

Instituto Politécnico Nacional

Escuela Superior de Cómputo

Trabajo terminal

Dra. Sandra Díaz Santiago

Generación de tokens para proteger datos de tarjetas bancarias

Número 20180008

Daniel Ayala Zamorano

Laura Natalia Borbolla Palacios

Ricardo Quezada Figueroa

Enero de 2018

Contenido

1. Introducción	3
1.1. Justificación	4
1.2. Objetivos	4
2. Antecedentes	5
2.1. Introducción a la criptografía	6
2.2. Cifrados por bloques	6
2.3. Cifrados de flujo	6
2.4. Modos de operación	7
2.4.1. <i>Electronic Codebook</i> (ECB)	8
2.4.2. <i>Cipher-block Chaining</i> (CBC)	9
2.4.3. <i>Cipher Feedback</i> (CFE)	9
2.4.4. <i>Output Feedback</i> (OFB)	10
2.5. Funciones hash	10
Bibliografía	12
Lista de figuras	13
Lista de tablas	14
Lista de algoritmos	15

Capítulo 1

Introducción

1.1. Justificación

1.2. Objetivos

Capítulo 2

Antecedentes

2.1. Introducción a la criptografía

2.2. Cifrados por bloques

2.3. Cifrados de flujo

2.4. Modos de operación

Por sí solos, los cifrados por bloques solamente permiten el cifrado y descifrado de bloques de información de tamaño fijo. Para la mayoría de los casos, menos de 256 bits[1], lo cual es equivalente a alrededor de 8 caracteres. Es fácil darse cuenta de que esta restricción no es ningún tema menor: en la gran mayoría de las aplicaciones, la longitud de lo que se quiere ocultar es arbitraria.

Los modos de operación permiten extender la funcionalidad de los cifrados por bloques para poder aplicarlos a información de tamaño irrestricto. Formalizamos este concepto definiendo a un cifrado por bloques como una función C (ecuación 2.1) y a un modo de operación como una función M (ecuación 2.2).

$$C(L, B) \rightarrow Bc \quad (2.1)$$

En donde L es la llave y B es el bloque a cifrar; ambos con un tamaño definido: $L \in \{0, 1\}^k$ (k es el tamaño de la llave) y $B \in \{0, 1\}^n$ (n es el tamaño de bloque). Bc representa al bloque cifrado, el cuál también tiene longitud n .

$$M(L, T) \rightarrow Tc \quad (2.2)$$

En este caso L es la misma que en 2.1, T y Tc son el texto original y el texto cifrado, respectivamente, y ambos son de longitud arbitraria: $T, Tc \in \{0, 1\}^*$.

Un primer enfoque (y quizás el más intuitivo) es partir el mensaje original en bloques del tamaño requerido y después aplicar el algoritmo a cada bloque por separado; en caso de que la longitud del mensaje no sea múltiplo del tamaño de bloque, se puede agregar información extra al último bloque para completar el tamaño requerido. Este es, de hecho, el primero de los modos que presentamos a continuación (*Electronic Codebook*, ECB); su uso no es recomendado, pues es muy inseguro cuando el mensaje original es simétrico a nivel de bloque [1]. También presentamos otros tres modos, los cuales junto con ECB, son los más comunes.

2.4.1. *Electronic Codebook* (ECB)

La figura 2.1 muestra un diagrama esquemático de este modo de operación. Según la ecuación 2.2, el algoritmo recibe a la entrada una llave y un mensaje de longitud arbitraria: la llave se pasa sin ninguna modificación a cada función del cifrado por bloques; el mensaje se debe de partir en bloques ($T = B_1 || B_2 || \dots || B_n$).

