

La criptografía carrancista

Juan Antonio Pérez
Unidad Académica de Matemáticas
Universidad Autónoma de Zacatecas

noviembre 30, 2025

*Para servir a la Patria,
nunca sobra el que llega
ni hace falta el que se va.*

VENUSTIANO CARRANZA (1859 - 1920)

En el período del 9 al 19 de febrero de 1913 se produjo el golpe de estado militar que llevó ilegítimamente al poder al General José Victoriano Huerta Márquez (1845 - 1916), derrocando al entonces presidente Francisco Ignacio Madero González (1873 - 1913), asesinado el día 22 de ese mismo mes, apenas tres días después de la llamada *Decena Trágica*.

Durante la revuelta, la heroica defensa de Palacio Nacional corría a cargo del General Lauro Villar Ochoa (1849 - 1923), quien luego de ser herido fue sustituido, por orden de Madero, ocupando su lugar el General Huerta quien pronto lo traicionaría. El hermano del presidente, Gustavo Adolfo Madero (1875 - 1913), enterado de la conspiración de Huerta lo capturó presentándolo ante el titular del ejecutivo, quien desestimando la versión de su familiar ordenó el 17, la liberación de quien sería dos días después el asesino de Gustavo y de él mismo el 22.

La respuesta revolucionaria se dio con la organización del llamado Ejército Constitucionalista bajo la dirección del General José Venustiano Carranza de la Garza (1859 - 1920), cuyos subalternos idearon varias formas de proteger la información contenida en sus comunicaciones internas. De este modo, parte de la secrecía descansaba en la variedad de mecanis-

mos de encriptación. La matemática contenida en estos sistemas criptográficos, si bien son bastante ingeniosos, es altamente elemental, por lo que el presente texto se limitará a describir uno de ellos.

El método más básico de los usados por las fuerzas carrancistas se construye sobre algo llamado *sustitución recíproca*, que consiste en una permutación de 26 símbolos, que se reduce a un apareamiento de los símbolos en el alfabeto. Por simplicidad, los carrancistas excluyeron las dobles como "RR" y "LL", además de la virgulillada "Ñ". Una *permutación* del conjunto $\mathcal{A}$, es una biyección de $\mathcal{A}$ en $\mathcal{A}$, es decir, una *correspondencia bi-unívoca*; un apareamiento en el que cada pareja tiene elementos diferentes.

Si $f : \mathcal{A} \rightarrow \mathcal{A}$ es un apareamiento de $\mathcal{A}$, y $f(a) = b$, entonces $a \neq b$. Técnicamente, un apareamiento es una permutación libre de puntos fijos. En la siguiente figura se ilustra un apareamiento f de las letras vocales del alfabeto castellano, en la que, por ejemplo $f(A) = O$ y $f(E) = U$.

x	A	E	I	O	U
$f(x)$	O	U	E	I	A

Si adicionalmente suponemos que que $f(S) = M$ y $f(M) = Q$, la palabra "OSO" se codifica como "IMI", en tanto que "AME" sería encriptada mediante "OQU".

Una *involución* es una función tal que si $f(x) = y$, entonces $f(y) = x$. No es posible encontrar una involución que sea además un apareamiento sobre un conjunto con una cantidad impar de elementos, lo que el lector podrá verificar con facilidad, por lo menos en el caso de las letras vocales. Esto es posible en un conjunto de 26 elementos ya que 26 es par, y es muy probable que sea esta la razón para excluir la "Ñ".

El método de sustitución recíproca se fundamenta en la elección de un apareamiento involutivo. En la siguiente tabla se ofrece un ejemplo de tal apareamiento en un conjunto de 8 letras: las vocales y tres consonantes.

x	A	E	I	O	U	R	S	T
$f(x)$	T	S	R	U	O	I	E	A

En el caso presente "OSO" se escribe "UEU", mientras que "ATE" se ve como "TAS". Se verifica facilmente que, si se sabe que el método es el de la sustitución recíproca, la decodificación no es tan complicada.

En matemáticas se sabe que toda permutación se descompone en ciclos ajenos. El primer ejemplo es un ciclo único, a saber $(AOIEU)$, en el que x es seguido de $f(x)$ hasta que se cierra el ciclo, en este caso, por ejemplo $f(U) = A$ constituye el cierre.

