La criptografía de Porfirio Diaz.

Article *in* Ciencia y desarrollo · October 2019

CITATIONS
0

READS
10

1 author:

José De Jesús Angel-Angel
Anáhuac University
23 PUBLICATIONS **8** CITATIONS

SEE PROFILE

RADIO DIGITAL: ¿LA HAS ESCUCHADO?

CIENCIA Y DESARROLLO

MAYO 2008 VOLUMEN 34 NÚMERO 219 MÉXICO

→ **CRIPTOGRAFÍA** EN EL PORFIRISMO

→ **NUEVOS MATERIALES** EN CARRETERA

EUTANASIA:
UNA RESPUESTA EN CADA CASO

→ MEDICINA, ¿HASTA DÓNDE LLEGAR?
→ EUTANASIA, ¿UN ALIVIO EXCEPCIONAL?
→ ¿QUÉ OFRECER AL ENFERMO TERMINAL?
→ LA LEY, ¿PLURALIDAD O INTOLERANCIA?

$20.00
7 509997 150345 00219

HÉLIX: Súper computadoras

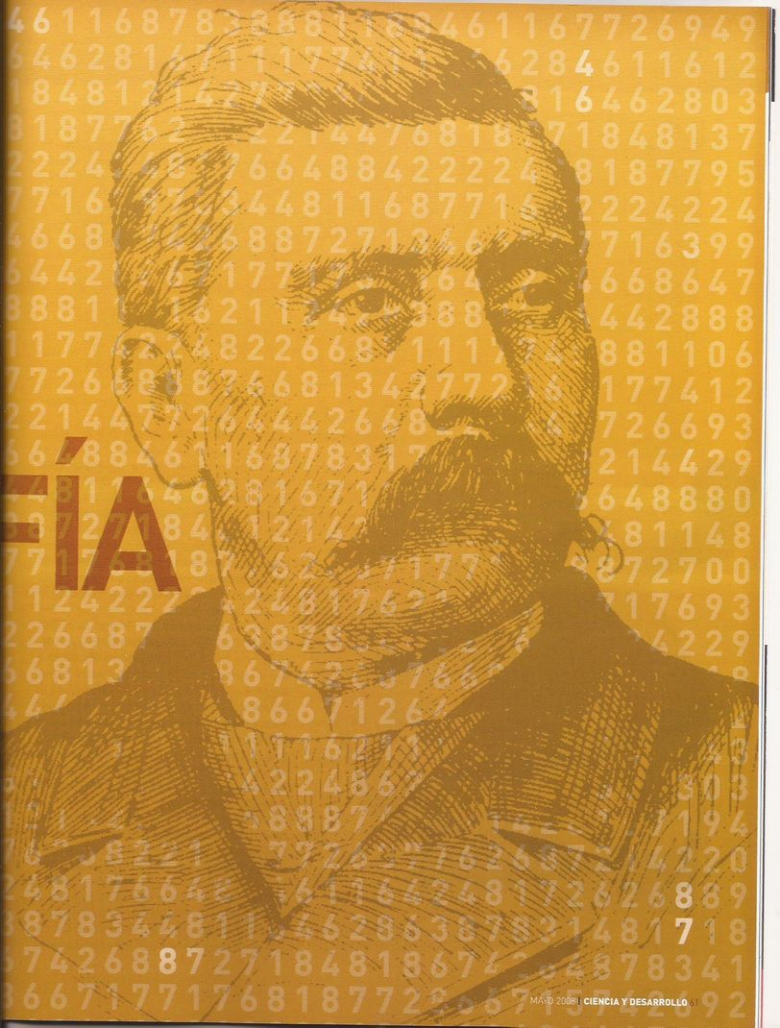
TECNOINFORMACIÓN: Políticas públicas para la SIC

ENTREVISTA: Alfonso Dueñas González

La criptografía es el arte y la ciencia de enviar mensajes de manera cifrada o transformada, de tal manera que sólo un receptor autorizado – o , enterado de las claves o procesos de transformación– pueda conocer el contenido de éstos. La criptografía ha sido utilizada a lo largo de la historia en todo el mundo, de manera frecuente, y en varios ámbitos como el militar, el diplomático y el financiero.

