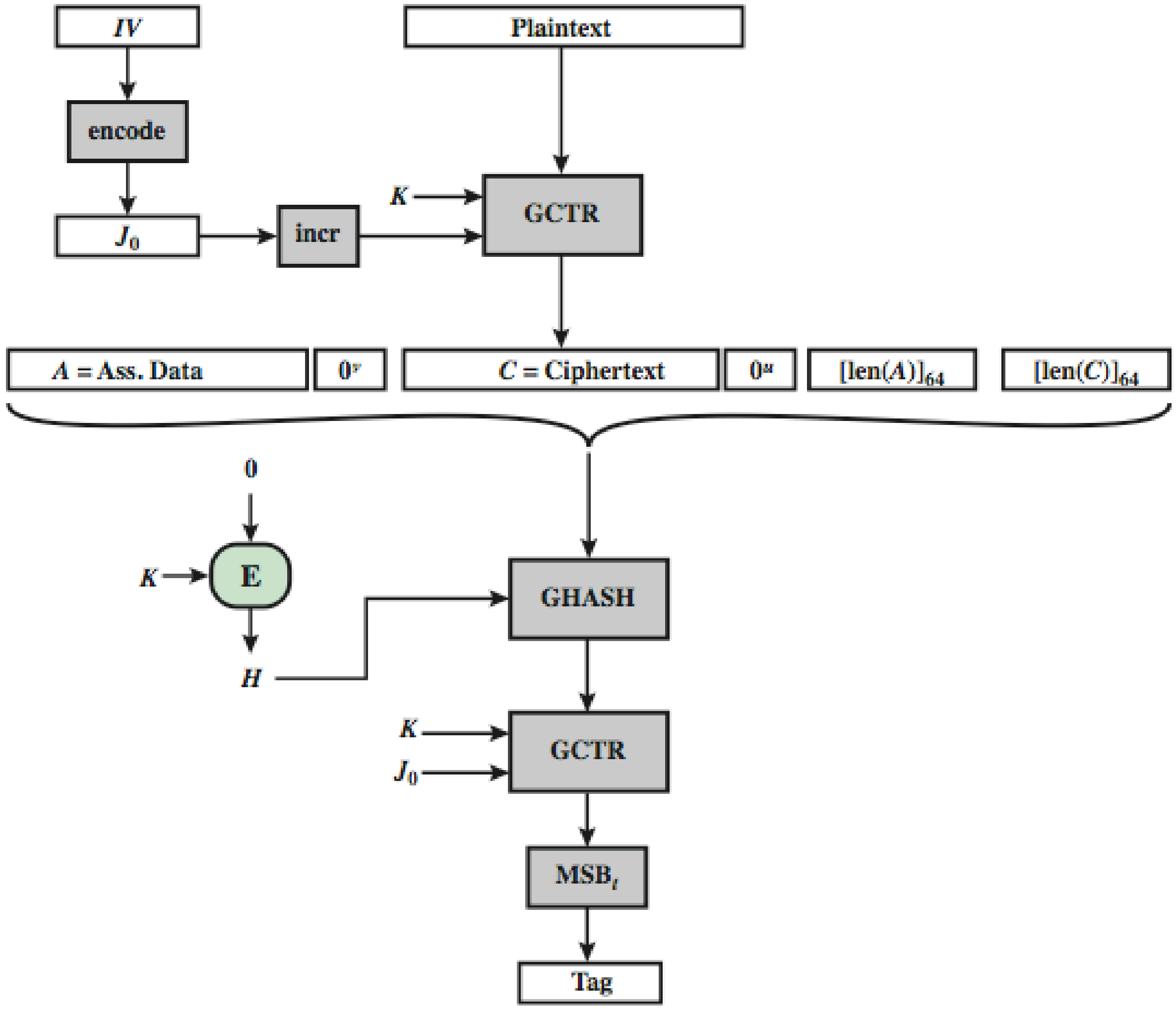
(b) $GCTR_K(ICB, X_1 \| X_2 \| \ldots \| X_n^*) = Y_n^*$

- Z_i's are constructed from the encrypted text Y_i and associated data
- MAC-only mode also



