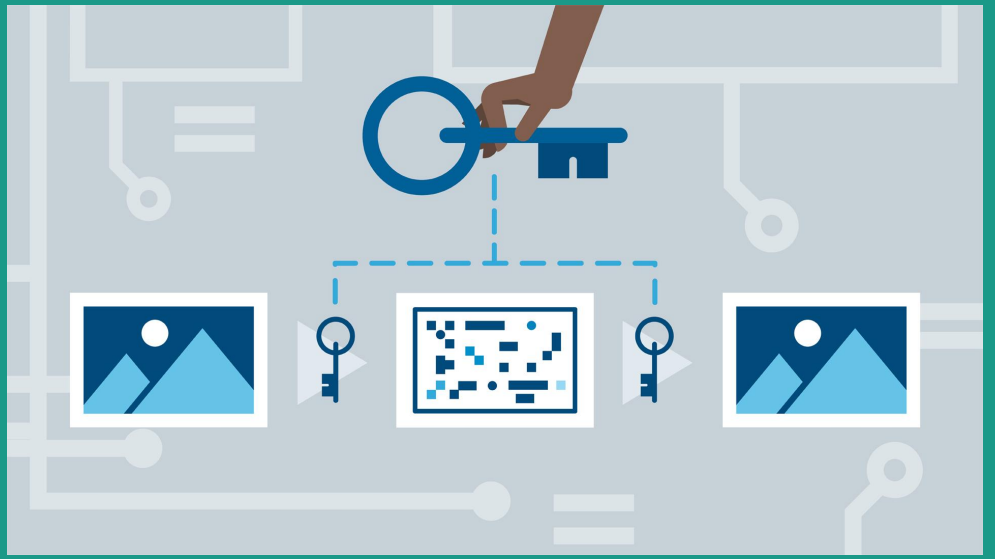
Propagating cipher block chaining (PCBC)

PARTE 1

¿Qué es?

En criptografía, un modo de operación de cifrado en bloque es un algoritmo que utiliza un cifrado en bloque para proporcionar seguridad de la información, como confidencialidad o autenticidad.

Un modo de operación describe cómo aplicar repetidamente la operación de bloque único de un cifrado para transformar de forma segura cantidades de datos mayores que un bloque.



¿Cómo funciona?

Se han definido muchos modos de operación. Algunos de ellos se describen a continuación. El propósito de los modos de cifrado es enmascarar patrones que existen en los datos cifrados, como se ilustra en la descripción de la debilidad del BCE.

Summary of modes

Mode		Formulas	Ciphertext
Electronic codebook	(ECB)	$Y_i = F(\text{PlainText}_i, \text{Key})$	Y_i
Cipher block chaining	(CBC)	$Y_i = \text{PlainText}_i \text{ XOR } \text{Ciphertext}_{i-1}$	$F(Y, \text{Key}); \text{Ciphertext}_0 = IV$
Propagating CBC	(PCBC)	$Y_i = \text{PlainText}_i \text{ XOR } (\text{Ciphertext}_{i-1} \text{ XOR } \text{PlainText}_{i-1})$	$F(Y, \text{Key}); \text{Ciphertext}_0 = IV$
Cipher feedback	(CFB)	$Y_i = \text{Ciphertext}_{i-1}$	$\text{Plaintext XOR } F(Y, \text{Key}); \text{Ciphertext}_0 = IV$
Output feedback	(OFB)	$Y_i = F(Y_{i-1}, \text{Key}); Y_0 = F(IV, \text{Key})$	$\text{Plaintext XOR } Y_i$
Counter	(CTR)	$Y_i = F(IV + g(i), \text{Key}); IV = \text{token}()$	$\text{Plaintext XOR } Y_i$

¿Cómo funciona PCBC?

El modo de encadenamiento de bloques de cifrado de propagación fue diseñado para causar pequeños cambios en el texto cifrado que se propagan indefinidamente al descifrar, así como al cifrar. En el modo PCBC, cada bloque de texto sin formato se XOR con el bloque de texto sin formato anterior y el bloque de texto cifrado anterior antes de encriptarse. Al igual que con el modo CBC, se usa un vector de inicialización en el primer bloque.

Usos del Cipher

PCBC se usa en Kerberos v4 y WASTE, especialmente, pero no es común. En un mensaje cifrado en modo PCBC, si se intercambian dos bloques de texto cifrado adyacentes, esto no afecta el descifrado de los bloques posteriores. Por esta razón, PCBC no se usa en Kerberos v5.

