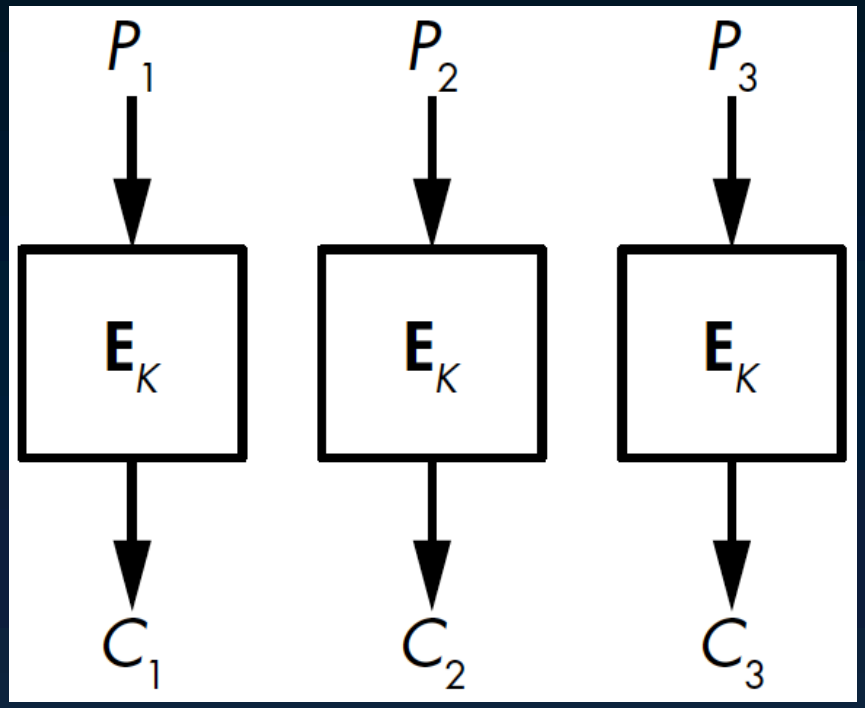
Applied Cryptography
CPEG 472/672
Lecture 3B

