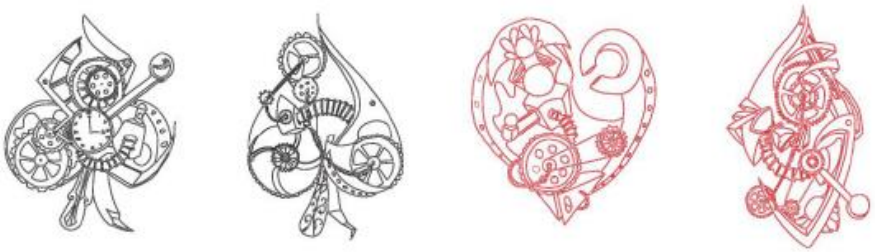
EL ALGORITMO DE CIFRADO *SOLITARIO*

De la novela Criptonomicón

Escrita por Neal Stephenson



Jonathan Carrero

Abril 2018

«Generadores eléctricos» tiene, ¿cuántas?, ¿nueve sílabas?
¡Ni siquiera podría encajarlo en la segunda frase!

Bobby Shaftoe

Índice de contenido

1. Introducción

En la novela de Neal Stephenson *Criptonomicón*, el personaje de Enoch Root describe un criptosistema llamado «Pontifex» a otro personaje llamado Randy Waterhouse, y más tarde revela que los pasos del algoritmo se ejecutan empleando un mazo de cartas. El algoritmo, cuyo nombre real es «Solitario», está pensando para el intercambio de mensajes sin levantar sospechas, porque… ¿quién sospecharía de un mazo de cartas?

Manipulando el mazo, un emisor puede crear una cadena de letras y cifrarlas. Evidentemente, Solitario puede simularse en un ordenador, pero se le ha diseñado para ser ejecutado a mano. Puede que Solitario sea de baja tecnología, pero la intención es que su seguridad sea de lo más potente. Bruce Schneier, creador del algoritmo, lo diseñó para que fuese lo más seguro posible aun teniendo los mejores ordenadores y criptoanalistas más inteligentes. Por supuesto, nada garantiza que alguien no pueda encontrar un ataque ingenioso contra Solitario, pero el algoritmo es claramente mejor que otros de lápiz y papel. Aunque el principal problema de Solitario es que no es rápido. Puede llevar toda una tarde cifrar y descifrar un mensaje razonablemente largo.

Durante el siguiente documento se explica en qué consiste el algoritmo y se ven algunos ejemplos sencillos para entender su funcionamiento. Evidentemente, es necesario tener a mano una baraja de póker (tréboles, diamantes, corazones y picas) para seguir los pasos. También se adjunta información adicional que podría interesar al lector referente a la novela y a algunas características del algoritmo. Para evitar leer todo el documento, recomiendo consultar el índice para que, por ejemplo, si simplemente se está interesado en el funcionamiento del algoritmo, vayas directamente a Funcionamiento del algoritmo.

2. Sinopsis de la novela

En 1942, Lawrence Pritchard Waterhouse, genio matemático y joven capitán de la marina estadounidense, recibe la orden de colaborar con Bobby Shaftoe en una misión secreta que consiste en descifrar los códigos de las potencias del Eje y evitar que los nazis descubran que la Inteligencia aliada ha interpretado su mítico código Enigma. Sesenta años más tarde, Randy Waterhouse, brillante criptohacker, proyecta la creación en el sureste asiático de un paraíso de datos que ha de convertirse en el mayor exponente de la libertad informática: la Cripta. Cuando los gobiernos y las multinacionales atacan este proyecto, Randy se alía con Amy, la nieta de Shaftoe, para intentar rescatar un submarino nazi que contiene la clave para mantener a flote el sueño de la Cripta. Su estratagema pronto saca a la luz una gigantesca conspiración y un código indescifrable llamado Aretusa. Por primera vez en castellano aparece en un solo volumen la edición completa del libro más logrado de Neal Stephenson. *Criptonomicón*, un tour de force narrativo, una obra profunda y profética, hipnótica y trepidante. Una obra de arte, producto de una imaginación iconoclasta y sorprendente.

3. Características del algoritmo

El corazón de Solitario se basa en la idea de que un mazo de póker, incluyendo sus dos comodines, tiene un total de 54 cartas que pueden ordenarse de millones de formas diferentes. Hay 54!, sobre 2,3 x 10^{71} formas posibles de ordenar todas las cartas. Mejor aún, si quitamos los comodines, hay 52 cartas en una baraja, y 26 letras en el alfabeto. Este tipo de coincidencia es demasiado buena para dejarla pasar.

El principal problema de este tipo de criptosistemas suele ser la debilidad de la clave, que es la misma para los dos interlocutores y que podría ser interceptada por un tercero. Pero ¿a quién le podría parecer que en una baraja de cartas desordenadas que va en la maleta podría ir guardada una clave de alto secreto?