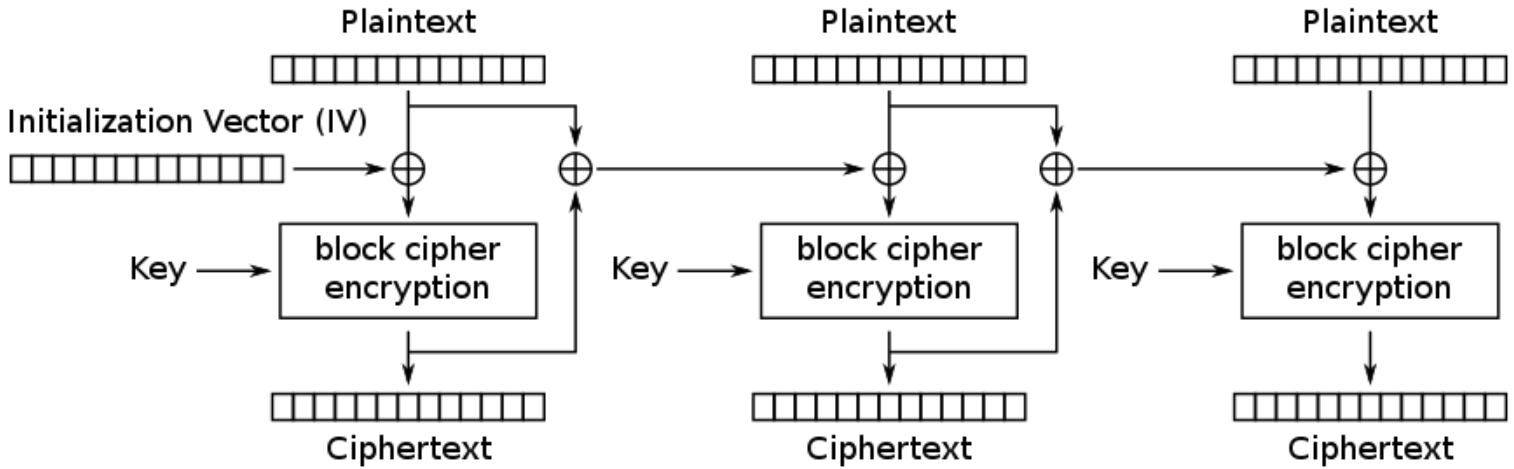
Ventajas y desventajas:

Cifrado paralelizable: No

Descifrado paralelo: No

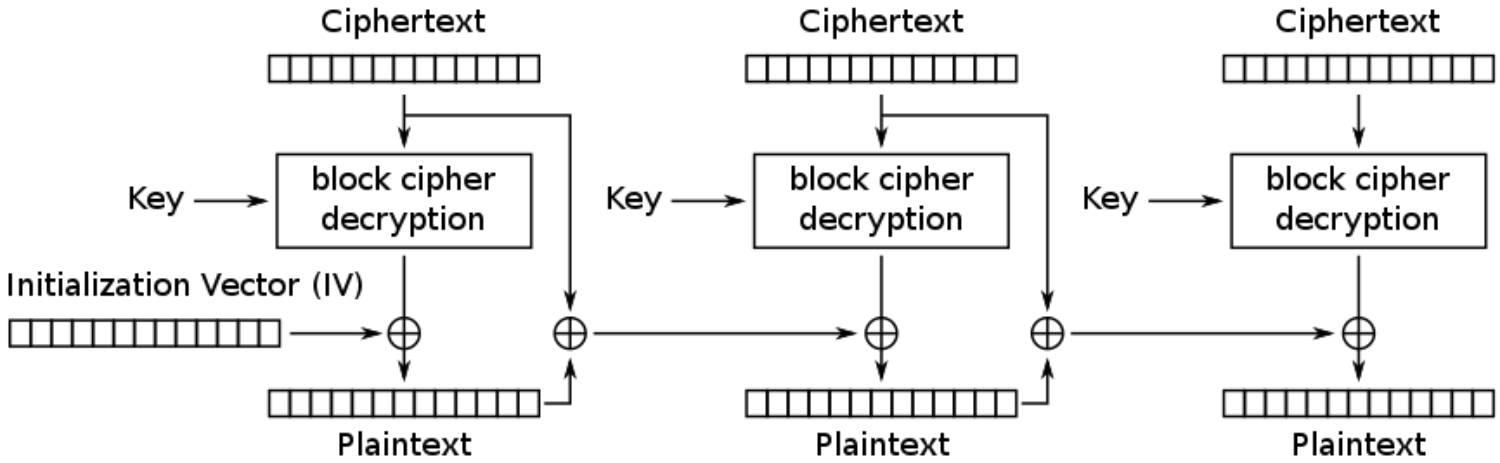
Acceso de lectura aleatorio: No

Diagrama de Funcionamiento: Encripción



Propagating Cipher Block Chaining (PCBC) mode encryption

Diagrama de Funcionamiento: Desencripción



Propagating Cipher Block Chaining (PCBC) mode decryption

Referencias

Huang, Y. L., Leu, F. Y., Liu, J. C., Yang, J. H., Yu, C. W., Chu, C. C., & Yang, C. T. (2013, May). Building a block cipher mode of operation with feedback keys. In 2013 IEEE International Symposium on Industrial Electronics (pp. 1-4). IEEE.

Yu, T., Hartman, S., & Raeburn, K. (2004, February). The Perils of Unauthenticated Encryption: Kerberos Version 4. In NDSS (Vol. 4, pp. 4-4).

Gligor, V. D., & Donescu, P. (1999, April). Integrity-aware PCBC encryption schemes. In International Workshop on Security Protocols (pp. 153-168). Springer, Berlin, Heidelberg.

Gracias.