

# Cryptography Basics – Block ciphers and modes

Assignment Project Exam Help  
<https://powcoder.com>  
Add WeChat powcoder

---

ECEN 4133  
Jan 26, 2021

# Alternative to stream cipher:

## Block Ciphers

---

Today's most common block cipher:

**AES** (Advanced Encryption Standard)

Designed by NIST competition, long public comment/discussion period

Widely believed to be secure, *but we don't know how to prove it*

Variable **key size** and **block size**

We'll use 128-bit key, 128-bit block (also exist 192-bit and 256-bit versions)

Ten **rounds**: Split **k** into ten **subkeys**, performs set of operations ten times, each with diff. subkey

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# Each AES round

128-bits in, 128-bit sub-key, 128-bits out

Four steps:

picture as operations on a 4x4 grid of 8-bit values

## 1. Non-linear step

Run each byte thru a non-linear function (lookup table)

## 2. Shift step

Circular-shift each row:  $i^{\text{th}}$  row shifted by  $i$  (0-3)

## 3. Linear-mix step

Treat each column as a 4-vector; multiply by a constant invertible matrix

## 4. Key-addition step

XOR each byte with corresponding byte of round subkey

To decrypt, just undo the steps, in reverse order

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# Remaining problem: How to encrypt longer messages?

---

## Padding

Can only encrypt in units of cipher blocksize, but message might not be multiples of blocksize

*Solution:* Add padding to end of message

Must be able to recognize and remove padding afterward

Common approach:

Add  $n$  bytes that have value  $n$

[Caution: What if message ends at a block boundary?]

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# Cipher modes

---

We know how to encrypt one block,  
but what about multiblock messages?

Different methods, called “cipher modes”

Straightforward (but bad) approach:

**ECB mode** (encrypted codebook)

Just encrypt each block independently

$$C_i := E_k(P_i)$$

[Disadvantages? Solutions?]

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# Cipher modes

---

We know how to encrypt one block,  
but what about multiblock messages?

Different methods, called “cipher modes”

Straightforward (but bad) approach:

**ECB mode** (encrypted codebook)

Just encrypt each block independently

$$C_i := E_k(P_i)$$

[Disadvantages? Solutions?]

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder



Plaintext

Pseudorandom

ECB mode

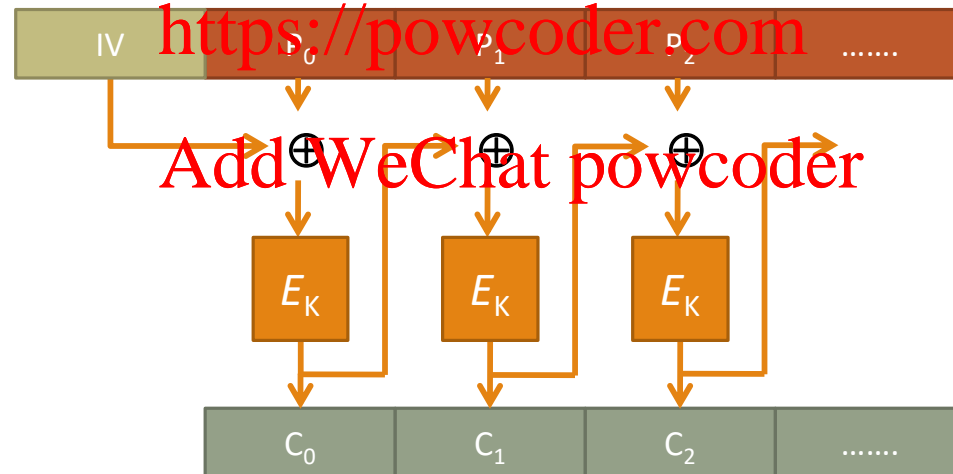
# Better (and common): CBC mode (cipher-block chaining)

For each block  $P_i$ :

$$C_i := E_k(P_i \text{ xor } C_{i-1})$$

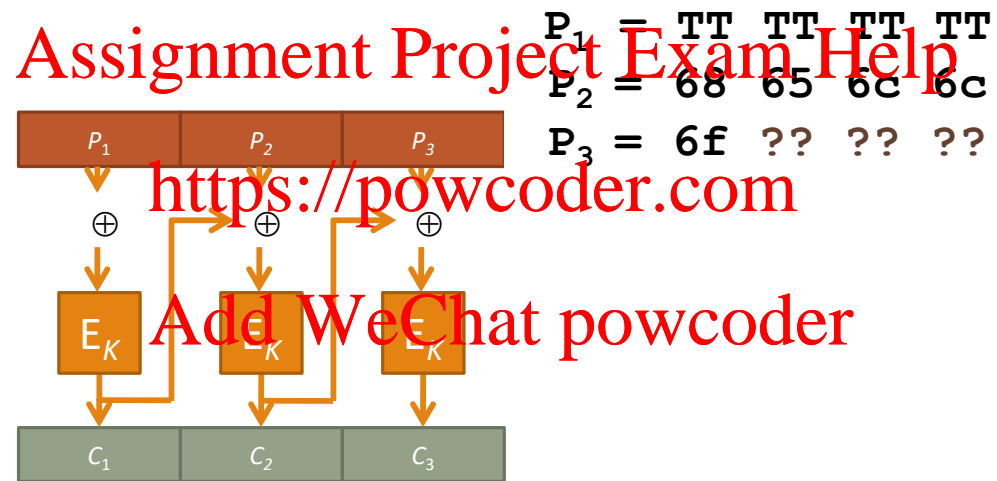
(Need to generate random IV ("Initialization Vector") at start)

[Pros and cons?]



# Padding oracle attack

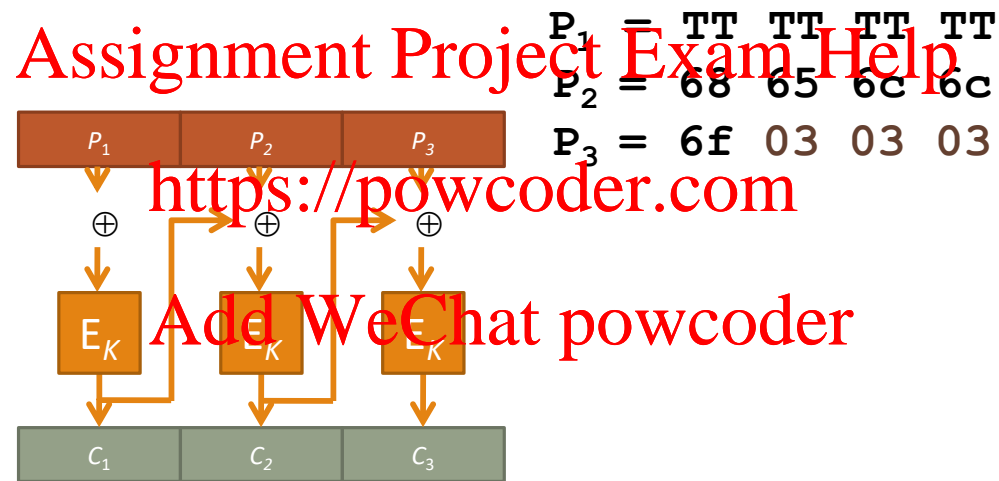
---





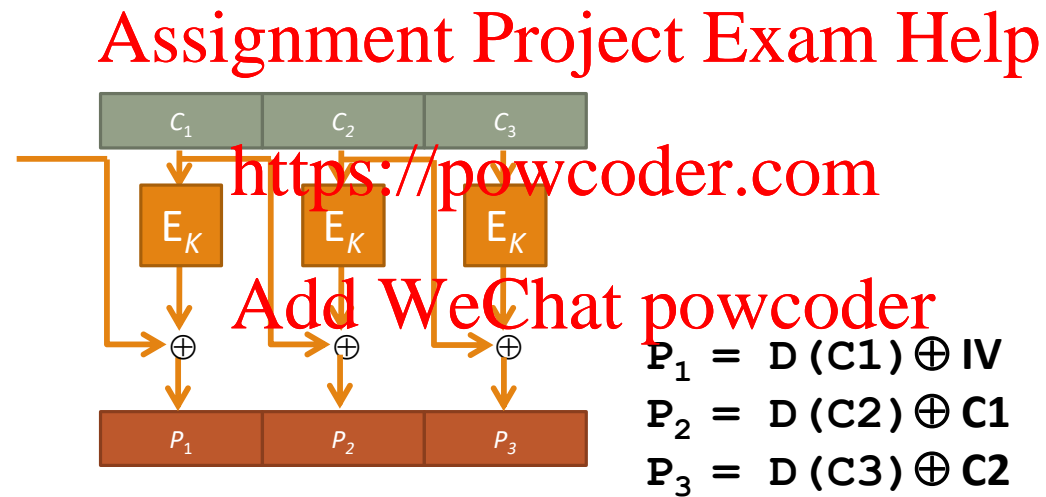
# Padding oracle attack

---

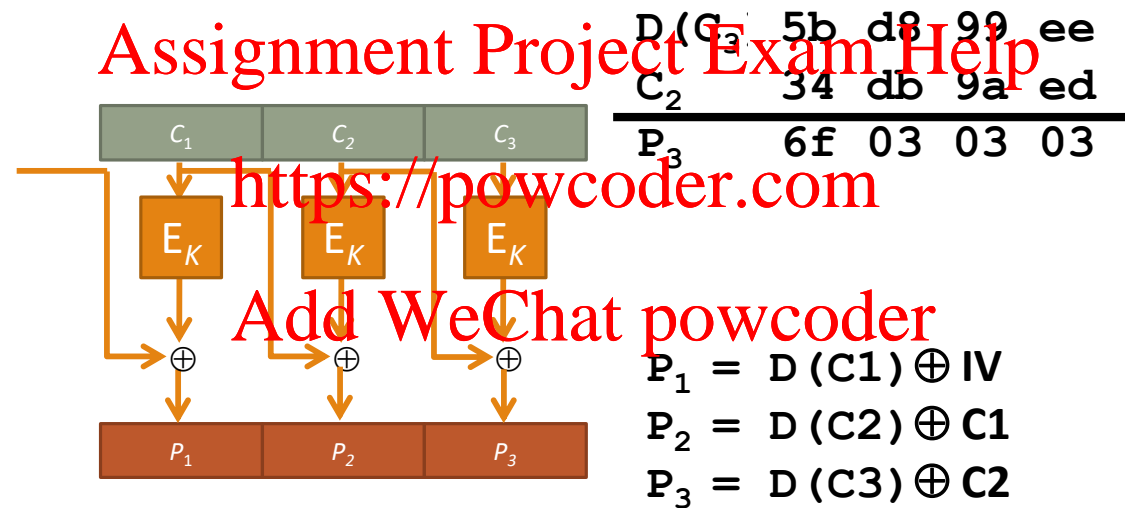


# Padding oracle attack

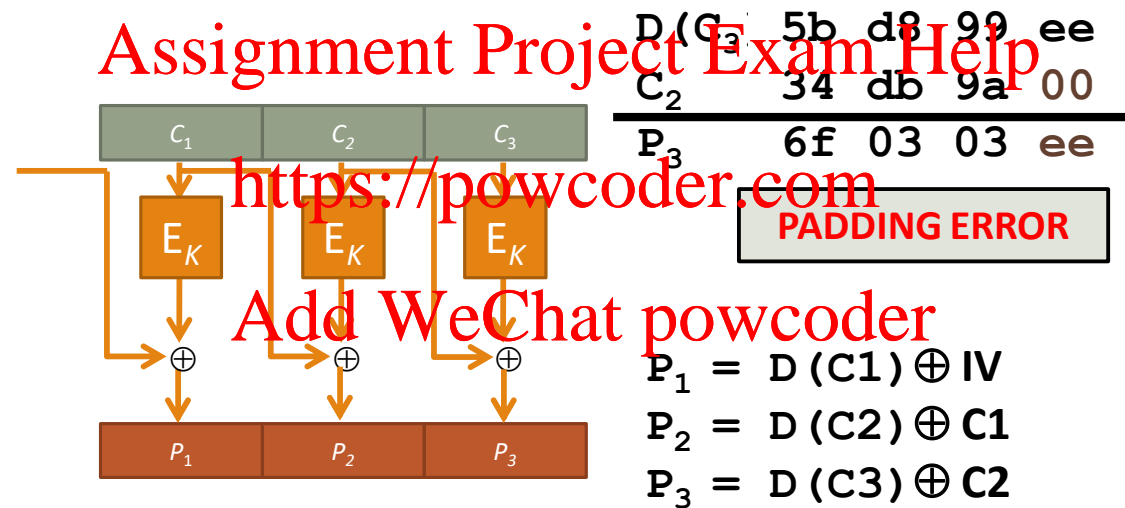
Decryption:



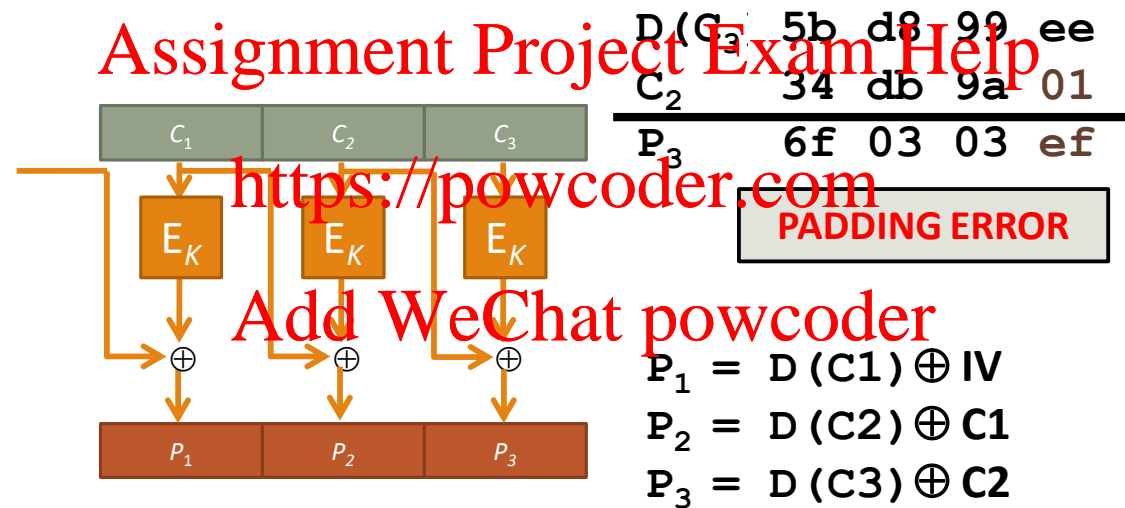
# Padding oracle attack



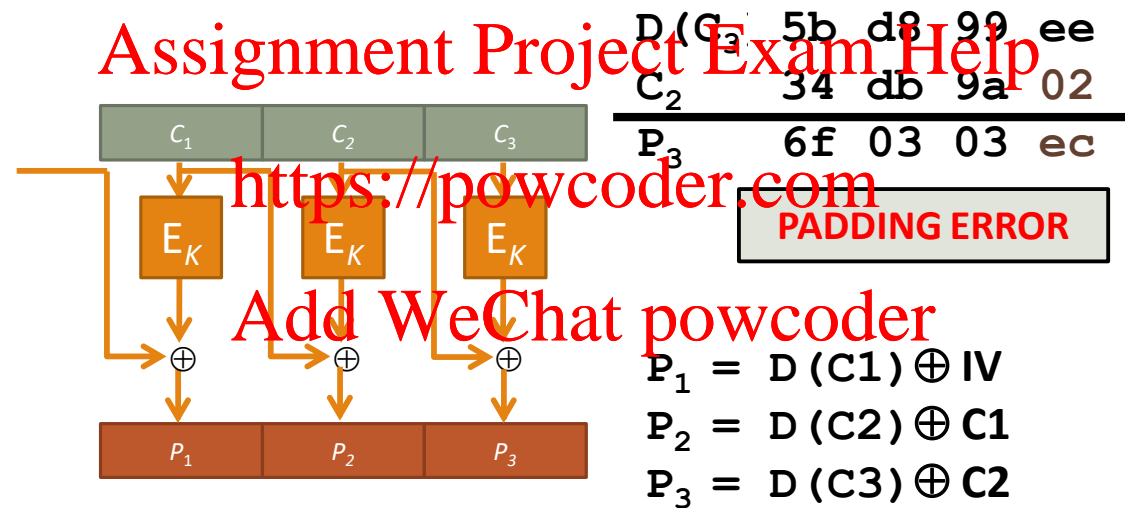
# Padding oracle attack



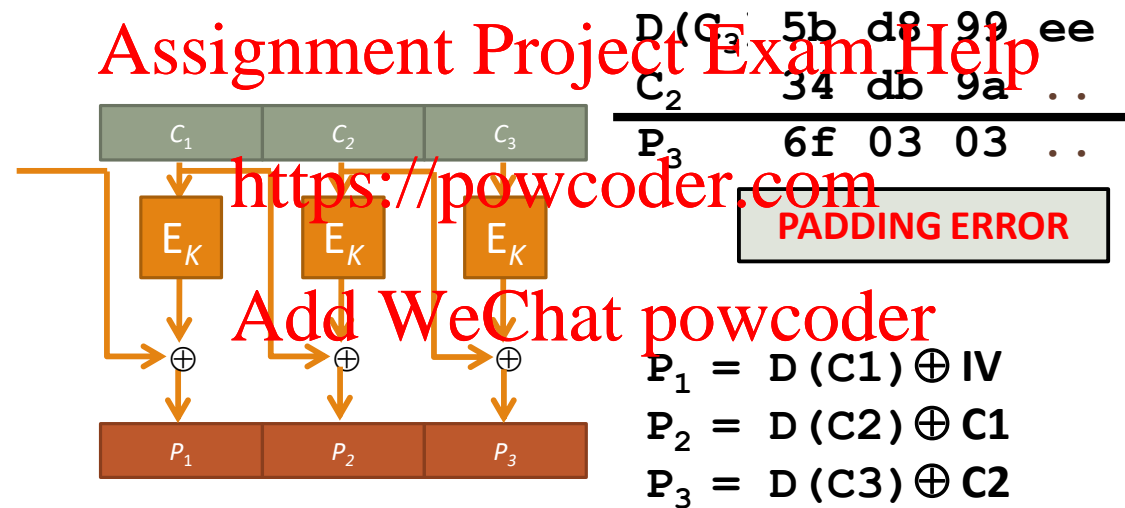
# Padding oracle attack



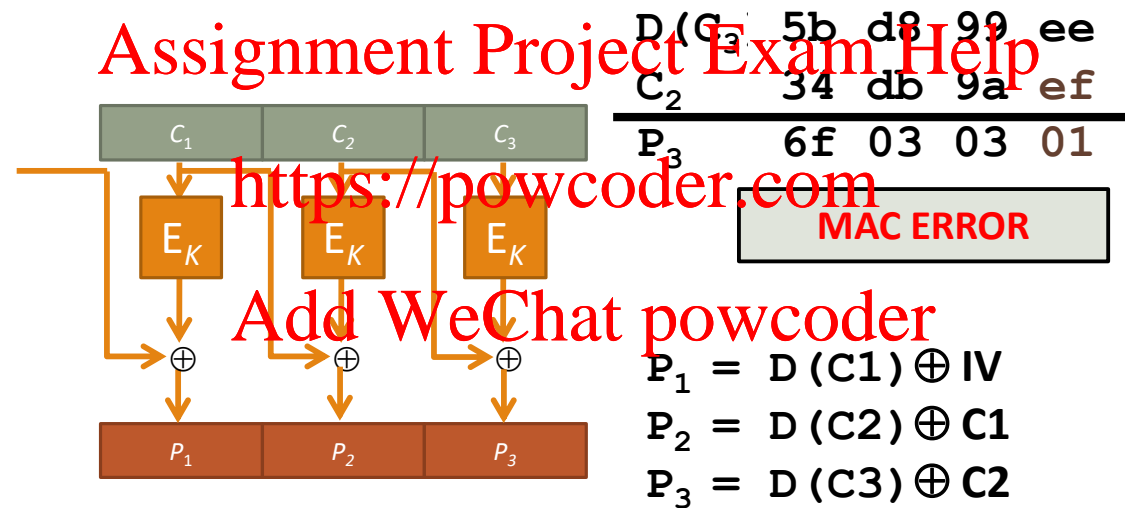
# Padding oracle attack



# Padding oracle attack



# Padding oracle attack





# Padding oracle attack

---

Original  $C_2$ : 34 db 9a ed

Modified  $C_2'$ : 34 db 9a ef

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

D(C <sub>3</sub> )	5b	d8	99	ee
C <sub>2</sub>	34	db	9a	ef
E <sub>3</sub>	6f	cb	b3	01

MAC ERROR

# Padding oracle attack

---

Original  $C_2$  : 34 db 9a ed

Modified  $C_2'$  : 34 db 9a ef

To get a MAC Error, It must be:  $D(C_3) \oplus C_2 = \text{xx xx xx 01}$   
(valid padding)

So what is  $D(C_3)$  ?

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# Padding oracle attack

---

Original  $C_2$  : 34 db 9a ed

Modified  $C_2'$  : 34 db 9a ef

To get a MAC Error, It must be  $D(C_3) \oplus C_2 = \text{xx xx xx 01}$   
(valid padding)

So what is  $D(C_3)$  ?

$$\begin{aligned} D(C_3) &= \text{xx xx xx 01} \oplus C_2' \\ &= \text{xx xx xx 01} \oplus 34 \text{ db 9a ef} \\ &= \text{xx xx xx ee} \end{aligned}$$

Also tells us the padding byte:

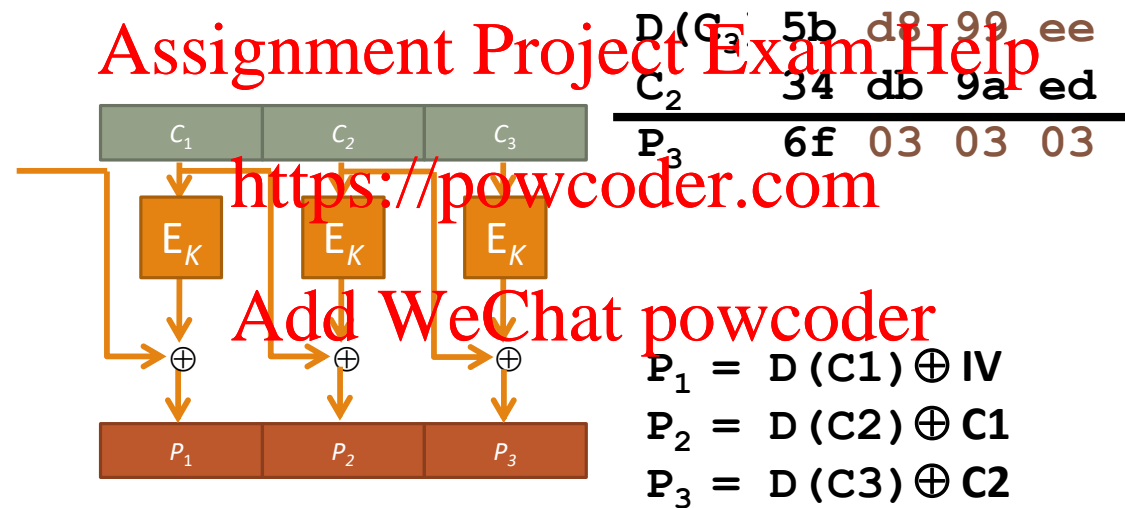
$$\begin{aligned} P_3 &= D(C_3) \oplus C_2 \\ &= \text{xx xx xx ee} \oplus 34 \text{ db 9a ed} \\ &= \text{xx xx xx 03} \\ &= \text{xx 03 03 03 (valid padding)} \end{aligned}$$

Assignment Project Exam Help

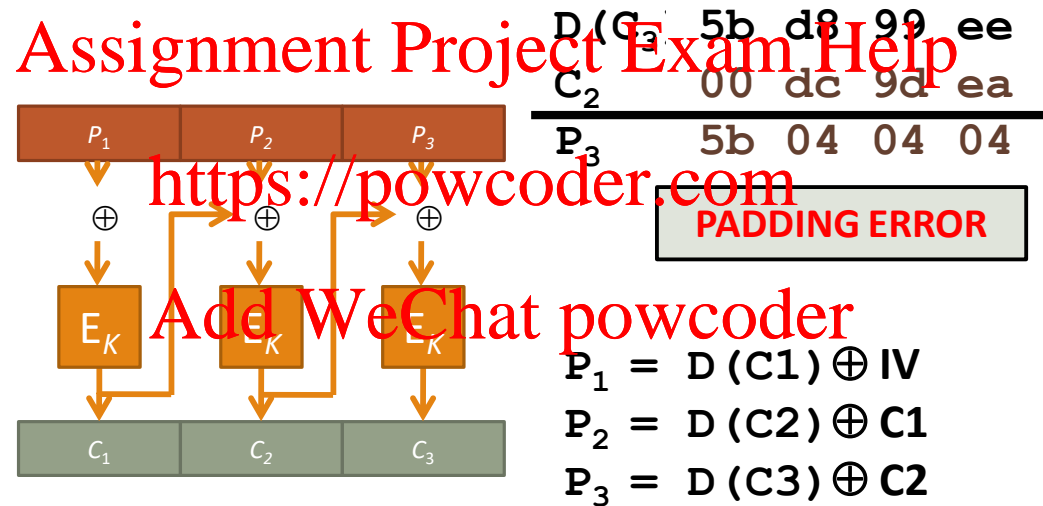
<https://powcoder.com>

Add WeChat powcoder

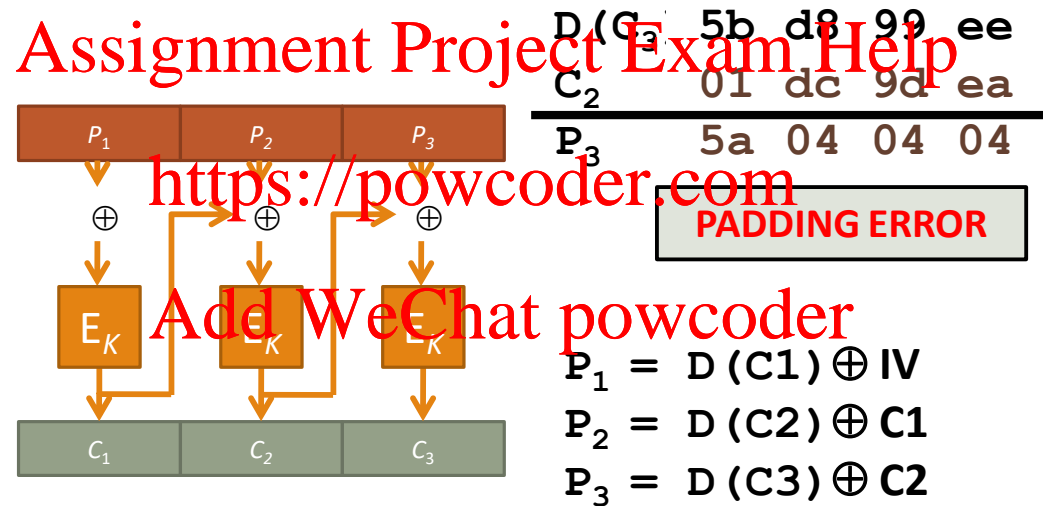
# Padding oracle attack



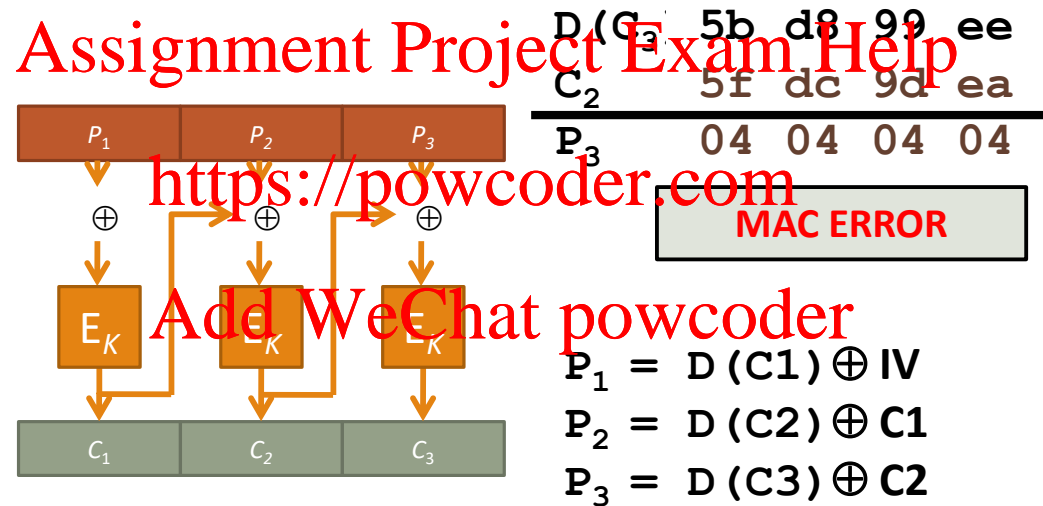
# Padding oracle attack



# Padding oracle attack



# Padding oracle attack



# Other modes

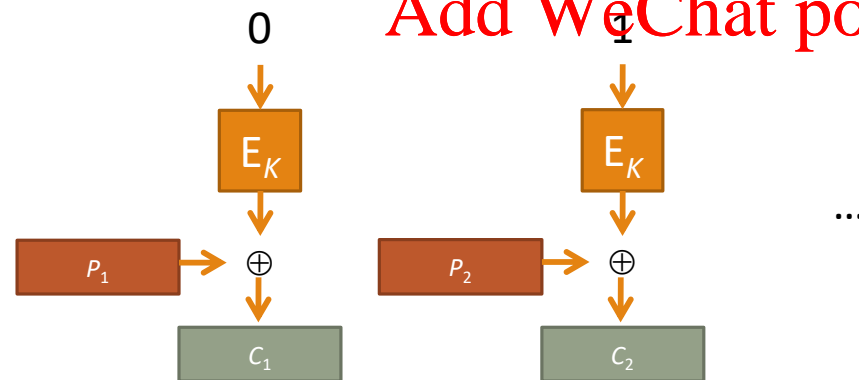
OFB, CFB, etc. – used less often

## Counter mode (CTR)

Essentially uses block cipher as a pseudorandom generator

XOR  $i^{\text{th}}$  block of message with  $E_K(\text{message\_id} || i)$

Turns a block cipher into a stream cipher!



Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder



# Building a **secure channel**

---

What if you want **confidentiality** and **integrity** at the same time?

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# Building a secure channel

---