CRIPTOGRAF en la presidencia de Porfirio Díaz

GUILLERMO MORALES LUNA Y JOSÉ DE JESÚS ÁNGEL ÁNGEL


-ÍA

CRIPTOGRAFÍA en la presidencia de Porfirio Díaz

Hasta antes de la década de 1970, los métodos utilizados para los mensajes ocultos requerían que las partes por comunicarse, compartieran claves para cifrar y descifrar, las cuales debían mantenerse en secreto, por lo que éstos se conocen como métodos simétricos o de clave secreta, y han sido tan diversos como las famosas *escítalas* (mensajes usados por los espartanos en el siglo V a. C, caracterizados por ocultar el significado real de un texto alterando el orden de los signos que lo conformaban), o como el sistema DES *(Data Encryption Standard*, sistema de clave privada que emplea una longitud de *bits* y que fue un estándar comercial hasta el año 2002).

En la actualidad, los métodos de cifrado son de clave pública, inventados en la década de 1970, y se utilizan ampliamente en diversas actividades como en la seguridad de las comunicaciones electrónicas (basadas en estándares de internet, de cifrado y de firma electrónica).

→TELÉGRAFO Y FERROCARRIL DE LA ÉPOCA PORFIRIANA

Por ejemplo, el Sistema de Administración Tributaria del Gobierno Federal Mexicano certifica firmas digitales en el universo de contribuyentes para que éstos puedan realizar transacciones confidenciales, autenticables, íntegras y vinculadoras, y los procedimientos involucrados están basados en protocolos criptográficos de clave pública.

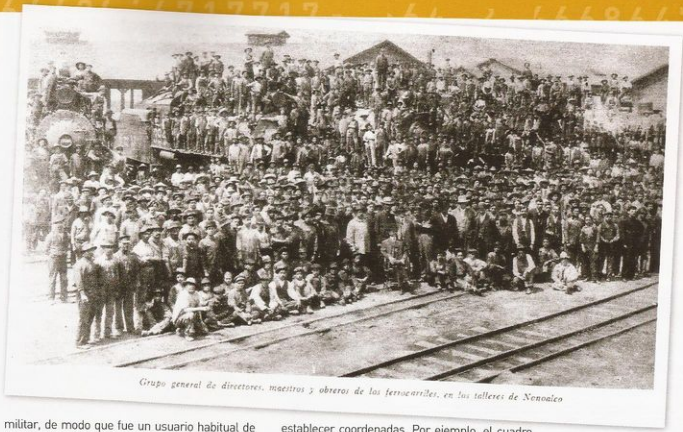
LA CRIPTOGRAFÍA EN MÉXICO

Existen varios tratados y artículos de investigación sobre la historia de la criptografía en el mundo;[1,2] sin embargo, en México se desconocen aún muchos aspectos de su historia, tales como los métodos y las claves utilizadas, pues pocos personajes documentaban el cifrado de textos, y las claves se perdían cuando sus propietarios abandonaban la vida pública.

Es posible identificar varias etapas históricas en las cuales la criptografía ha tenido un papel trascendente en México. De una de ellas proviene el primer documento cifrado conocido en América: una carta escrita por Hernán Cortés a su primo Francisco Núñez, representante suyo ante la Corte; en la misiva lo instruía, entre otros asuntos, para que gestionara una indemnización consistente en unas tierras en el actual estado de Michoacán, ya que la ciudad de Antequera (hoy Oaxaca) se fundó en una parte de su Marquesado.[3]

En la época colonial, las técnicas de cifrado fueron utilizadas, principalmente, en correspondencia oficial entre la Corona Española y los virreyes u otros funcionarios de la Nueva España[2] y en el periodo que abarca desde la Guerra de Independencia y los primeros años del México Independiente seguramente fue usada alguna técnica de cifrado, pero lamentablemente, la documentación es sumamente escasa. Fue durante de la Reforma cuando se incrementó el uso de la criptografía en la telegrafía, reciente en el México de esa etapa.