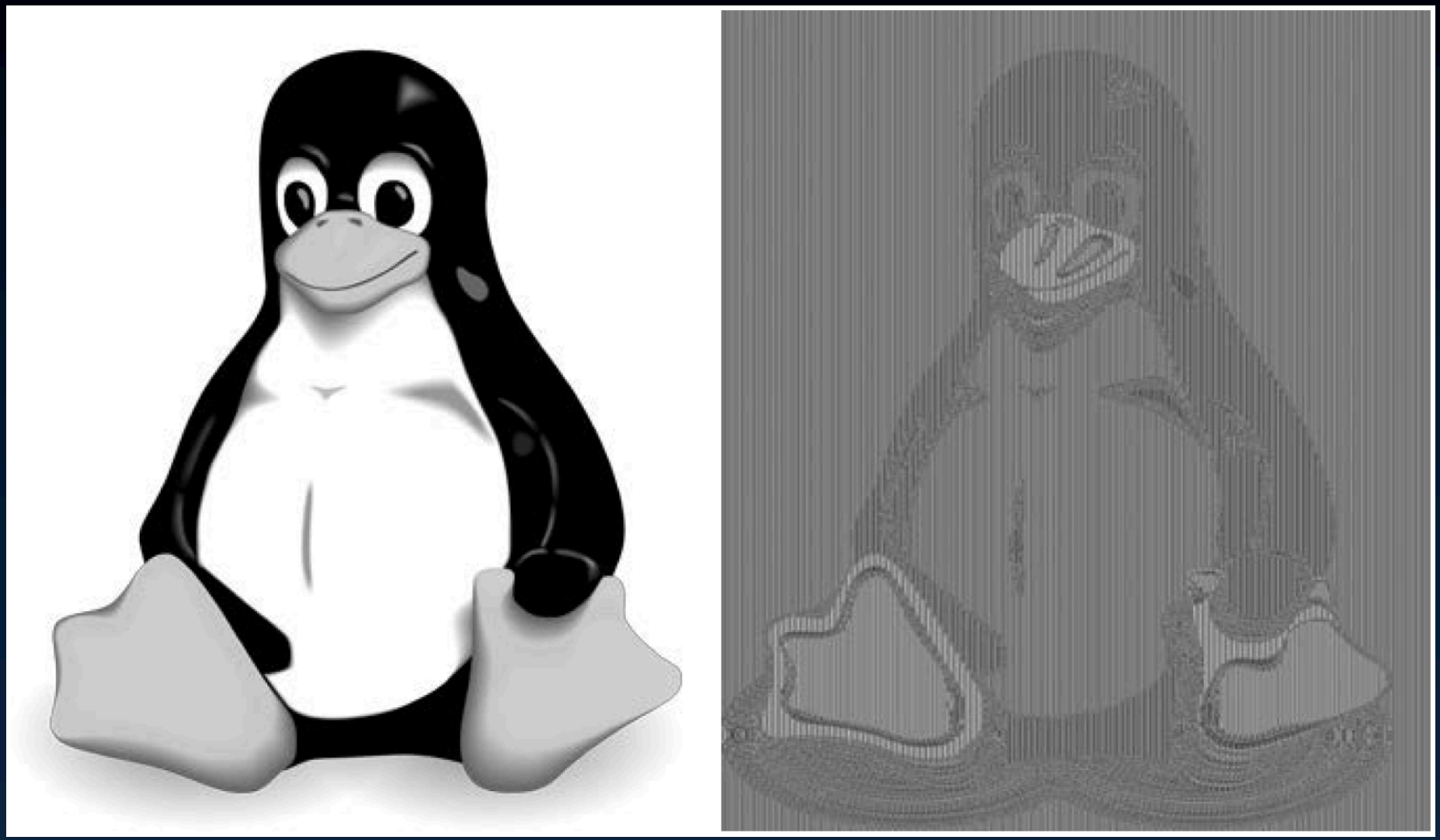
Instructor: Nektarios Tsoutsos

Modes of operation

- Electronic Codebook (ECB) Mode
  - Never use - not semantically secure
- Parallelizable

