# CRIPTOGRAFÍA USADA EN LA REVOLUCIÓN MEXICANA

José de Jesús Angel Angel
Guillermo Morales-Luna
CINVESTAV-Instituto Politécnico Nacional

## *Antecedentes de la criptografía en México*

Aparentemente antes de la Conquista Española en México, las diversas formas de escritura, jeroglífica y pictórica, eran muy limitadas socialmente, por lo que no hay evidencia de la necesidad de ocultar información en esa época.

Luego de la Conquista, la Historia de México cambió bruscamente: la lengua española y su escritura se establecieron como elementos nacionales. Fue precisamente en la década posterior a la Conquista, que Hernán Cortés escribe cartas cifradas, conservadas en la actualidad en el Archivo de Indias en Sevilla, y éstas son los primeros textos cifrados en el continente americano. Posteriormente fue común la comunicación cifrada entre funcionarios de la Corona Española y los gobernantes en la Nueva España.

Tras la independencia, en 1821, hubo un largo periodo en México de conflictos políticos que dieron lugar a enfrentamientos armados. Suponemos que en medios militares educados en el antiguo Ejército Realista se utilizó alguna forma de criptografía, como era común en varios ejércitos sudamericanos, sin embargo no hemos encontrado evidencia de ello. Fue hasta le época de Benito Juárez que, ya habiéndose inventado el telégrafo, creció de manera considerable el uso de la criptografía incorporada a las comunicaciones por telegramas. Como es el caso del propio Don Benito Juárez que mantuvo una constante comunicación cifrada con Don Ignacio L. Vallarta, gobernador de Jalisco, usando un sistema de substitución simple [3].

## *La criptografía de Porfirio Díaz*

Porfirio Díaz, militar de profesión, asumió la Presidencia de México en 1876, su primer periodo terminó en 1880, su segundo periodo como presidente inició en 1984 y concluyó con su renuncia en mayo de 1911.

Don Porfirio Díaz usó de manera intensa los sistemas criptográficos para comunicarse con gobernadores y jefes militares importantes. Fue su secretario particular, Don Rafael Chousal, el encargado de "seleccionar" los métodos criptográficos particulares utilizados. A lo largo de toda su estadía en el poder, Díaz usó de manera estable las técnicas y las claves fijadas con sus corresponsales y no se sabe que hayan sido comprometidas sus comunicaciones de manera importante. Gracias a que hoy en día se conserva de manera extraordinaria su archivo personal [1], se puede conocer con exactitud los métodos criptográficos empleados. La siguiente tabla ilustra el método de substitución simple que Díaz. Esa clave la usó con I. Bravo, uno de sus más importantes jefes militares en el sur del país [2].

**Tabla 1**

Clave de sustitución correspondiente al General Ignacio A. Bravo.

| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **0** |
|---|---|---|---|---|---|---|---|---|---|---|
| **1,2,3** | a | u | i | l | rr | o | h | g | e | c |
| **4,5,6** | | x | r | | | q | j | d | p | ll |
| **7,8,9** | ch | s | z | t | n | y | v | m | b | |

La tabla anterior sintetiza un método criptográfico de substitución simple, es decir, asocia un número a cada letra del mensaje abierto. En este caso por ejemplo al mensaje "LEVANTAMIENTO" se le asocia el texto cifrado "24, 39, 77, 11, 95, 84, 21, 78, 33, 29, 75, 94, 16". A cada letra se le puede asociar hasta tres números posibles, por ejemplo a la letra "A" se le pueden asociar los números "11, 21, 31", tomado el primer dígito a elegir de los números que están en la primera fila {1,2,3}, el segundo dígito es el número de la columna {1}. A la letra "M", se le pueden asociar los números "78, 88, 98" , tomado el primer dígito a elegir de los números que están en la primera fila {7,8,9}, el segundo dígito es el número de la columna {8}.

**Tabla 2**

Ejemplo para cifrar las letras "a" y "m".

| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **0** |
|---|---|---|---|---|---|---|---|---|---|---|
| **1,2,3** | a | u | i | l | rr | o | h | g | e | c |
| **4,5,6** | | x | r | | | q | j | d | p | ll |
| **7,8,9** | ch | s | z | t | n | y | v | m | b | |

En el caso del descifrado se procede de manera inversa, es decir, si se quiere descifrar el mensaje "24, 39, 77, 11, 95, 84, 21, 78, 33, 29, 75, 94, 16", el primer dígito conduce a la fila donde aparece ese dígito, el segundo dígito nos conduce a la columna. Así, por ejemplo, el texto cifrado "24, 39" se descifra como "LE".