En nuestro segundo ejemplo, que es al caso típico de la sustitución recíproca carrancista, la descomposición en ciclos se escribe como se expresa abajo, en la que solo cuatro pares expresan toda la permutación.

$$(AT)(ES)(IR)(OU)$$

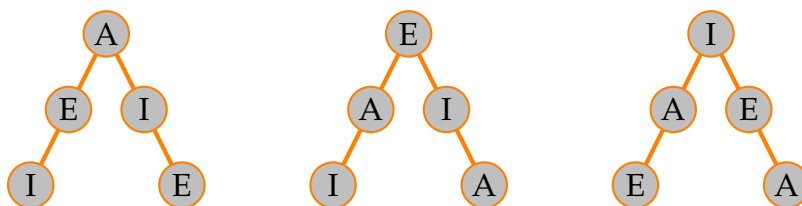
Consideremos ahora una permutación f de las cinco vocales que no es un ciclo, y que tampoco es una involución.

x	A	E	I	O	U
$f(x)$	O	U	A	I	E

En este caso la permutación se descompone en un ciclo de longitud tres y otro de longitud dos.

$$(AOI)(EU)$$

El número de permutaciones crece extremadamente rápido en relación con el número de elementos que se permutan. Las permutaciones de 3 elementos son $1(2)(3) = 3! = 6$ y las de 5, las vocales por ejemplo, son $(1)(2)(3)(4)(5) = 5! = 120$. El siguiente diagrama de árbol ilustra las seis permutaciones de un conjunto con tres elementos.



Un conjunto de cuatro elementos admite $4! = 24$ permutaciones y el conjunto de los 26 caracteres usados por la tropas carrancistas, tiene

más de 403 sextillones de permutaciones, es decir, un número superior a 403×10^{24} , aunque, por supuesto, no todas ellas resultan admisibles para la metodología carrancista. Buscamos *configuraciones*, es decir, permutaciones libres de puntos fijos.

Como puede observarse del ejemplo anterior, las únicas dos configuraciones del conjunto $\{A, E, I\}$ son las permutaciones (AEI) y (AIE) . La primera corresponde a los pares ordenados (A, E) , (E, I) , (I, A) . La segunda describe los apareamientos (A, I) , (I, E) , (E, A) . Ninguna de nuestras alternativas presenta un par con dos componentes iguales, es decir, no tienen puntos fijos.

Se observa sin dificultad que cualquier otra permutación deja fijo algún elemento. El número de configuraciones para 3 elementos es entonces 2. Si designamos por $P(n)$ el número de configuraciones de un conjunto de n elementos, tenemos que $P(3) = 2$. Usted puede verificar también, mediante exploración directa que $P(4) = 9$ y $P(5) = 44$. Puede demostrarse adicionalmente que, en general, y de forma recursiva

$$P(n) = nP(n-1) + (-1)^n,$$

de manera que $P(6) = 6(44) + 1 = 265$, de donde se advierte que la alta velocidad con la que este número crece.

Otra propiedad útil es que $P(n)$ es un número entre $\frac{n!}{4}$ y $\frac{n!}{2}$, pero 100 sextillones parece todavía excesivamente grande. La restricción carrancista de la sustitución recíproca reduce las posibilidades. Veamos, en un conjunto de 26 letras el número de apareamientos posibles es el número de biyecciones del conjunto de las 13 primeras en el conjunto de las 13 que completan el alfabeto. No es muy complicado concluir que este número es justamente $13!$, es decir, es igual al número de permutaciones en un conjunto de 13 elementos.

A pesar de que el ejército constitucionalista contaba con

$$13! = 6,227,020,800$$

códigos posibles, por razones probabilísticas, cada uno de ellos es bastante débil, pues basta explorar la frecuencia de aparición de cada uno de los caracteres empleados para descifrarlo.

Entonces, el número de involuciones sin puntos fijos en un conjunto de 26 elementos es, como ya calculamos $13!$. En general, hay $n!$ involuciones sin puntos fijos en un conjunto de $2n$ elementos.

El nacionalismo del General Carranza no deja dudas, su capacidad diplomática dejó también testimonio al evitar la guerra con los Estados Unidos, y como vemos, la habilidad matemática de su ejército tampoco es despreciable.