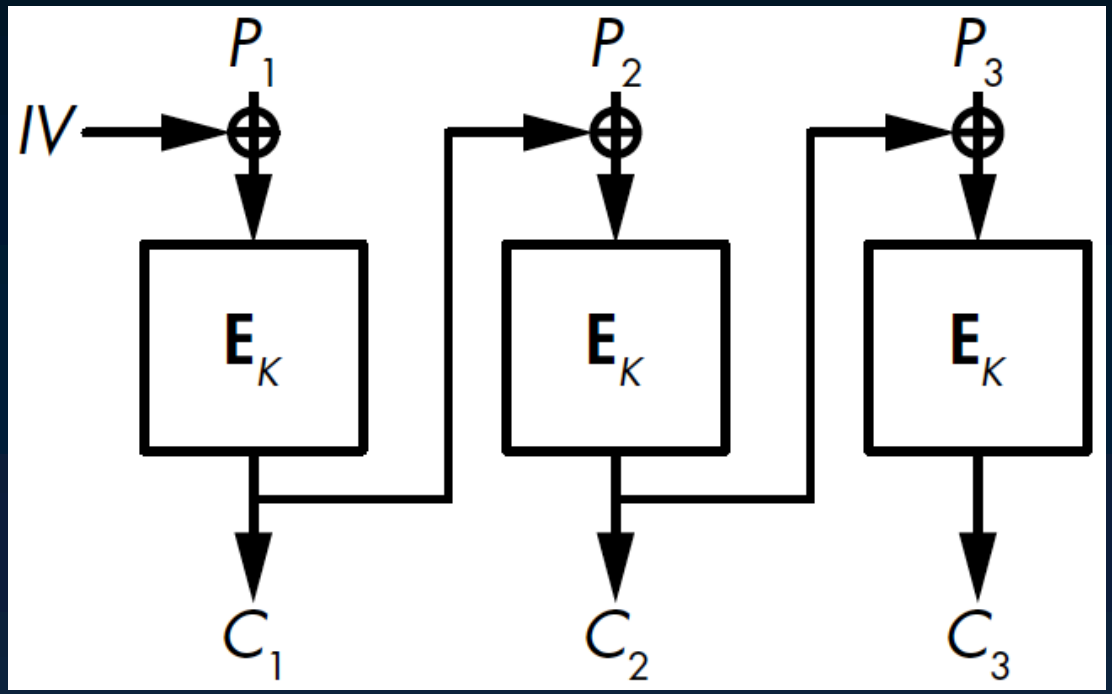


ECB insecurity example



Cipher Block Chaining (CBC) Mode

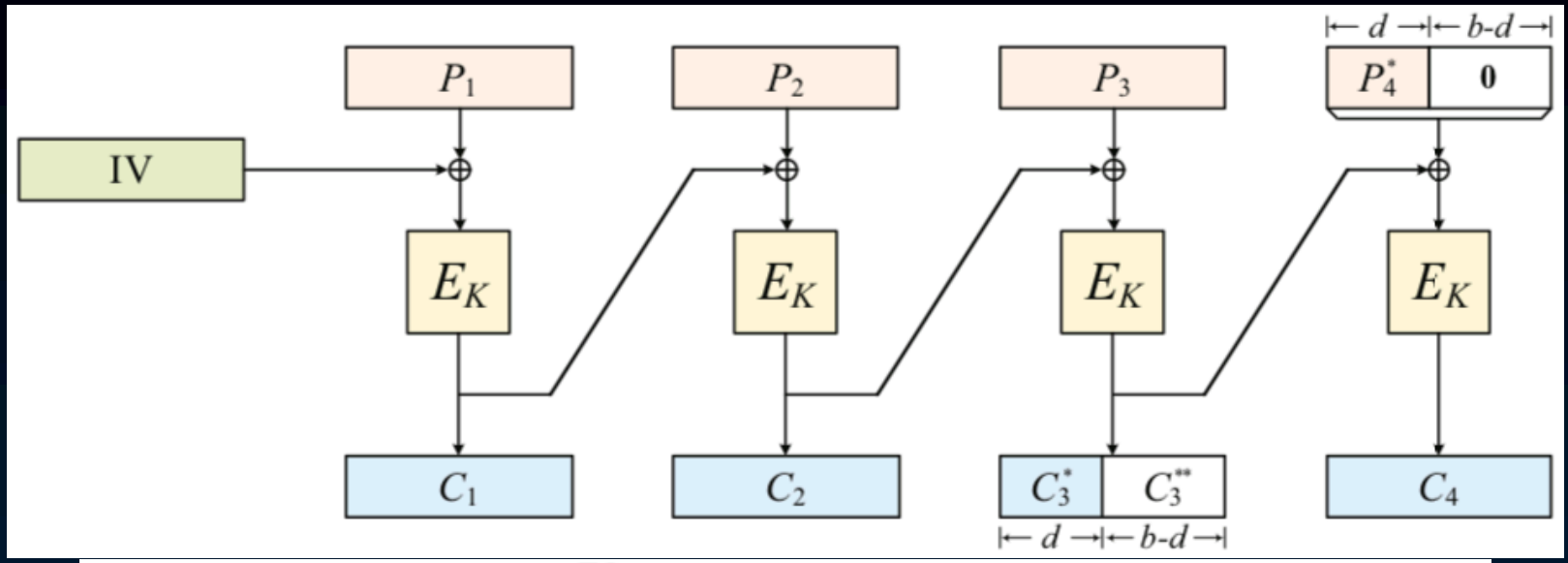
- Needs a random IV (not a secret)
  - Not semantic security otherwise
- Decryption can be parallelized



CBC for any message length

- What if the ptxt is not aligned with 16 byte length?
- Padding (append extra bytes)
  - 01, 02 02, 03 03 03, …, fifteen 0f
  - If ptxt aligns to blocks, pad with sixteen 10
  - Padding oracle attacks
  - ctxt size increases
- Ciphertext stealing
  - No increase in ctxt size