**Tabla 3:**

Ejemplo para descifrar los textos "24" y "39".

| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **0** |
|---|---|---|---|---|---|---|---|---|---|---|
| **1,2,3** | a | u | i | l | rr | o | h | g | e | c |
| **4,5,6** | | x | r | | | q | j | d | p | ll |
| **7,8,9** | ch | s | z | t | n | y | v | m | b | |

*Criptografía de F.I. Madero*

Tiempo después, Don Francisco I. Madero usó sistemas criptográficos de substitución simple también, de diferentes tipos, algunos muy similares a los de Díaz, sólo que se reemplazaba letras por otras letras en lugar de números. Por ejemplo la siguiente clave fue utilizada entre Madero y Pino Suárez [3]:

**Tabla 4**

Clave de sustitución correspondiente Pino Suárez.

| | **M** | **A** | **R** | **B** | **O** | **R** | **I** | **L** | **E** |
|---|---|---|---|---|---|---|---|---|---|
| **J** | a | b | c | d | e | f | g | h | i |
| **R** | j | k | l | m | n | ñ | o | p | q |
| **B** | r | s | t | u | v | w | x | y | z |

Entonces el mensaje: "Congreso Nacional" queda "Jrrirojibmjobari Rojmjrjerirojmrr".

El proceso de cifrado es el mismo que el método de Díaz, y se asocia a cada letra un par de letras, donde la primera corresponde a fila donde se encuentra el texto original y la segunda letra corresponde a la columna.

**Tabla 5**

Ejemplo para cifrar la letra "C".

| | **M** | **A** | **R** | **B** | **O** | **R** | **I** | **L** | **E** |
|---|---|---|---|---|---|---|---|---|---|
| **J** | a | b | c | d | e | f | g | h | i |
| **R** | j | k | l | m | n | ñ | o | p | q |
| **B** | r | s | t | u | v | w | x | y | z |

Por lo tanto a la letra "C", le corresponde el texto cifrado "JR".

*Criptografía de los Constitucionalistas*

Los años más duros de la guerra estaban aún por venir. En 1913 Huerta dio un golpe de estado contra el presidente Madero, quien junto con su vicepresidente José María Pino Suárez, es asesinado. Varios sectores de la sociedad, incluso algunos porfiristas, se levantaron en armas contra el usurpador Huerta. Venustiano Carranza, otro personaje importante en la Revolución Mexicana, usó también mensajes cifrados. Para

esta etapa avanzada de la guerra, era de suponerse que los sistemas anteriores evolucionaran. Carranza y sus jefes principales usaron diferentes tipos de sistemas, varios de substitución simple como los anteriores. Sin embargo hay evidencia de que varios jefes revolucionarios, incluso Francisco Villa, usaron un sistema que combinaba la idea anterior para asignar diferentes claves.

El sistema llamado "*Mexican Army Cipher Disk*"[6][7], una de cuyas claves se muestra en la siguiente tabla, fue conocida por el ejército norteamericano ya que fue interceptado, es el sistema criptográfico mexicano más conocido. El telegrama interceptado fue uno entre Treviño y Obregón fechado en noviembre de 1916. El sistema es una combinación entre los usados en la época de Díaz y Madero con el típico sistema Julio César de desplazamiento.

**Tabla 6**

Método de Julio César

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 00 | 01 | 02 |

El método de Julio César consiste en sustituir las letras del alfabeto con números del 00 al 25. Posteriormente sumar 3 a cada número correspondiente, si el número correspondiente es menor a 23, y restar 23 si el número correspondiente es menor o igual a 23, por lo tanto el texto cifrado queda como lo mostrado en la figura 6. De manera formal, si x representa el número asociado a cada letra al inicio, el texto cifrado esta dado por la fórmula $f(x)=x+3 \bmod 26$.

