Instituto Politécnico Nacional

Escuela Superior de Cómputo

Trabajo terminal

Dra. Sandra Díaz Santiago

Generación de tokens para protejer datos de tarjetas bancarias

Número 20180008

Daniel Ayala Zamorano
Laura Natalia Borbolla Palacios
Ricardo Quezada Figueroa

Enero de 2018

Contenido

Capítulo 1

Introducción

Justificación

Objetivos

Capítulo 2

Antecedentes

Introducción a la criptografía

La palabra criptografía proviene de las etimologías griegas *Kriptos* (ocultar) y *Graphos* (escritura), y es definida por la Real Academia Española como el arte de escribir con clave secreta o de un modo enigmático. De manera más formal se puede definir a la criptografía como la ciencia encargada de estudiar y diseñar por medio de técnicas matemáticas métodos y modelos capaces de resolver problemas en la seguridad de la información, como la confidencialidad de esta, su integridad y la autenticación de su origen.

Objetivos de la Criptografía

La criptografía tiene como finalidad cumplir los siguientes cuatro servicios.

1. **Confidencialidad**

   Es el servicio encargado de mantener legible la información solo a aquellos que estén autorizados a visualizarla.

2. **Integridad**

   Este servicio se encarga de evitar la alteración de la información de forma no autorizada, esto incluye la inserción, sustitución y eliminación de los datos.

3. **Autenticación**

   Este servicio se refiere a la identificación tanto de las personas que establece una comunicación, garantizando que cada una es quien dice ser; como del origen de la información que se maneja, garantizando la veracidad de la hora y fecha de origen, el contenido, tiempos de envió, entre otros.

4. **No repudio**

   Es el servicio que evita que el autor de la información o de alguna acción determinada, pueda negar su validez, ayudando así a prevenir situaciones de disputa.

Criptoanálisis y Ataques

La criptografía forma parte de una ciencia más general llamada criptología, la cual tiene otras ramas de estudio, como es el criptoanálisis, que es la ciencia encargada de estudiar los posibles ataques a sistemas criptográficos, que son capaces de contrariar sus servicios ofrecidos. Los ataques que realizan a sistemas criptográficos dependen de la cantidad de recursos o conocimientos con los que cuenta el adversario que realiza dicho ataque, dando así a la siguiente clasificación.

1. **Ciphertext-only attack**

En este ataque el adversario solo es capaz de obtener la información cifrado, y tratara de conocer su contenido en claro a partir de ella. Esta forma de atacar es la más básica, y todos los métodos criptográficos deben poder soportarla.

2. **Known-plaintext attack**

   Esta clase de ataques ocurren cuando el adversario puede obtener pares de información cifrada y su correspondiente información en claro, y por medio de su estudio, trata de descifrar otra información cifrada para la cual no conoce su contenido.

3. **Chosen-plaintext attack**

   Este ataque es muy parecido al anterior, con la diferencia de que en este el adversario es capaz de obtener los pares de información cifrada y en claro con el contenido que desee.

4. **Adaptively-chosen-plaintext attack**

   En este ataque el adversario es capaz de obtener los pares de información cifrada y en claro con el contenido que desee y además tiene amplio acceso o puede usar de forma repetitiva el mecanismo de encriptación.

5. **Chosen and adaptively-chosen-ciphertext attack** En este caso el adversario puede elegir información cifrada y conocer su contenido, dado que tiene acceso a los mecanismos de descifrado.

Cifrados por bloques

Cifrados de flujo

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**modos˙de˙operacion** 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).

$$C(L, B) \rightarrow Bc \tag{2.1}$$

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.

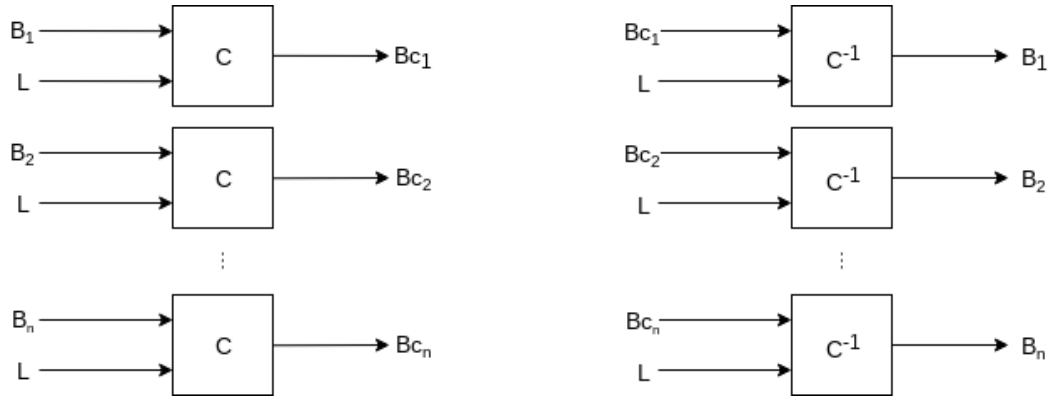
$$M(L, T) \rightarrow Tc \tag{2.2}$$

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 **modos˙de˙operacion** También presentamos otros tres modos, los cuales junto con ECB, son los más comunes.