(a) $GHASH_H(X_1 \| X_2 \| \ldots \| X_m) =$ Tag

GCM Mode Overview

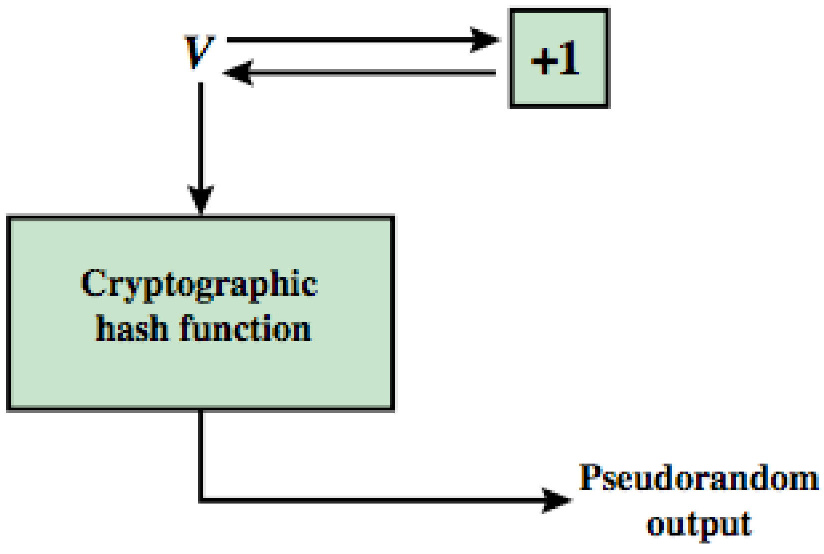


PRNG Using Hash and MACs

- Essential elements of Pseudo-Random Number generation:
  - Seed value
  - Deterministic algorithm
- Seed must be known only as needed
- PRNG can be based on
  1. Encryption algorithm
  2. Hash function (ISO18031 & NIST SP 800-90)
  3. MAC (NIST SP 800-90)

PRNG using a Hash Function

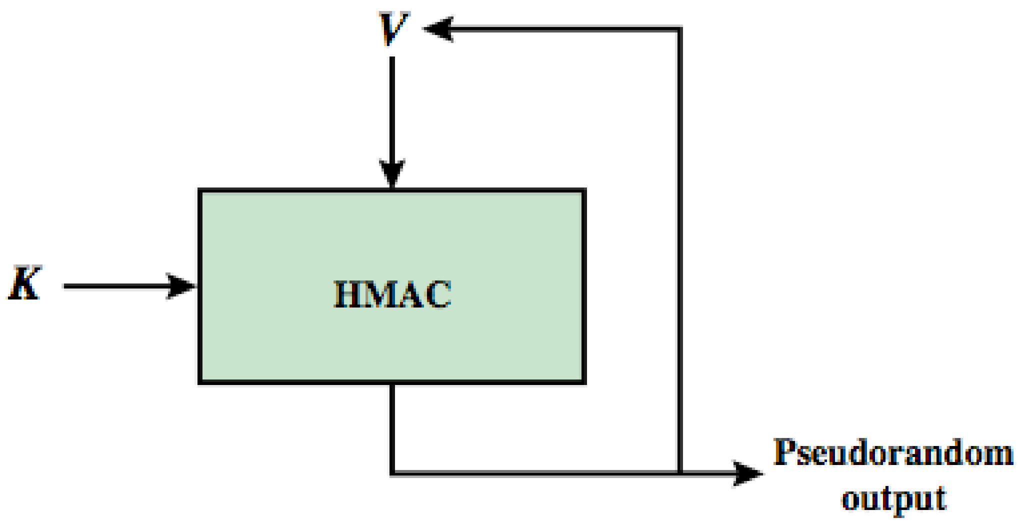
- SP800-90 and ISO18031
  - Take seed V
  - Repeatedly add 1
  - Hash V
  - Use n-bits of hash as random value
- Secure if good hash used



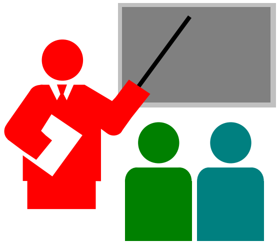
(a) PRNG using cryptographic hash function