Ciphertext stealing



algorithm $\mathrm{CBC\text{-}CS}_K^{IV}(P)$

$n \leftarrow \lceil |P|/b \rceil$

$P_1 \cdots P_{n-1} P_n^* \leftarrow P$ **where** $|P_1| = \cdots = |P_{n-1}| = b$

$P_n \leftarrow P_n^* \, 0^{b-d}$ **where** $d \leftarrow |P_n^*|$

$C_0 \leftarrow IV;$

$C_1 \cdots C_n \leftarrow \mathrm{CBC}_K^{IV}(P_1 \cdots P_n)$ **where** $|C_1| = \cdots = |C_n| = b$

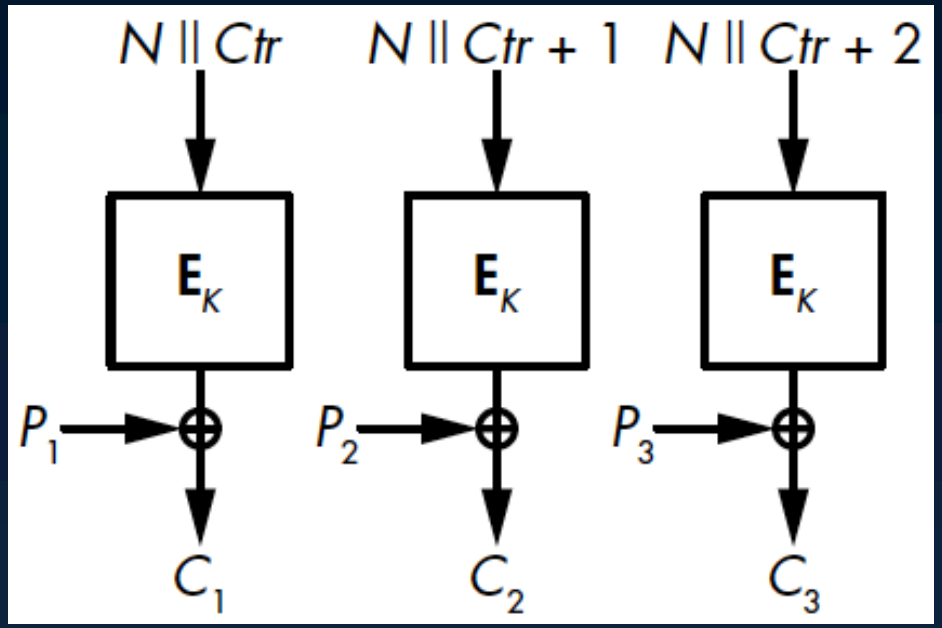
$C_{n-1}^* \leftarrow \mathrm{MSB}_d(C_{n-1})$

return $C_1 \cdots C_{n-2} C_{n-1}^* C_n$

https://link.springer.com/content/pdf/10.1007%2F978-3-642-34047-5_11.pdf

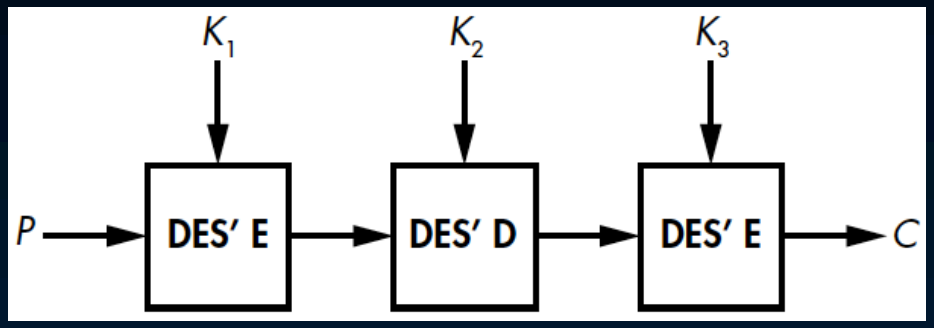
Counter (CTR) Mode

- Unique nonce per message
  - Nonce = number used once (non secret)
- Increase counter for each block
- Parallelizable