**Enseguida describimos el** "*Mexican Army Cipher Disk*"

**1.- Elementos del sistema.** Se consideran la siguiente tabla 7 de 5 filas, como lo muestra la tabla 7. La primera fila corresponde al alfabeto de 26 letras, la segunda fila corresponde a los números ordenados del 01 al 26, de acuerdo a la fórmula queda como $f(x)=(x+b_1 \bmod 26)+1$, donde $b_1$ en este caso es 23. La tercera columna consiste de los números ordenados del 27 al 52, de acuerdo a la fórmula es $f(x)=(x+b_2 \bmod 26)+27$. La cuarta columna de manera similar corresponde a los números ordenados del

53 al 78, o con la fórmula a $f(x)=(x+b_3 \text{ mod } 26)+53$. Finalmente la quinta columna corresponde sólo de los números del 79 al 99, con la fórmula $f(x)=(x+b_4 \text{ mod } 26)+79$.

**2.- La clave del sistema.** La clave del sistema consiste de los números ($b_1$ $b_2$ $b_3$ $b_4$), que sin embargo de manera más simple es también la letra donde inicia la numeración correspondiente a cada fila, por ejemplo en la tabla 5, la clave es "DMWG", este ejemplo es tomado de [6]. El manejo de las claves se llevaba de diferentes maneras. La forma más común era por medio de un "Code Book", es decir un cuaderno de claves que previamente se acordaba y que sólo ambos lados de la comunicación conocían. Por ejemplo en un telegrama mostrado en [7], se dice como clave "EN LA G". Entonces el receptor del telegrama revisaba su "Code Book" y obtenía de ahí la clave correspondiente a la "palabra clave" EN LA G, que era "AWIO".

**3.- Método de cifrado.** Una vez que se tiene la tabla de alfabetos, a partir de la clave se procede a cifrar el mensaje. Por ejemplo el mensaje "AVANCE" queda cifrado como "57 19 99 11 59 02" como corresponde a la tabla 7.

**4.- Método de descifrado.** Con el mensaje cifrado simplemente hay que obtener la letra de la tabla la letra correspondiente y así obtener el mensaje descifrado.

**Tabla 7**

*Mexican Army Cipher Disk*.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 |
| 4 | 5 | 6 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 |
| 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 2 | 2 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 4 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
| 5 | 5 | 5 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 6 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 5 | 5 | 5 | 5 |
| 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 3 | 4 | 5 | 6 |
| 9 | | | | | | 7 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 | 9 |
| 9 | | | | | | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

*Conclusiones*

Una de las etapas donde mayormente se usó criptografía en México fue precisamente la Revolución Mexicana. Debido a lo estratégico de la información que se usaba se considero usar métodos que permitieran dar confidencialidad a la información.

Los métodos usados en su mayoría, fueron simples pero aparentemente resultaron suficientemente seguros para los contendientes de la época. Los métodos de Días y Madero se basaban en ideas muy conocidas en el mundo, que data del año 100 A.C. dadas por el Griego Polybius. Que sin embargo fue siendo adaptado para evitar ataques conocidos. Hasta le fecha no se conoce documento alguno donde se muestre claramente que un sistema de este tipo fue comprometido.

Por otra parte del sistema Mexican Army Cipher Disk se sabe que fue criptoanalizado por criptoanalistas Norteamaericanos [5].

Aparentemente se sabe también que varios contendientes de la Revolución Mexicana usaban sistemas más fuertes principalmente cuando se comunicaban con sus agentes en Estados Unidos, estos sistemas consistían de sustituciones simples únicas.

## *BIBLIOGRAFÍA*

Acervo Histórico de Porfirio Díaz "*Telegramas de Porfirio Díaz,"* Biblioteca: Francisco Xavier Clavijero, Universidad Iberoamericana, campus Santa Fe, México, D. F.

ANGEL, Jesús y Morales L. Guillermo**,** "Algunos Sistemas Criptográficos durante la Presidencia de Porfirio Díaz", *CINVESTAV* , Noviembre, 2007.

ANGEL, Jesús y Morales L. Guillermo**,** *La Historia de la Criptografía en México*, en preparación México: *CINVESTAV*, Noviembre, 2007.

Colección Francisco I. Madero, "*Biblioteca del Recinto Juárez*", Palacio Nacional, Mexico, D.F.

HITT, Parker., *Manual For The Solution Of Military Ciphers.* USA: Aegean Park Press, 1976.

KAHN, David, *The Codebreakers - The Story of Secret Writing.* USA: The Macmillan Co, 1967.

National Security Agency. *NSA reveals how codes of Mexico were broken*. USA: Aegean Park Press, Ca., 2000.