Porfirio Díaz llegó a cobrar relevancia en los medios militares mexicanos desde la Intervención Francesa y se convirtió en presidente de 1876 a 1880, en un primer periodo y, de 1884 a 1910 transcurrió la etapa que fue conocida como el *porfiriato*, durante la cual tuvo una gran actividad de *inteligencia*; su preparación militar lo capacitó en el uso de las técnicas y los medios con los que en esos tiempos se contaba para el control



Grupo general de directores, maestros y obreros de los ferrocarriles, en los talleres de Nonoalco

militar, de modo que fue un usuario habitual de las técnicas criptográficas clásicas en el medio militar de su tiempo.

Desde 1884, Don Rafael Chousal y Rivera Melo,[4] hombre de toda su confianza, se convirtió en su secretario particular y fue el encargado de administrar y operar los esquemas criptográficos hasta 1911, y su labor consistió en escribir y descifrar los telegramas cifrados que Porfirio Díaz enviaba a los gobernadores de los estados y a diversos jefes militares.

ESQUEMAS CRIPTOGRÁFICOS DE P. DÍAZ

Hasta la primera mitad del siglo XX era común utilizar métodos de cifrado conocidos como de *sustitución simple*, es decir, cada uno de los caracteres de un alfabeto se sustituye por una cadena de símbolos, y fue este el esquema utilizado por Porfirio Díaz. Aparentemente, fue Chousal quien eligió los esquemas usados, y éstos eran comunes para la época, no sólo habían sido utilizados otros similares desde los tiempos de Juárez, sino que los mismos principios pueden remontarse, incluso, a los llamados *Cuadros de Polibio* (historiador griego del siglo II a. C.). En ellos, los caracteres de un alfabeto se colocan en una cuadrícula y cada carácter se codificará por los índices de su posición, tomando como referentes la primera fila y la primera columna para establecer coordenadas. Por ejemplo, el cuadro codifica a A con 11, a M con 32, a O con 35 y a R con 43. Por tanto el mensaje AMOR queda cifrado como 11 32 35 43.

En el Acervo Histórico de Porfirio Díaz, conservado en la Biblioteca "Francisco Xavier Clavijero", de la Universidad Iberoamericana, *campus* Santa Fe, existe una nota manuscrita sobre un telegrama con la clave mostrada en las figuras 2 y 3.

FIGURA1

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	L	M	N	Ñ	O
4	P	Q	R	S	T
5	U	V	X	Y	Z

→ **EJEMPLO DE LA IDEA DE POLIBIO ADAPTADA AL ESPAÑOL ACTUAL.**

FIGURA 2

CLAVE DE SUSTITUCIÓN CORRESPONDIENTE AL GENERAL IGNACIO A. BRAVO

	1	2	3	4	5	6	7	8	9	0
123	A	U	I	L	RR	O	H	G	E	C
456		X	R			Q	J	D	P	LL
789	CH	S	Z	T	N	Y	V	M	B	

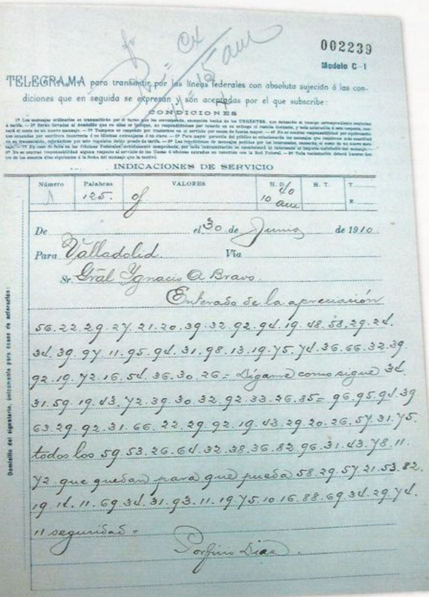
Este esquema es típico de los utilizados por Chousal para generar diversas claves. De acuerdo con ella, a cada letra podía asignarse tres diferentes enteros entre el 10 y el 99. Por ejemplo a la letra "a", al momento de cifrar le es asignado uno cualquiera de los números 21, 61, 71, a "t" uno de entre 14, 44, 54, a "c" uno de entre 23, 63, 73 y a "r" uno de entre 11, 41, 51 y a "p" uno de entre 39, 89, 99, entonces el mensaje atacar puede cifrarse como 21,54,61,73,71,51. Al cambiar de orden los números en la primera columna se puede obtener un cuadro diferente.