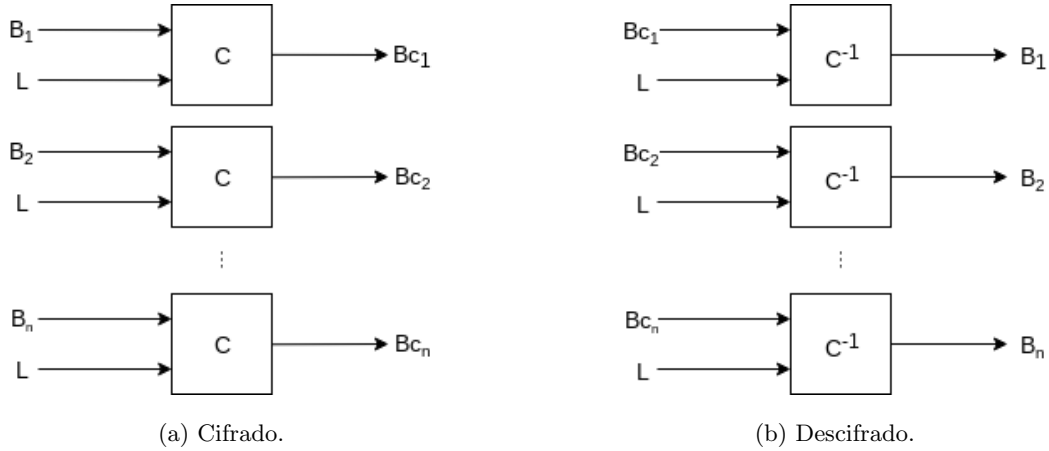


Figura 2.1: Modo de operación ECB.

```

1  entrada: llave  $L$ ; bloques de mensaje  $B_1, B_2 \dots B_n$ .
2  salida: bloques de mensaje cifrado  $Bc_1, Bc_2 \dots Bc_n$ .
3  inicio
4    para_todo  $B$ 
5       $Bc_i \leftarrow C(L, B_i)$ 
6    fin
7    regresar  $Bc$ 
8  fin

```

Algoritmo 2.1: Modo de operación ECB, cifrado.

```

1  entrada: llave  $L$ ; bloques de mensaje cifrado  $Bc_1, Bc_2 \dots Bc_n$ .
2  salida: bloques de mensaje original  $B_1, B_2 \dots B_n$ .
3  inicio
4    para_todo  $Bc$ 
5       $B_i \leftarrow C^{-1}(L, Bc_i)$ 
6    fin
7    regresar  $B$ 
8  fin

```

Algoritmo 2.2: Modo de operación ECB, descifrado.

2.4.2. *Cipher-block Chaining (CBC)*

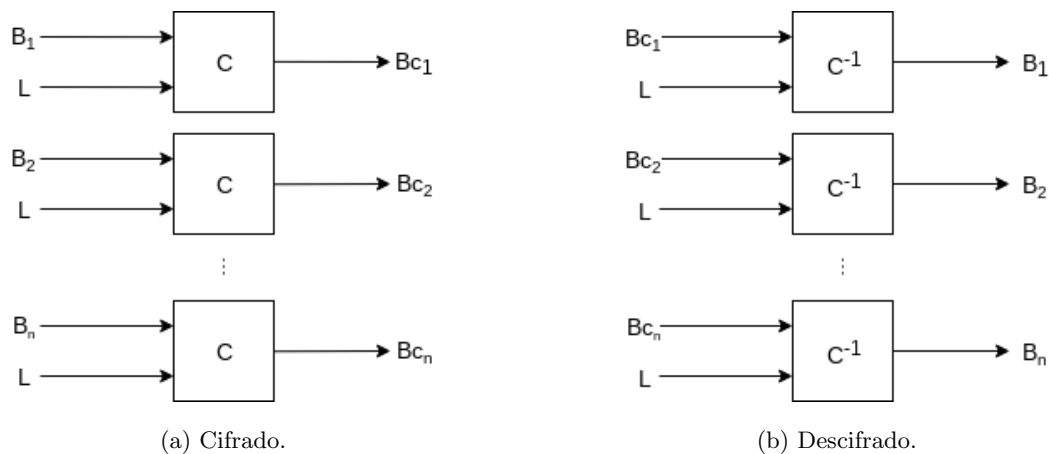


Figura 2.2: Modo de operación ECB.

2.4.3. *Cipher Feedback (CFE)*

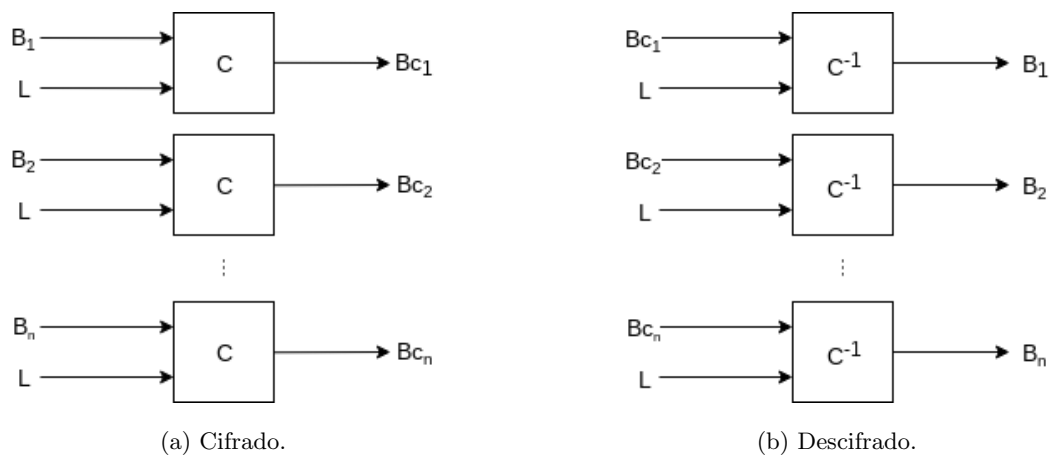


Figura 2.3: Modo de operación ECB.

2.4.4. *Output Feedback* (OFB)

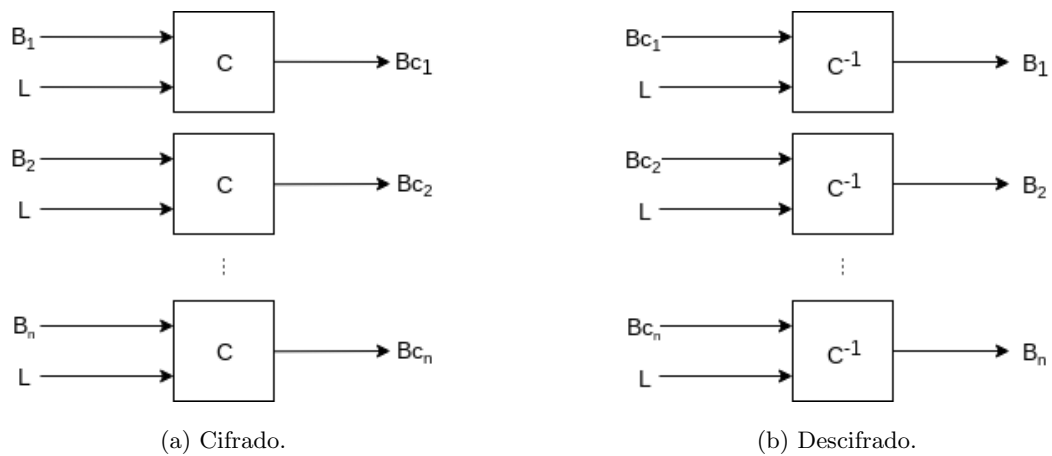


Figura 2.4: Modo de operación ECB.

2.5. Funciones hash

Bibliografía

- [1] Debrup Chakraborty y Francisco Rodríguez-Henríquez. “Block Cipher Modes of Operation from a Hardware Implementation Perspective”. En: *Cryptographic Engineering*. Ed. por Çetin Kaya Koç. Springer, 2009, págs. 321-363. ISBN: 978-0-387-71816-3. DOI: 10.1007/978-0-387-71817-0_12. URL: https://doi.org/10.1007/978-0-387-71817-0_12.

Lista de figuras

2.1. Modo de operación ECB.	8
2.2. Modo de operación ECB.	9
2.3. Modo de operación ECB.	9
2.4. Modo de operación ECB.	10

Lista de tablas

Lista de algoritmos

2.1. Modo de operación ECB, cifrado.	8
2.2. Modo de operación ECB, descifrado.	8