Universidad de Oviedo

Departamento de Informática

Campus de Gijón

Problemas de propagación de errores en Cifradores Simétricos

Presentación

Daniel F. García

Problema: Propagación de errores en CBC

Con el modo ECB (*Electronic Code Book*),
si hay un error en un bloque del texto cifrado transmitido,
solo el bloque de texto plano correspondiente, es afectado.
No obstante, en el modo CBC (*Cipher Block Chaining*) este error se propaga.

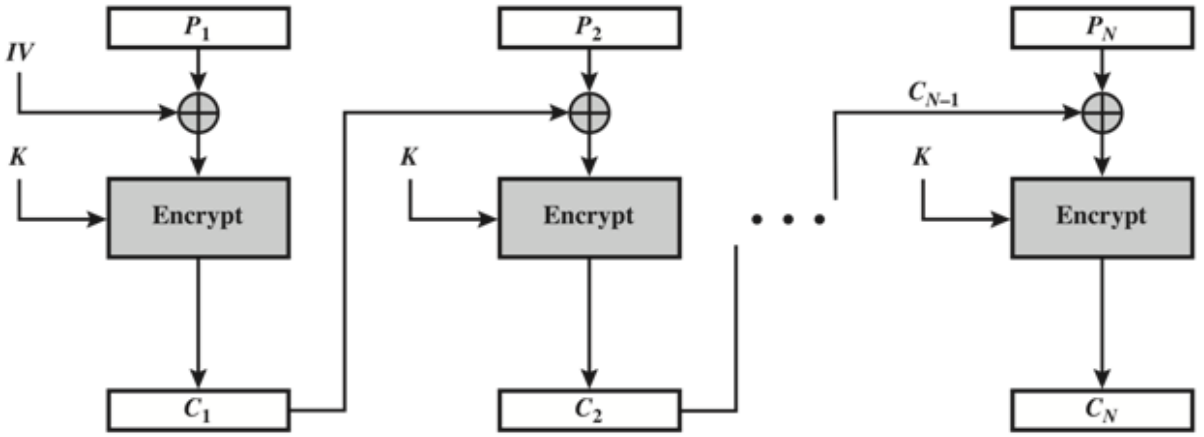
Por ejemplo, un error en el C1 transmitido (generado en el cifrado)
obviamente corrompe a P1 y P2 (generados en el descifrado).

PREGUNTAS:

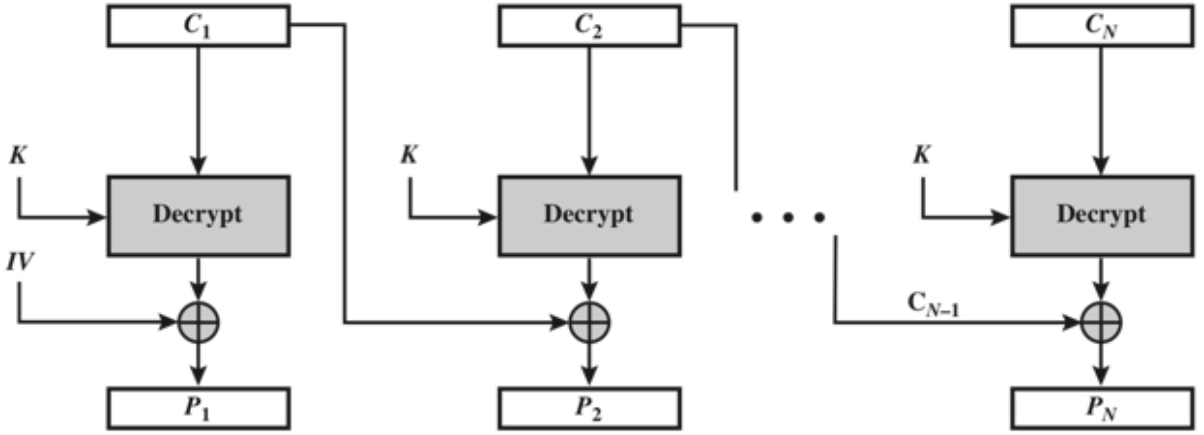
a) ¿Hay algún bloque por encima de P2 afectado?

b) Suponer que hay un error de un bit en el bloque original de P1.
¿A través de cuántos bloques de texto cifrado se propaga este error?
¿Cuál es el efecto en el receptor?

Problema: Propagación de errores en CBC



(a) Encryption



(b) Decryption

Problema: Propagación de errores en OFB

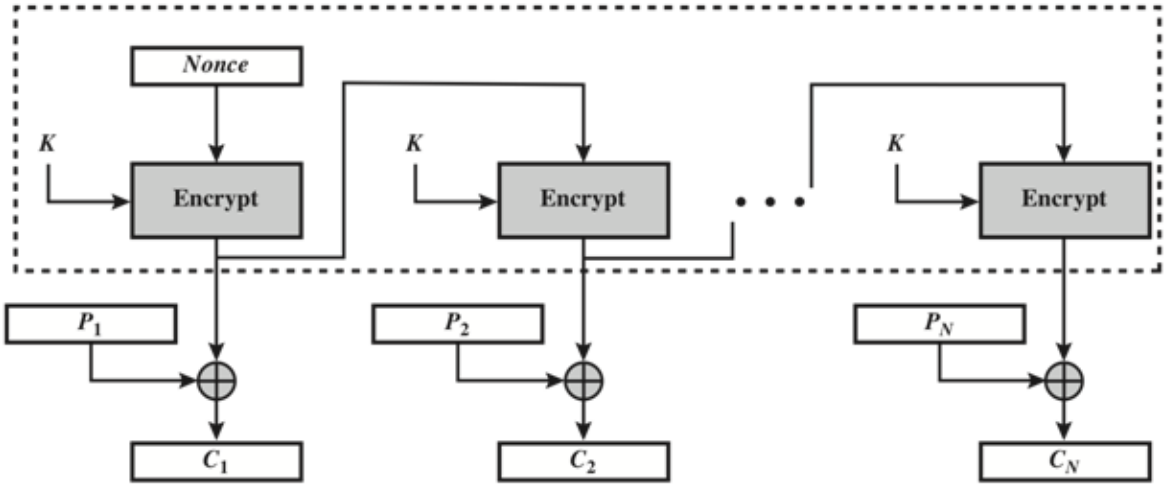
Con el modo ECB (*Electronic Code Book*),
si hay un error en un bloque del texto cifrado transmitido,
solo el bloque de texto plano correspondiente, es afectado.
No obstante, en el modo OFB (*Output Feedback*) …

PREGUNTAS:

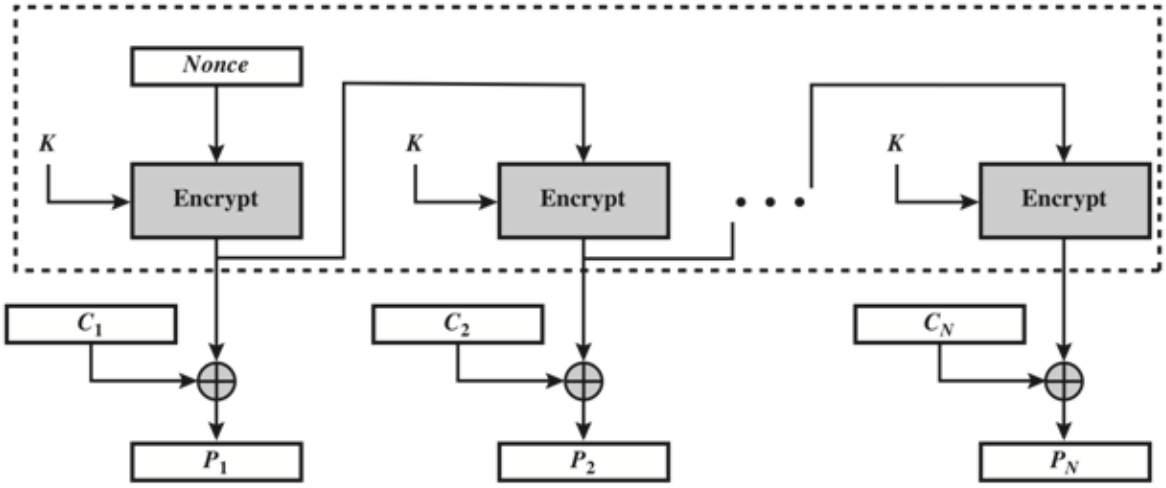
a) Si ocurre un error de un bit en la transmisión de un bloque de texto cifrado en el modo OFB, ¿Hasta dónde se propaga el error?

b) Si se cifra con un vector de inicialización y por error se descifra con un vector de inicialización modificado ¿hasta dónde se propaga el error en el texto plano descifrado?

Problema: Propagación de errores en OFB



(a) Encryption



(b) Decryption

Operación de OFB - Recordatorio

En OFB la serie de bloques de cifrado debe ser la misma para cifrar y para descifrar.
De hecho, no hay descifrador, solo se usa un elemento cifrador.
Para cifrar se usa la operación XOR y para descifrar otra vez la operación XOR.
(Concepto: dos operaciones XOR con la misma máscara dejan la información inalterada)

EJEMPLO:

1010 1011 = AB = Bloque de texto plano

0111 0010 = 72 = Bloque de la serie de cifrado

---------- XOR

1101 1001 = D9 = Bloque de texto cifrado

0111 0010 = 72 = Bloque de la serie de cifrado (idéntico)

---------- XOR

1010 1011 = AB = Bloque de texto plano descifrado