PRNG using a MAC

- SP800-90, IEEE 802.11i, TLS
  - Use key
  - Input based on last hash in various ways



(b) PRNG using HMAC



Summary

1. Message authentication = Integrity + Source Authentication (with or without encryption)
2. Double public key encryption can be used but complex ⇒ Hash with a secret key
3. HMAC is a general procedure usable with any hash function ⇒ HMAC-MD5, HMAC-AES
4. Data Authentication Algorithm (DAA) was found insecure ⇒ Fixed by CMAC using keys derived from a single key
5. Authenticated Encryption:
    1. CCM = CMAC + Counter mode
    2. GCM = Multiplication in GF(2^{128}) + Counter mode
6. Pseudorandom Number Generation (PRNG) using Hash Functions and MACs

Homework 12

There are four general approaches in authenticated encryption: HtE, MtE, EtM, and E&M.

A. Which approach is used for CCM?

B. Which approach is used for GCM?

Lab 12: Snort for Intrusion Detection

- The snort homepage: www.snort.org.
- Snort FAQ: www.snort.org/snort/faq
- Snort Overview: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/
- Write Your Own Snort Rules: http://archive.oreilly.com/pub/h/1393

❑ Install Snort
- For Mac Users: http://deepnode.us/apps/macosx_snort_install.pdf (snort section)
- For windows User: https://www.snort.org/ & follow this link: https://www.securityarchitecture.com/learning/intrusion-detection-systems-learning-with-snort/configuring-snort/

Lab 12 (Cont)

- Use ipconfig or ifconfig to find the wireless interface on your computer
- Try various flags with Snort
- On Mac/Linux, you need to use sudo to invoke root privilege, e.g., sudo snort –v –i your_wireless_interface
- On Windows, you need to run with administrator privilege
- Write a rule that allows Snort to capture all TCP packets.
- Run snort and access some website/websites, i.e., use port 80.
- Go to the log directory and check the files
  - Hint: for mac use u2spewfoo command to open the files for windows you can view it with notepad.
- Submit the alert file in addition to log file.

Acronyms

AE	Authenticated encryption
AES	Advanced Encryption System
CBC	Cipher Block Chaining
CCM	Counter mode with Cipher block chaining
CMAC	Cipher Message Authentication Code
CTR	Counter mode
DAA	Data Authentication Algorithm
DES	Data Encryption System
E&M	Encrypt-and-MAC
EtM	Encrypt-then-MAC
GCM	Counter with Cipher-block chaining
GCTR	Counter mode with incremented counter
GF	Galois Field
GHASH	G-Hash - a keyed hash function
HMAC	Hybrid Message Authentication Code
HtE	Hash-then-encrypt

Acronyms (Cont)

IEEE	Institution of Electrical and Electronics Engineers
IPsec	IP Security
ISO	International Standards Organization
IV	Initialization Value
MAC	Message Authentical Code
MACS	Message Authentical Codes
MD5	Message Digest 5
MtE	MAC-then-encrypt
NIST	National Institute of Science and Technology
PRa	Private for a
PRb	Private for b
PRF	Pseudo-Random Function
PRNG	Pseudo-Random Number Generator
PUa	Public a
PUb	Public b
RFC	Request for Comments

Acronyms (Cont)

- RIPEMD RACE Integrity Primitives Evaluation Message Digest)
- SHA Secure Hash Algorithm
- SP Standard Protocol
- SSH Secure Socket H
- SSL Secure Socket Layer
- TLS Transmission Label Security
- WiFi Wireless Fidelity

Scan This to Download These Slides

Raj Jain

http://rajjain.com

Related Modules

CSE571S: Network Security (Spring 2017),
http://www.cse.wustl.edu/~jain/cse571-17/index.html

CSE473S: Introduction to Computer Networks (Fall 2016),
http://www.cse.wustl.edu/~jain/cse473-16/index.html

Wireless and Mobile Networking (Spring 2016),
http://www.cse.wustl.edu/~jain/cse574-16/index.html

CSE571S: Network Security (Fall 2014),
http://www.cse.wustl.edu/~jain/cse571-14/index.html

Audio/Video Recordings and Podcasts of
Professor Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw