Revista Digital Universitaria
10 de marzo 2008 • Volumen 9 Número 3 • ISSN: 1067-6079

ARTICULO

BREVE DESCRIPCIÓN DE LA CRIPTOGRAFÍA EN LA REVOLUCIÓN MEXICANA

José de Jesús Ángel Ángel y Guillermo Morales-Luna
Departamento de Computación, CINVESTAV-IPN, México
jjangel@computacion.cs.cinvestav.mx, gmorales@cs.cinvestav.mx

10 de marzo 2008 • Volumen 9 Número 3 • ISSN: 1067-6079

Resumen:

En este artículo describimos algunos métodos criptográficos usados durante la Revolución Mexicana. Movimiento bélico, donde de manera natural nació y creció el uso de técnicas estratégicas comúnmente utilizadas en la guerra, tal es el caso de la criptografía. El propósito principal de este artículo es hacer una breve reseña de los métodos criptográficos de esa época en México. Hoy en día las evidencias muestran que fueron diseñados al calor de la contienda por militares mexicanos.

Palabras clave: Revolución mexicana, criptografía, ejército mexicano.

Abstrac:

In this paper we describe some cryptographic methods that were used during the Mexican Revolution. Movement war, which will naturally born and grew strategic use of techniques commonly used in the war, as in the case of cryptography. The main purpose of this article is to make a brief statement about the cryptographic methods of that time in Mexico. Today, the evidence shows that were designed in the heat of the struggle for Mexican military.

Keywords: Mexican Revolution, cryptography, Mexican army.

http://www.revista.unam.mx/vol.9/num3/art18/int18.htm

INTRODUCCIÓN

La Revolución Mexicana es una etapa de estudio obligado para todo mexicano, sobre ella hay una gran cantidad de libros, estudios y artículos que dan versiones diversas de este acontecer. Las hay de todo tipo, obviamente de acuerdo con quien las escribe. No es nuestro propósito dar una más, sin embargo algunos relatos claramente tienen una inclinación de la interpretación personal de sus autores. Los personajes importantes de la Revolución Mexicana están claramente distinguidos hasta 1913, entre revolucionarios y seguidores del viejo régimen.

Después de la derrota de Victoriano Huerta los bandos se fragmentan en una situación muy confusa, incluso para los propios historiadores. Antes de 1914, Porfirio Díaz y Victoriano Huerta eran los representantes más destacados del viejo régimen y los caudillos revolucionarios eran Francisco I. Madero, Francisco Villa, Emiliano Zapata, Venustiano Carranza y Álvaro Obregón, entre otros. Después de la derrota de Huerta (junio de 1914-) la Revolución Mexicana toma un carácter más de guerra civil, y los principales bandos encontrados son los convencionalistas y los carrancistas. Para muchos, tras la muerte de Zapata y la desaparición de la Convención Revolucionaria, terminó el sueño de la Revolución Mexicana, mientras que para otros queda triunfante con la Constitución de 1917.

En el lustro de 1912 a 1917 creció la necesidad de usar técnicas estratégicas para triunfos militares. El objetivo claro de la criptografía en ese lapso fue dotar de métodos que permitieran la comunicación segura. En caso que fuese interceptada no debería ser comprensible. En esta breve descripción de los métodos criptográficos usados en la Revolución pretendemos dar a conocer una parte de la historia técnica de México. Aunque quizá los métodos no hayan sido muy sofisticados, tienen una importancia histórica evidente.

En la sección primera relatamos algunos antecedentes de la criptografía en México, desde el S. XVI a mediados del XIX; en la segunda mencionamos los sistemas criptográficos usados por Porfirio Díaz; en la tercera, los usados por Francisco I. Madero; la cuarta describe la criptografía utilizada por el Ejército Constitucionalista (a las órdenes de Venustiano Carranza), finalmente en la quinta sección formulamos algunas conclusiones.

Antecedentes de la criptografía en México

Aparentemente antes de la Conquista española en México, las diversas formas de escritura, jeroglífica y pictográfica eran muy limitadas socialmente, por lo que no hay evidencia de la necesidad de ocultar información. 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, éstas constituyen los primeros textos cifrados en el continente americano. Posteriormente fue común la correspondencia codificada entre funcionarios de la Corona Española y los gobernantes en la Nueva España.

Tras la independencia de México en 1821, hubo un largo periodo 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 , cuando ya se había inventado el telégrafo, que creció de manera considerable el uso de la criptografía mediante telegramas. Tal es el caso de Don Benito Juárez que mantuvo una constante comunicación cifrada con Don Ignacio L. Vallarta, gobernador de Jalisco, usando un sistema de substitución simple.

10 de marzo 2008 • Volumen 9 Número 3 • ISSN: 1067-6079

La criptografía de Porfirio Díaz

Don 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 utilizó 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, se puede conocer con exactitud los métodos criptográficos empleados. La siguiente tabla por ejemplo muestra el método de substitución simple de Díaz e I. Bravo, uno de sus más importantes jefes militares en el sur del país (Ángel, Morales, 2007).

	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	

Tabla1: Clave de sustitución correspondiente al General Ignacio A. Bravo.

La tabla anterior sintetiza un método criptográfico de substitución simple, es decir, empata un número con la letra del mensaje abierto. Cada letra del alfabeto español se encuentra en una casilla en el cruce de un renglón y de una columna y se le asigna como código un número entero de la forma XY donde X es uno de los índices asociados al renglón e Y el asociado a la columna. Por ejemplo la letra "G" (primer renglón y octava columna) tiene asociados cualquiera de los códigos 18, 28 o 38, como un segundo ejemplo al mensaje LEVANTAMIENTO se le puede asociar el texto cifrado 24,39, 77, 11, 95, 84, 21, 78, 33, 29, 75, 94, 16.

Los otros sistemas criptográficos utilizados por el gobierno de Díaz eran similares, o combinación de éstos con otra tabla de substitución simple que asociaba un número a cada dígrafo de aparición muy frecuente. Por ejemplo se tiene el sistema (llamado clave) del general Abraham Bandala, jefe militar en Tabasco,

	1	2	3	4	5	6	7	8	9	0
2,6,8	y		s		a				u	
0,4,7	g		c		l			h	m	
3,5	p				rr			q	e	
9				f				i	n	
1	z		d	o				r	v	

Tabla2: Clave de sustitución correspondiente al General Abraham Bandala

SE	10
OR	16
CON	22,62
EN	26
LIC	27
LA	30
RIO	32
IN	36

LA	50
DO	70
EL	80
LE	90
CION	92
OS	96
ES	97

Tabla3:Suplemento de la clave de sustitución correspondiente al General Abraham Bandala.

El anterior sistema tiene dos modificaciones: la primera consiste en que a algunas letras se les asocia las tres posibilidades de la clave de Bravo, en tanto que a otras letras sólo se les asigna un número. La segunda modificación es que para varias cadenas comunes de letras como LA, CION se les da un número particular. De esta manera el mensaje: revolución queda cifrado como 18, 59, 19, 14, 05, 69, 92. Tales claves eran muy comunes, casi todos los sistemas que Díaz usó por medio de Chousal eran de este tipo. También eran utilizadas otras claves de sustitución simple. En éstas, se reemplazaba cada palabra por un número, tales como QUE por 6355, ME por 1868 y PIDE por 158493. Estos ejemplos aparecen en el sistema empleado por Díaz y Diego Redo (2007), gobernador de Sinaloa, aprehendido en 1911 y salvado de ser fusilado por órdenes del presidente Madero.

Criptografía de Francisco I. Madero

Durante el gobierno de don Francisco I. Madero se emplearon sistemas criptográficos de sustitución simple, también de diferentes tipos, algunos muy similares a los de Díaz. A su vez existieron otros que consistían en reemplazar algunas letras por otras en lugar de números. Por ejemplo las siguientes dos claves fueron utilizadas por Madero (2007):

	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

Tabla 4: Clave de sustitución correspondiente a F. I. MaderolGeneralAbrahamBandala.

Como antes, cada letra se cifraba con la pareja de letras XY donde X es la letra que aparece como índice del renglón en que se ubica la letra Y de la columna. Entonces el mensaje: "Congreso Nacional" queda "Jrrirojibmjobari Rojmjrjerirojmrr".

10 de marzo 2008 • Volumen 9 Número 3 • ISSN: 1067-6079

Madero utilizó otro tipo de sistemas, que utilizaba números como códigos, pero aparentemente prefería usar letras. En su comunicación con Francisco Vázquez Gómez, su Ministro del Interior, usó un sistema de substitución simple que reemplazaba palabras con códigos de 5 letras. Algunos de éstos son [4]: "gathi", "nkbeb", "lqkre", "hpezd", "tpiby", etc.

Criptografía de los Constitucionalistas

Los años más duros de la guerra estaban aún por venir. En 1913 el General Victoriano Huerta dio un golpe de estado contra el presidente Madero, quien junto con su vicepresidente José María Pino Suárez, fue 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, utilizó también mensajes cifrados. Para esta etapa avanzada de la guerra, era de suponerse que los sistemas anteriores se modificaran. Carranza y sus jefes principales usaron diferentes tipos de mensajes varios de sustitución simple como los anteriores, sin embargo hay evidencia de que algunos jefes revolucionarios, incluso Francisco Villa, emplearon un sistema que combinaba la idea anterior para asignar diferentes claves.

El sistema llamado Mexican Army Cipher Disk (Kahn, 1967) es el sistema criptográfico mexicano más conocido. Una de sus claves se muestra en la siguiente tabla. Fue interceptada y reconocida por el ejército norteamericano. El telegrama interceptado cifraba un mensaje entre los generales Jacinto Treviño y Álvaro 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, en el que identificando al alfabeto latino de 26 caracteres, cada letra en el mensaje a cifrar era sustituida por la correspondiente a un desplazamiento (cíclico de módulo 26) dado por la clave del sistema.

Elementos del sistema: se considera el siguiente arreglo de 5 renglones, el primero de los cuales corresponde al alfabeto de 26 letras, el segundo corresponde a los números del 1 al 26 colocados de manera secuencial, módulo 26, a partir de una letra (D, en este caso), el tercero consiste de los siguientes 26 números enteros, es decir del 27 al 52 puestos de manera secuencial, donde al primer número, 27, marca el inicio de ese ciclo dependiendo de la clave. La cuarta columna, de manera similar corresponde a los siguientes 26 números enteros, del 53 al 78, donde el número 53 marca el inicio de ese ciclo, dependiendo de una clave. Finalmente la quinta columna corresponde a los números del 79 al 99, donde 79 corresponde al inicio de ese ciclo en alguna letra de acuerdo con la clave (observamos aquí que siempre quedan faltando 5 letras por asociar en esta columna).

La clave del sistema: En el caso anterior, la clave es AWIO. El manejo de las claves se llevaba de diferentes maneras. La forma más común era por medio de libros de código, es decir cuadernos de claves que previamente se acordaban y que sólo ambos lados de la comunicación conocían. En el telegrama mencionado, se dice como clave EN LA G. Entonces el receptor del telegrama revisaba su libro de código y obtenía la clave, a saber, AWIO.

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: "Hoy sigo mi avance" queda cifrado como "08 15 25 19 39 37 45 13 53 01 22 71 14 33 05" que corresponde al telegrama de arriba, pero también pudo haber sido cifrado así "98 79 89 83 09 07 45 13 09 31 22 31 44 03 75". No hay ninguna ambigüedad: a pesar de que un mismo texto en claro puede tener dos textos cifrados, cada uno de ellos, al ser descifrado, ha de reproducir el mismo mensaje en claro.

Método de descifrado: Con el mensaje cifrado simplemente hay que obtener de la tabla la letra correspondiente para de esta manera descifrar el contenido.

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
24	25	26	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
41	42	43	44	45	46	47	48	49	50	51	52	27	28	29	30	31	32	33	34	35	36	37	38	39	40
57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	53	54	55	56
99						79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98

Tabla5: Clave criptográfica entre Treviño y Obregón. Según el método de cifrado de los constitucionalistas.

Conclusiones

Una de las etapas, quizás la primera, donde se empleó criptografía en México de manera extendida fue precisamente la Revolución Mexicana. Casi todos los participantes se sirvieron de estos métodos criptográficos, algunos muy similares a los usados en la época en otros lados del mundo, sin embargo algunos fueron diseñados de manera original por los combatientes mexicanos.

Debido a lo estratégico de la información de los diversos bandos beligerantes fue necesario mantener la confidencialidad en las comunicaciones. Los métodos usados, en su gran mayoría, fueron simples. Aparentemente resultaron seguros en esa época. Los códigos de Díaz y de Madero se basan en ideas muy conocidas en el mundo, algunas que se remontan al primer siglo antes de Cristo debidas al estratega griego Polibio y adaptadas de manera ingeniosa y original para evitar ataques. Hasta la fecha no se conoce documento alguno donde se muestre claramente que un sistema criptográfico haya sido comprometido en su momento.

El sistema Mexican Army Cipher Disk fue descifrado por criptoanalistas norteamaericanos (Hitt, 1976) y documentado plenamente.

Además de mantener la confidencialidad en comunicaciones en el territorio nacional, varios contendientes utilizaron sistemas reforzados para comunicarse con sus agentes en Estados Unidos, que también consistían en sustituciones simples únicas.

Aunque no fue visto así en su momento, los métodos empleados constituyeron una manifestación de desarrollo tecnológico nacional.

10 de marzo 2008 • Volumen 9 Número 3 • ISSN: 1067-6079

Bibliografía

Acervo Histórico de Porfirio Díaz "Telegramas de Porfirio Díaz," Biblioteca: Francisco Xavier

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

----------Guillermo. La Historia de la Criptografía en México, en preparación México. CINVESTAV, 2007.

CLAVIJERO, Universidad Iberoamericana, campus Santa Fe, México.

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.