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 ($T = B_1||B_2||\ldots||B_n$).



(a) Cifrado. (b) Descifrado.

Figura 2.1: Modo de operación ECB.

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

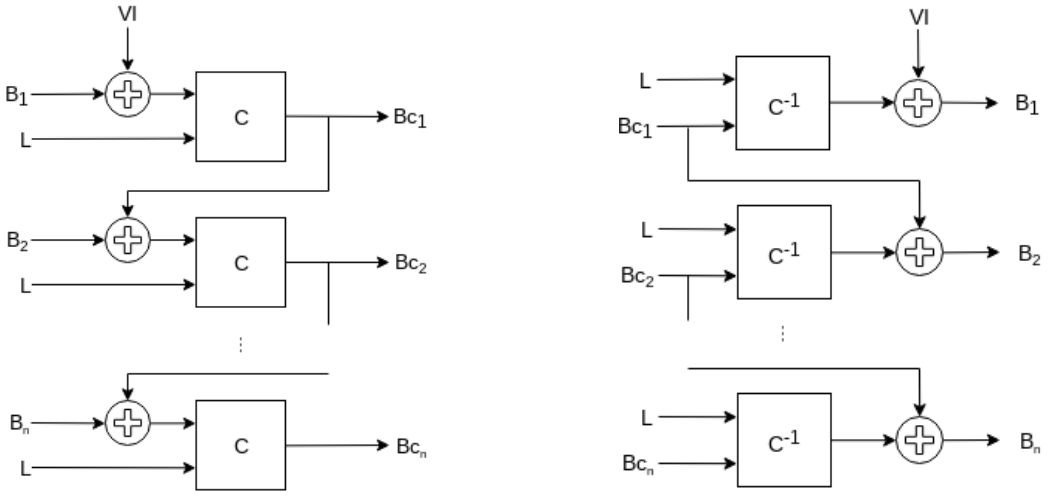
Pseudocódigo 2.1: Modo de operación ECB, cifrado.

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

Pseudocódigo 2.2: Modo de operación ECB, descifrado.

Cipher-block Chaining (CBC)

En CBC la salida del bloque cifrador uno se introduce (junto con el siguiente bloque del mensaje) en el bloque cifrador dos, y así en sucesivo. Para poder replicar este comportamiento en todos los bloque cifradores, este modo de operación necesita un argumento extra a la entrada: un vector de inicialización. De esta manera la salida del bloque i depende de todos los bloques anteriores; esto incrementa la seguridad con respecto a ECB.



(a) Cifrado. (b) Descifrado.

Figura 2.2: Modo de operación CBC.

En la figura 2.2 se muestran los diagramas esquemáticos para cifrar y descifrar; en los pseudocódigos 2.3 y 2.4 se muestran unos de los posibles algoritmos a seguir. Es importante notar que mientras que el proceso de cifrado debe ser forzosamente secuencial (por la dependencias entre salidas), el proceso de descifrado puede ser ejecutado en paralelo.

```
1   entrada: llave L; vector de inicialización VI;
2            bloques de mensaje B_1, B_2 ... B_n.
3    salida: bloques de mensaje cifrado Bc_1, Bc_2 ... Bc_n.
4   inicio
5     Bc_0 ← VI                    // El vector de incialización
6     para_todo B                  // entra al primer bloque.
7       Bc_i ← C(L, B_i ⊕ Bc_{i-1})
8     fin
9     regresar Bc
10  fin
```

Pseudocódigo 2.3: Modo de operación CBC, cifrado.

```
1  entrada: llave L; vector de inicialización VI;
2           bloques de mensaje cifrado Bc_1, Bc_2 ... Bc_n.
3   salida: bloques de mensaje original B_1, B_2 ... B_n.
4  inicio
5    Bc_0 ← VI
6    para_todo Bc
7      B_i ← C^{-1}(L, Bc_i) ⊕ Bc_{i-1}
8    fin
9    regresar B
10 fin
```

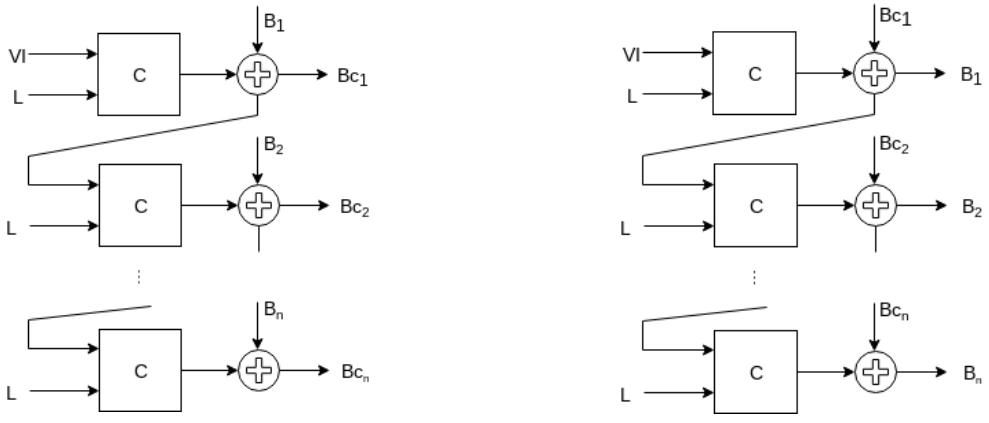
Pseudocódigo 2.4: Modo de operación CBC, descifrado.