Chousal desarrolló un sistema de claves que incluía algunas variantes de cifrado para comunicarse con diversos funcionarios del gobierno de Díaz, lo que se comprueba al examinar su archivo,[5] en el que cada gobernador o jefe militar tenía su propio cuadro. A manera de ejemplos mostramos el cuadro diseñado para comunicarse con el General Ignacio A. Bravo, Jefe Militar del Sureste, con base en Valladolid, Yucatán, el cual era similar al ejemplo anterior, de mera sustitución simple, al que nos referiremos como el tipo Díaz-Bravo.

SISTEMA CRIPTOGRÁFICO DÍAZ-BRAVO

Parte del cuadro de sustitución empleada en la correspondencia cifrada con el General Ignacio A. Bravo aparece en la tabla 2 que fue reconstruida mediante la comparación de telegramas descifrados encontrados en el Acervo, los cuales proporcionan parejas de mensajes original y cifrado texto-en-claro, texto-cifrado.

Naturalmente, para cada mensaje que debía ser cifrado se elegía de manera aleatoria uno de los códigos para cada letra; por ejemplo, la palabra MENSAJE puede ser cifrada con la cadena 88 19 75 92 11 57 39. Con este cuadro es posible descifrar una gran cantidad de telegramas de


002239
Modelo C-1

TELEGRAMA para transmitir por las líneas federales con absoluta sujeción á las condiciones que en seguida se expresan y son aceptadas por el que subscribe:

CONDICIONES

INDICACIONES DE SERVICIO

Número	Palabras	VALORES	H. D.	H. T.	T.
1	125.	of	10 40 am		

De el 30 de Junio de 1910

Para Valladolid Vía

Sr. Gral Ygnacio A. Bravo

Enterado de la apreciación

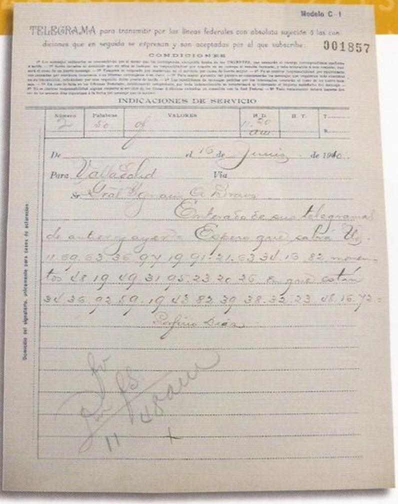
56.22.29.27.21.20.39.32.92.94.19.48.58.29.24.
34.39.97.11.95.94.31.98.13.19.75.74.36.66.32.39.
92.19.72.16.54.36.30.26= Dígame como sigue 34.
31.59.19.43.72.39.30.32.92.33.26.85= 96.95.94.39
63.29.92.31.66.22.29.92.19.43.29.20.26.57.31.75.
todos los 59.53.26.64.32.38.36.82.96.31.43.78.11.
72 que quedan para que pueda 58.29.57.21.53.82.
19.14.11.69.34.31.93.11.19.75.10.16.88.69.34.29.74.
11 seguridad=

Porfirio Díaz.

FIGURA 3

Telegrama (002239) de Díaz a Bravo

No. Catálogo: (002239)
Fecha: 30 junio de 1910
Enterado la apreciación QUE HACE USTED DEL LEVANTAMIENTO QUE SE SOFOCO. Dígame como sigue LA PERSECUCION. YNTERESA QUE SE RECOJAN todos los PROFUGOS Y ARMAS que quedan para que pueda DEJARSE LA PLAZA EN COMPLETA seguridad.


