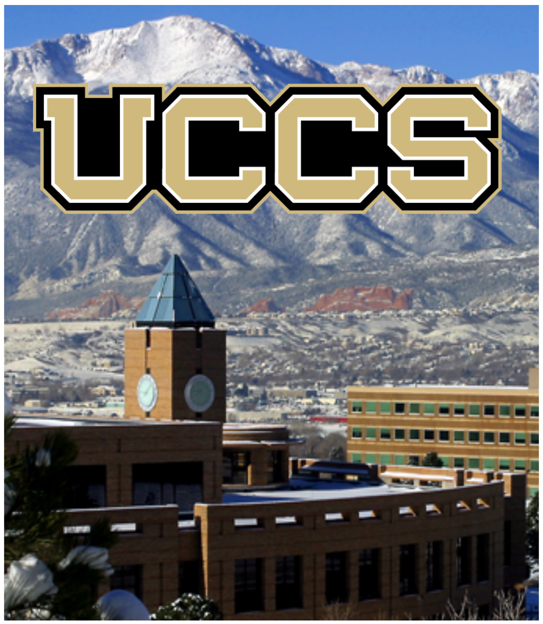


Cryptographic Hash and Integrity Protection

Message Authentication Code

Sang-Yoon Chang, Ph.D.

Module: Message Authentication Code

Message Authentication Approaches

Message Authentication Code (MAC)

MAC Security

MAC Using Block Ciphers, e.g., DAA, CMAC

Message Authentication

Message authentication is to:

- Protect message integrity
- Sender authentication

Message Authentication

Message authentication is to:

- Protect message integrity
- Sender authentication

Prevent threats, including:

- Masquerading/spoofing
- Content modification
- Sequence modification
- Timing modification

Message Authentication

Message authentication is to:

- Protect message integrity
- Sender authentication

Message authentication approaches:

- Hash function
- Encryption
- Message authentication code (MAC)

Symmetric Encryption for Message Authentication

Only receiver and sender know the key

Receiver knows that sender created the message

If altered by an attacker, then the plaintext format would change

Message Authentication Code (MAC)

Creates a small fixed-sized block
MAC depends on message and the key
Need not be reversible

Message Authentication Code (MAC)

Creates a small fixed-sized block

MAC depends on message and the key

Need not be reversible

Difference with Hash

Message Authentication Code (MAC)

Creates a small fixed-sized block

MAC depends on message and the key

Need not be reversible

Difference with Hash

Difference with encryption/decryption

Message Authentication Code (MAC)

Creates a small fixed-sized block
MAC depends on message and the key
Need not be reversible

Sender appends the MAC to message
The authorized parties share same key
Receiver computes based on message and checks the match with the MAC

Why MAC?

Application requirement

Performance

Flexibility

Longer protection

Why MAC?

Application requirement

Performance

Flexibility

Longer protection

Generally efficient, especially compared to digital signature

Brute-Force Attack on MAC

Assume key (K bits) and MAC (N bits)

Attack on the key: O(2^K)

More effort than finding decryption key because multiple keys possible

Attack on MAC: O(2^n)

Attack on one-way/weak collision resistance

Overall min(2^K,2^N)