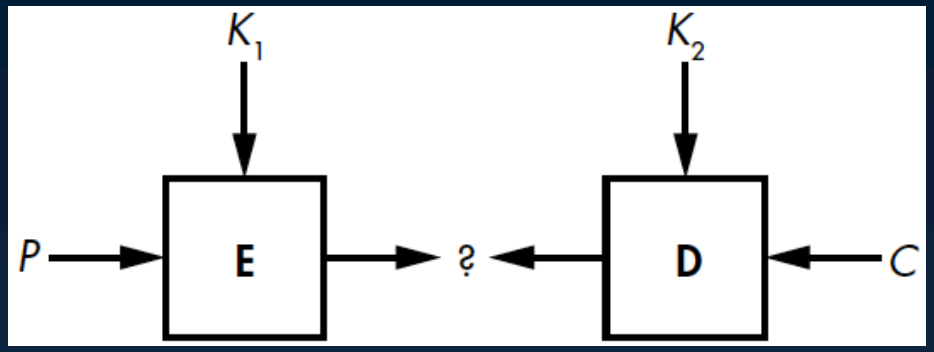


Attacks to Block Ciphers

- Meet-in-the-Middle
  - 112 bits 3DES security for 168 bit keys

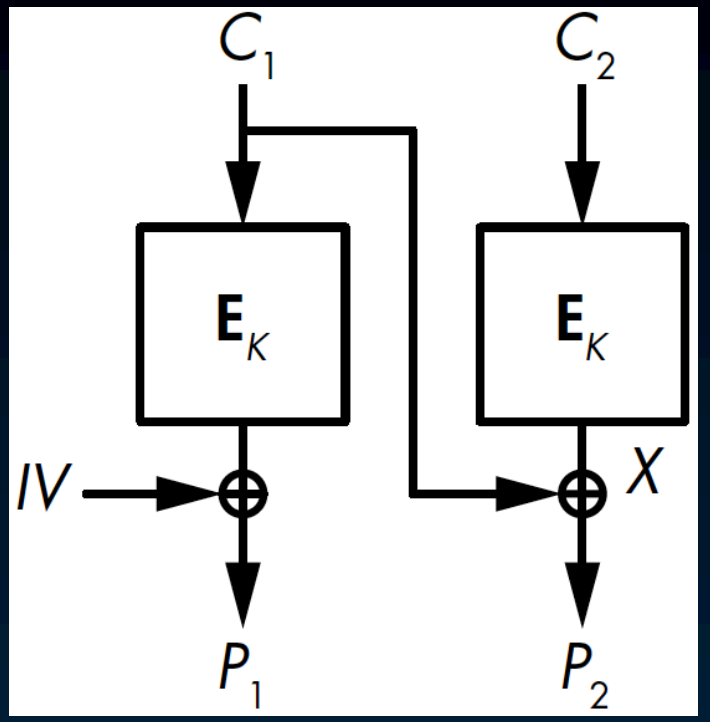


  - 2DES security == DES security (57 bits)
    - Encrypt 2^56 blocks, decrypt <= 2^56 blocks



Padding Oracle Attack

- Goal: Decrypt C2
- Steps:
  - Pick random C1
  - Brute force last byte until padding accepted
    - C1[15] XOR X[15] = 01
    - (Change other bytes of C1)
  - Repeat for other bytes:
    - See how padding 02 02 can be accepted
    - Find X[14] by setting C1[15] = X[15] XOR 02



Reading for next lecture

- Aumasson: Chapter 3

Hands-on exercises

Download tinyurl.com/my-blue-hen

Encrypt it with AES in ECB mode

Save the ciphertext as an image using PIL (Python) or Cimg (C++)

Use AES-CBC to encrypt the same image

Again, save the ctxt as an image

Compare these images; what do you see?