Modelo C-1

TELEGRAMA para transmitir por las líneas federales con absoluta sujeción á las condiciones que en seguida se expresan y son aceptados por el que subscribe: 001857

CONDICIONES

INDICACIONES DE SERVICIO

Número	Palabras	VALORES	H. D.	H. T.	T.
2	30	of	11.20 am		R.

De ______ el 16 de Junio de 1910

Para Valladolid Vía

Sr. Gral. Ygnacio A. Bravo

Enterado de sus telegramas de antier y ayer. Espero que sabrá U.
11.59.63 36 97 19 91.21.63 31 16 82 momen-
tos 28 19 59 31 95.23 20 26 en que están
91 36 92 59 19 43 85 39 38.35.23 48.16.72.
Porfirio Díaz

Domicilio del signatario, únicamente para casos de aclaraciones

FIGURA 4
Telegrama (001857) de Díaz a Bravo
No. Catálogo: (001857)
Fecha: 16 junio de 1910
De: Porfirio Díaz
Para: Ignacio A. Bravo
Enterado de su telegrama de antier y ayer. Espero que sabrá usted APROVECHAR LOS momentos DE PANICO en que estan los PERSEGUIDOS

Bravo. Las letras faltantes en el cuadro no figuran en la correspondencia Díaz-Bravo, por lo que son irrelevantes en el desciframiento de ella.

En las figuras 2 y 3 presentamos una imagen del telegrama de Porfirio Díaz a Ignacio A. Bravo, fechado el 16 de junio de 1910, con número de catálogo (001857), y su correspondiente decodificación; el primero fechado el 16 de junio de 1910 y el segundo el 30 de junio del mismo año.

LA HISTORIA DE NUESTRO PAÍS, EN CLAVE

Desde el punto de vista histórico, el criptoanálisis de textos de Porfirio Díaz tiene la ventaja de descubrir su contenido, pues las claves empleadas sólo eran conocidas por sus corresponsales y éstas no subsistieron. El criptoanálisis ofrece la llave de acceso a correspondencia que ejerció un importante impacto en la sociedad de su tiempo. Desde el punto de vista tecnológico, la decodificación de mensajes cifrados es un trabajo que descubre un nuevo apoyo para la investigación histórica de nuestro país.

En este artículo sólo se han mostrado algunos esquemas que forman parte de una investigación más amplia, la cual aborda el tema de la criptografía a lo largo de la historia nacional.

Guillermo Morales Luna es doctor en ciencias e investigador en el Departamento de Computación, CINVESTAV-IPN. Es autor de diversos artículos de investigación en el área de Fundamentos matemáticos, lógica y criptografía, y miembro del SNI.

José de Jesús Ángel Ángel es maestro en ciencias y cursa el doctorado en el CINVESTAV-IPN.

BIBLIOGRAFÍA

1. Bauer, F. L., *Decrypted Secrets*, Springer, Berlin, 2002.
2. Kahn, D., *The Codebreakers - The Story of Secret Writing*. The Macmillan Co, New York, 1967.
3. Martínez, J. L. *Hernán Cortés*. Fondo de Cultura Económica, México, 1990.
4. Salinas, L. *Inventario del Fondo Rafael Chousal (1860-1967)*. Guías y catálogos del Archivo Histórico de la UNAM, México, 1998.
5. Galende D., "Sistemas Criptográficos empleados en Hispanoamérica". *Revista Complutense de Historia de América*, 26:57-71, Madrid, 2000.
6. Hitt, P., *Manual For The Solution Of Military Ciphers 1*. Aegean Park Press, Walnut Creek, Cal. USA, 1976.
7. Wrixon, F. B., *Codes Ciphers & Other Cryptic & Clandestine Communication*. Black Dog & Leventhal Publishers, New York, 1998.