MAC Requirements

1. Large enough entropy

2. Collision resistance

3. MAC(K,M) is uniformly distributed

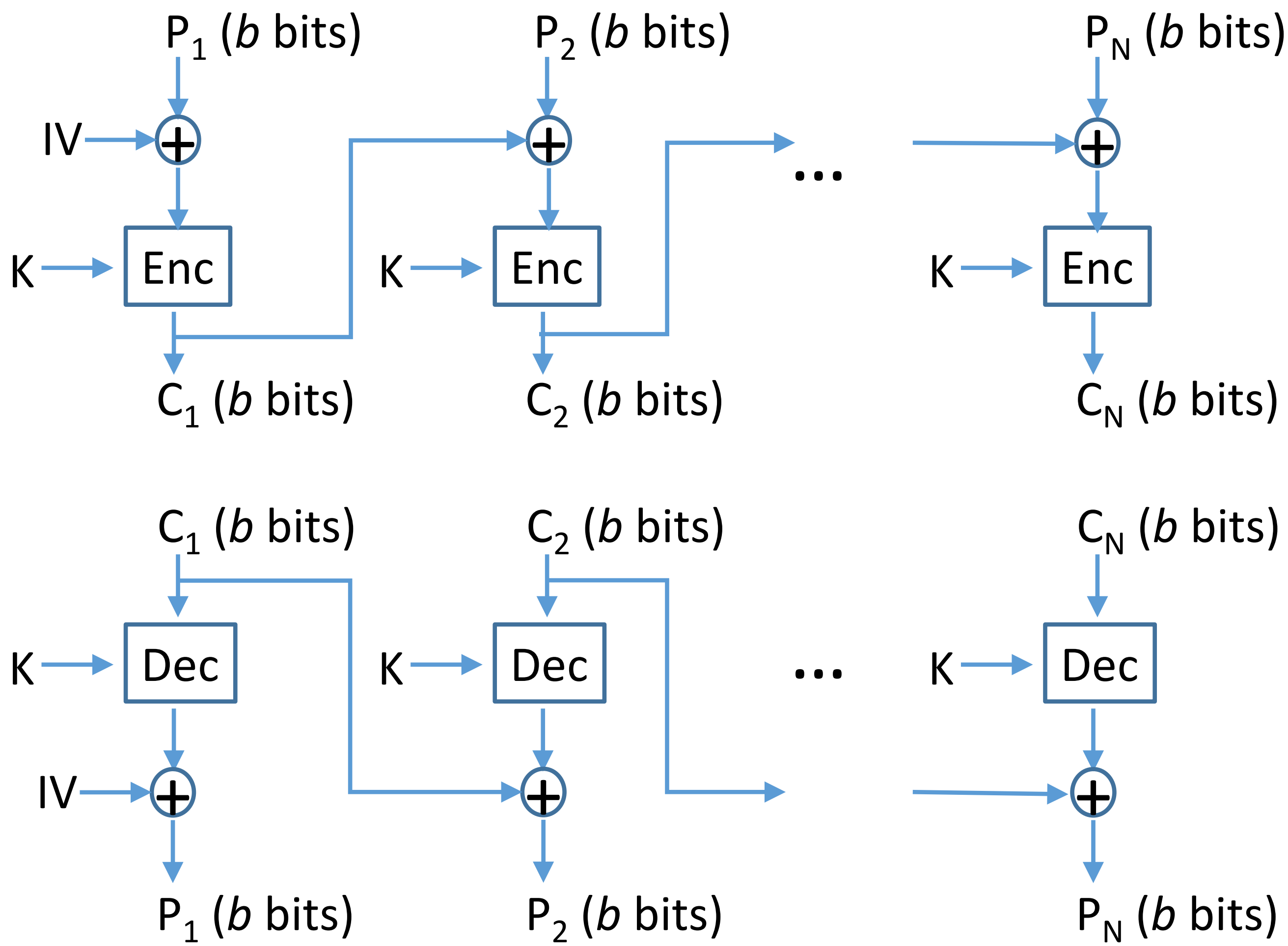
4. Avalanche Effect

MAC Using Block Ciphers

Two examples:

- DAA (Data Authentication Algorithm)
- CMAC (Cipher-Based MAC)