Cipher Feedback (CFB)

Al igual que la operación de cifrado de CBC, ambas operaciones de CFB (cifrado y descifrado) están encadenadas bloque a bloque, por lo que son de naturaleza secuencial. En este caso, lo que se cifra en el primer paso es el vector de inicialización; la salida de esto se opera con un `xor` sobre el primer bloque de texto en claro, para obtener el primer bloque cifrado (figura 2.3).

Esta distribución presenta varias ventajas con respecto a CBC: las operaciones de cifrado y descifrado son sumamente similares, lo que permite ser implementadas por un solo algoritmo (pseudocódigo 2.5); tanto para cifrar como para descifrar solamente se ocupa la operación de cifrado del algoritmo a bloques subyacente. Estas ventajas se deben principalmente a las propiedades de la operación `xor` (ecuación 2.3).

$$A \oplus B = C \quad \Rightarrow \quad A = B \oplus C \tag{2.3}$$



(a) Cifrado. (b) Descifrado.

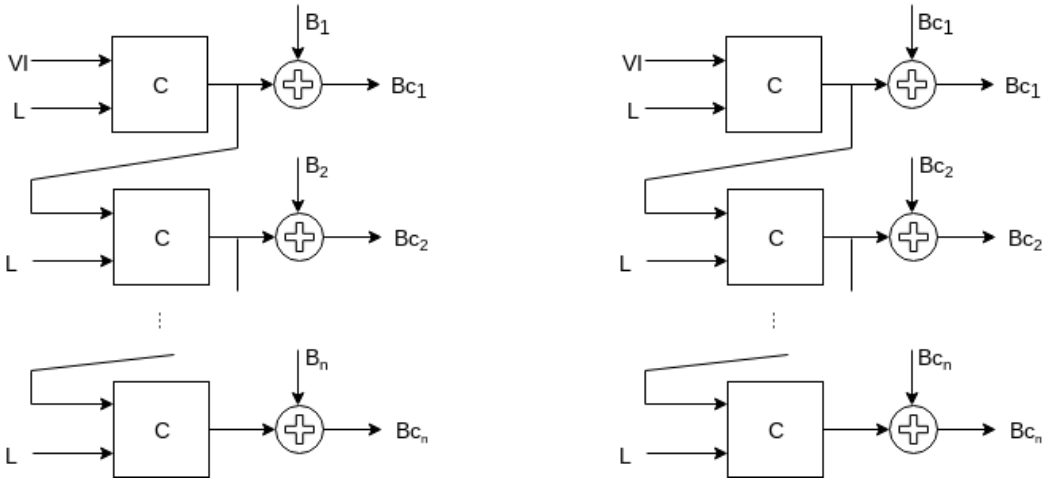
Figura 2.3: Modo de operación CFB.

```
1  entrada: llave L; vector de inicialización VI;
2           bloques de mensaje (cifrado o descifrado) B_1, B_2 ... B_n.
3   salida: bloques de mensaje (cifrado o descifrado) Bc_1, Bc_2 ... Bc_n.
4  inicio
5    Bc_0 ← VI
6    para_todo B
7      Bc_i ← C(L, Bc_{i-1}) ⊕ B_i
8    fin
9    regresar Bc
10 fin
```

Pseudocódigo 2.5: Modo de operación CFB (cifrado y descifrado).

Output Feedback (OFB)

Este es muy similar al anterior (CFB), salvo porque la retroalimentación va directamente de la salida del cifrador a bloques. De esta forma, nada que tenga que ver con el texto en claro, llega al cifrado a bloques; este solamente se la pasa cifrando una y otra vez el vector de inicialización.



(a) Cifrado.

(b) Descifrado.

Figura 2.4: Modo de operación OFB.

```
1  entrada: llave L; vector de inicialización VI;
2           bloques de mensaje (cifrado o descifrado) B_1, B_2 ... B_n.
3   salida: bloques de mensaje (cifrado o descifrado) Bc_1, Bc_2 ... Bc_n.
4  inicio
5    aux ← VI
6    para_todo B
7      aux ← C(L, aux)
8      Bc_i ← aux ⊕ B_i
9    fin
10   regresar Bc
11 fin
```

Pseudocódigo 2.6: Modo de operación OFB (cifrado y descifrado).

Funciones hash

Lista de figuras

Lista de tablas

Lista de pseudocódigos