What if you want **confidentiality** and **integrity** at the same time?

- *Encrypt, then add integrity,*  
not the other way around  
(reasons are subtle)
- Use separate keys for  
confidentiality and integrity
- Need two shared keys,  
but only have one?  
That's what PRGs are for!
- If there's a reverse (Bob to Alice) channel, use separate keys for that

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

# Modern encryption mode: Authenticated Encryption

AES-GCM – Galois/Counter Mode

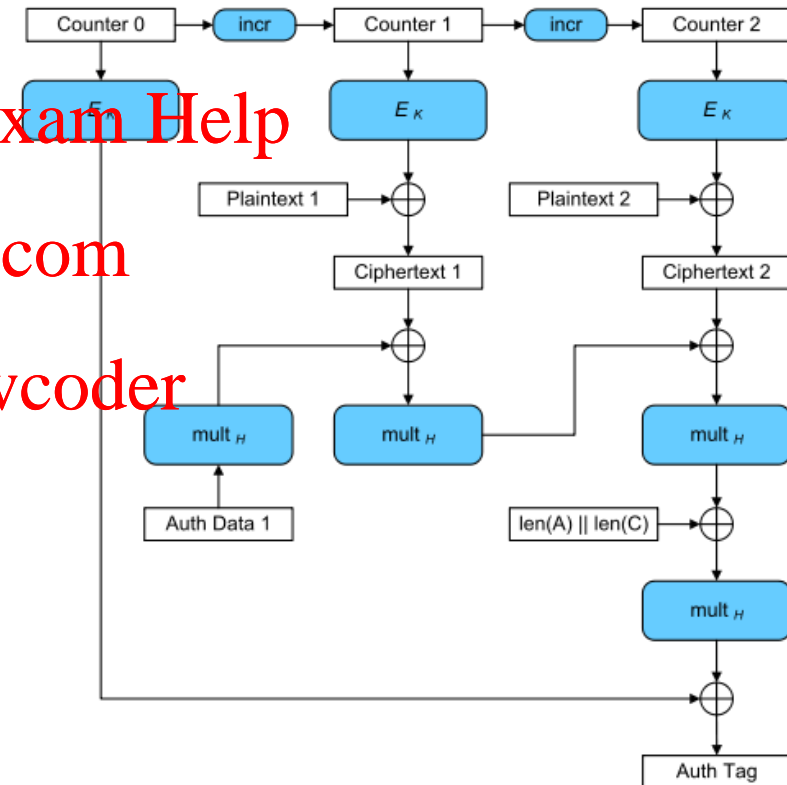
AES in CTR Mode for encryption

Galois Hashing for authentication

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder



---

*Assumption we've been making so far:*

Alice and Bob shared a secret key in advance

**Amazing fact:**

Alice and Bob can have a public conversation to derive a shared key!

**Assignment Project Exam Help**

<https://powcoder.com>

**Add WeChat powcoder**