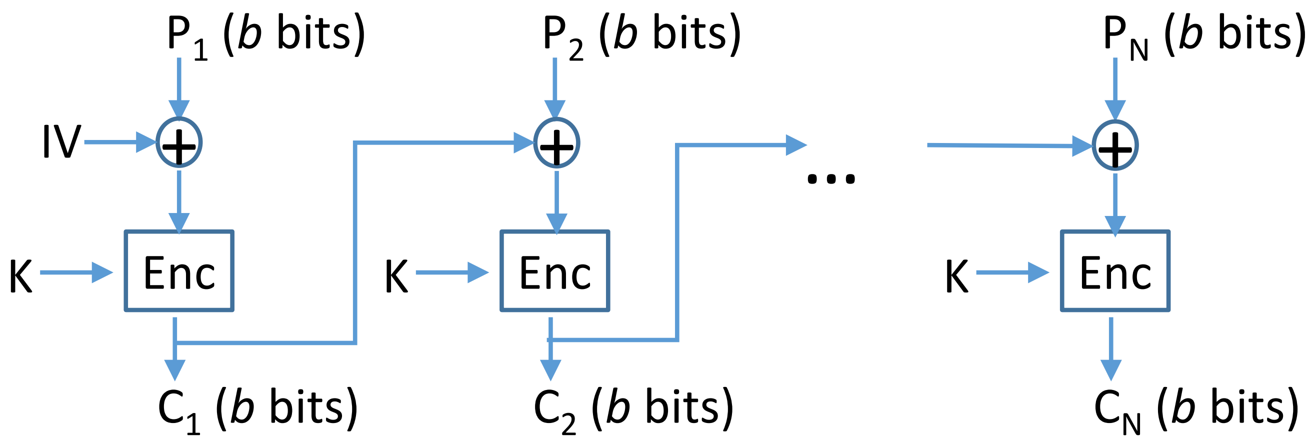
CBC Recap



CBC Encryption

CBC Decryption

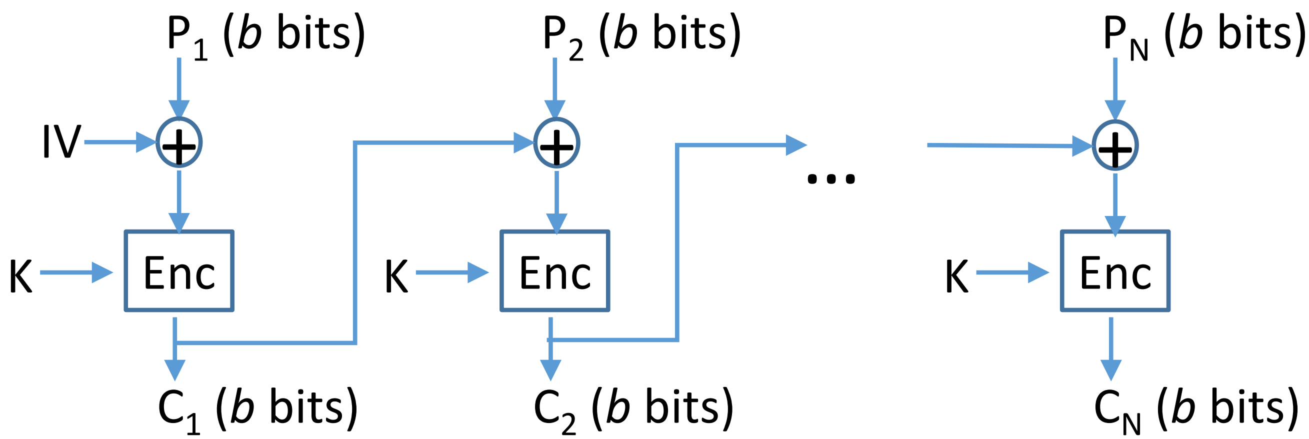
Data Authentication Algorithm (DAA)



DES for Enc. (b=64 and K is of 56 bits)

Use data blocks for Pi’s

Data Authentication Algorithm (DAA)

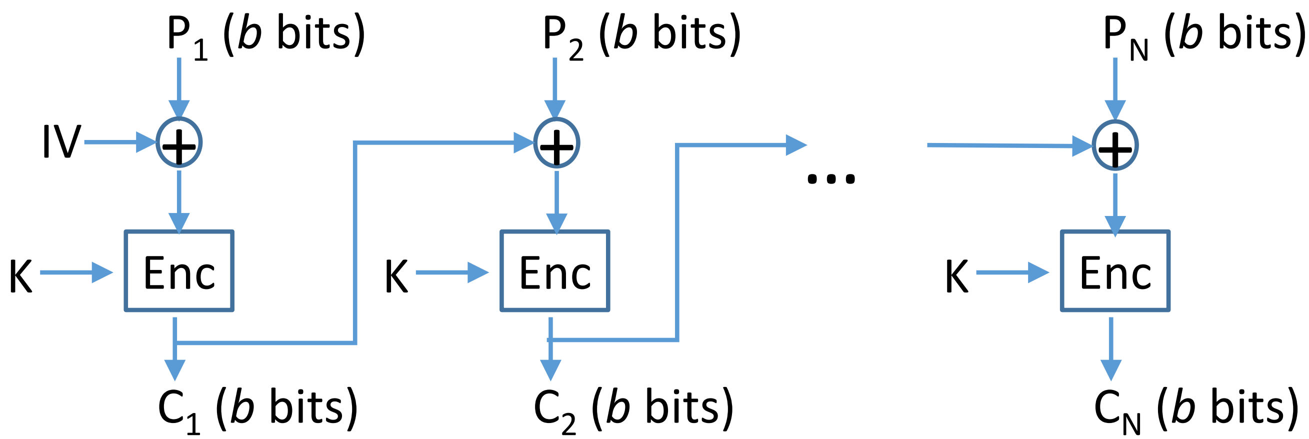


DES for Enc. (b=64 and K is of 56 bits)

Use data blocks for Pi's

MAC is leftmost bits of C_N (16-64 bits)

Data Authentication Algorithm (DAA)



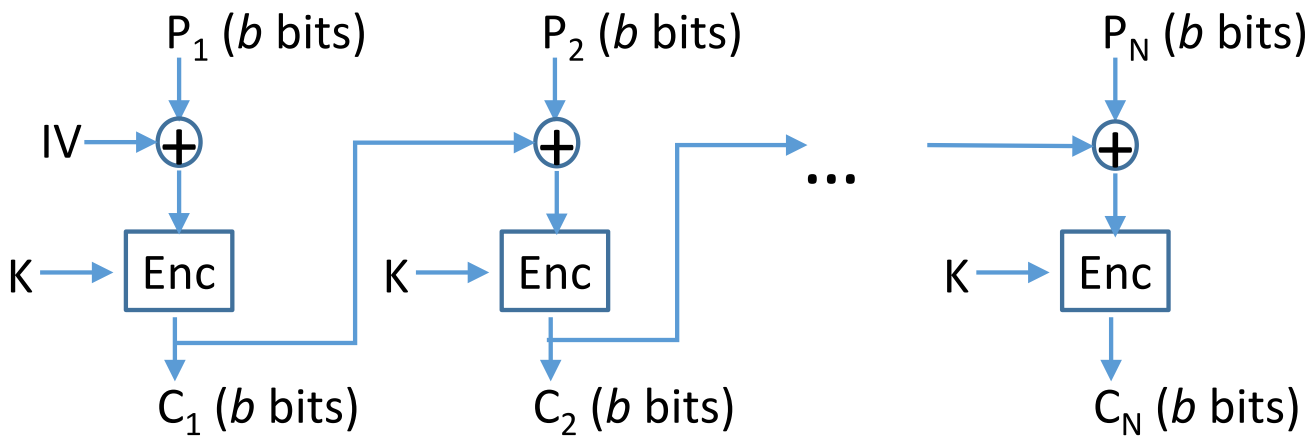
DES for Enc. (b=64 and K is of 56 bits)

Use data blocks for Pi’s

MAC is leftmost bits of C_N (16-64 bits)

Too small for security nowadays

Data Authentication Algorithm (DAA)



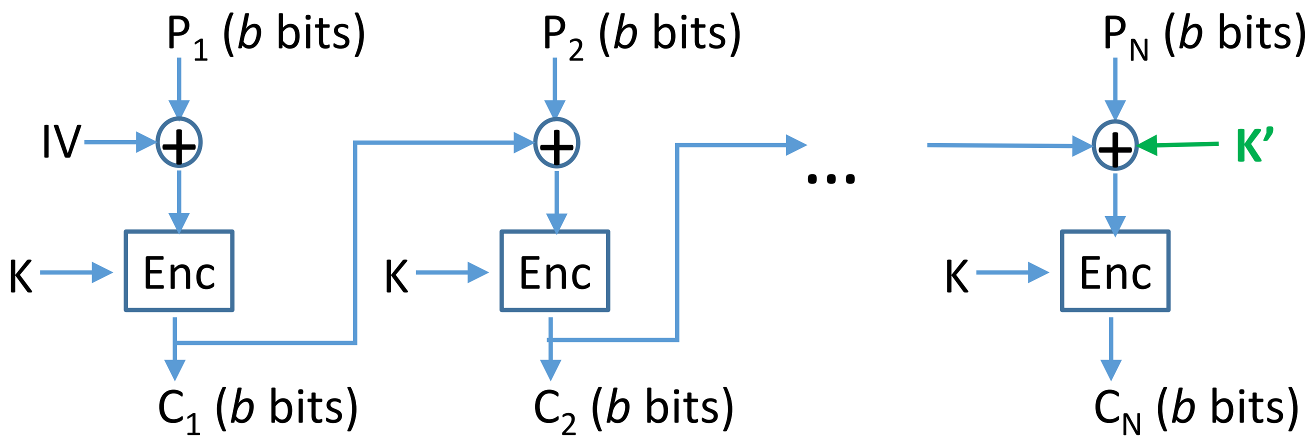
DES for Enc. (b=64 and K is of 56 bits)

Use data blocks for Pi's

MAC is leftmost bits of C_N (16-64 bits)

Also vulnerable, e.g., $X||X \oplus C_N$ if b evenly divides X

Cipher-Based MAC (CMAC)



Triple-DES or AES for Enc.

Use data blocks for Pi's

IV=0 and zero pad final block

MAC is leftmost bits of C_N

No longer vulnerable e.g., $X||X \oplus C_N$ if b evenly divides X