A continuación, se explican algunos puntos importantes a tener en cuenta sobre todo lo que rodea a Solitario y a muchos otros criptosistemas:

- El sistema ideado por Schneier es matemáticamente seguro: se ha calculado que equivale más o menos a una clave de 236 bits. El hecho de que Solitario sea público y de que la novela haya alcanzado popularidad, no le resta validez ni seguridad. El único punto crítico es que las claves (los mazos de cartas) se puedan intercambiar de antemano con seguridad. Si eso se hace correctamente, y si luego se utiliza una contraseña (frase) suficientemente segura, no hay problema aunque el «enemigo» conozca el sistema que se está usando.
- Es importante generar la clave correctamente e intercambiarla con el interlocutor de forma segura. De poco sirve generarla de forma correcta pero luego enviarla por correo electrónico o por teléfono, si el correo o el teléfono pueden ser interceptados.
- Nunca hay que cifrar dos mensajes con la misma clave. Esta es una regla que se aplica a muchos sistemas criptográficos básicos, sobre todos los que constan de un libro de claves y una serie de letras que se aplican para cifrar, descifrar y luego desechar. Si se reciclan las claves se está dando una valiosa pista al «enemigo», que podría adivinarlas examinando las diferencias entre los textos cifrados.
- Es mucho mejor si los mensajes a cifrar son cortos. Cuanta menos información haya que manejar, menos fallos y menos datos que transmitir y que puedan ser interceptados y analizados.

¿Lo mejor de solitario? Que a diferencia de las claves secretas y mensajes que manejaban Mortadelo y Filemón, una vez leídos los textos basta con mezclar la baraja unas cuantas veces para que no quede ni rastro de las claves que se utilizaron… sin necesidad de comérselas.

4. Funcionamiento del algoritmo

He leído algunos ejemplos en los que se intenta explicar el algoritmo lo más sencillamente posible, pero a veces no queda del todo claro o es difícil de seguir. Creo que la mejor manera de entender el algoritmo es directamente haciéndolo con un ejemplo. Debemos tener en cuenta que hay dos fases claramente diferenciadas en cualquier criptosistema: **cifrar** y **descifrar** un mensaje. Antes de ver cada una de las fases, vamos a preparar nuestro mazo de cartas.

En primer lugar, debemos tener dos comodines que sean diferentes. Observa los comodines, seguro que entre ellos hay alguna diferencia. Si no es así, haz una marca en uno de ellos. Esto nos sirve para decir que uno será el comodín `A` y otro será el comodín `B` (nómbralos como tú quieras).

Inicialmente vamos a utilizar un mazo sin clave (más tarde veremos qué significa eso, por el momento no te preocupes). Para ello debemos ordenar el mazo de la siguiente forma: si contamos el número de cartas que tiene cada palo, veremos que son 13 (del As al Rey van 13 cartas, ambos incluidos). Ahora, lo que tenemos que hacer es colocar primero los tréboles, luego diamantes, corazones y picas. De tal forma que, desde la parte superior del mazo hasta la parte inferior, primero nos encontraremos los tréboles (cartas de la 1 a la 13), luego nos encontraremos los diamantes (cartas de la 14 a la 26), luego nos encontraremos los corazones (cartas de la 27 a la 39) y por último las picas (cartas de la 39 a la 52). Podemos simplemente ver esta baraja como:

```
1 2 3 … 50 51 52
```

Una vez que tenemos la baraja ordenada, vamos a introducir el comodín `A` y `B` al final del mazo (en ese orden). Ahora nuestra baraja tendrá este aspecto:

```
1 2 3 … 50 51 52 A B
```

4.1. Obtener la clave

Antes de cifrar un mensaje es necesario que tengamos una contraseña con la que cifrar dicho mensaje. Debes saber que hay dos tipos de contraseñas: con clave y sin clave. Para que sea más sencillo, primero vamos a obtener una contraseña sin clave. De hecho, por eso anteriormente hemos ordenador la baraja de esa forma tan básica, para que nuestro mazo no tenga ninguna clave.

1. Encuentra el comodín `A`. Intercámbialo con la carta que tiene debajo. Si el comodín está al final de la baraja, ponlo debajo de la primera carta. Tras hacerlo tendremos:

   ```
   1 2 3 … 50 51 52 B A
   ```

2. Encuentra el comodín `B`. Muévelo bajo la carta que está debajo de la que tiene debajo. Si el comodín está al final de la baraja, muévelo debajo de la segunda carta. Si el comodín es la penúltima carta, muévelo debajo de la primera carta. Básicamente asume que la baraja es un bucle, ¿te haces la idea? Es importante

realizar los dos pasos anteriores en orden. Es tentador volverse perezoso y simplemente mover los dos comodines cuando los encuentras. Tras hacerlo, tu baraja quedará:

`1 B 2 3 … 50 51 52 A`

3. Corta la baraja en tres, intercambiando las cartas antes del primer comodín con las cartas que están detrás del segundo comodín. "Primer" y "segundo" comodín se refiere al comodín que está más arriba o más abajo respecto al extremo de la baraja. Ignora el hecho de que un comodín es `A` y otro es `B`, en este paso. Recuerda que los comodines y las cartas entre ellos no se mueven. Esto es fácil de hacer con las manos. Si no hay cartas en una de las secciones (porque los comodines están juntos, o porque uno está arriba y otro debajo de la baraja), simplemente considera esa sección como vacía y muévela de todos modos.

   `B 2 3 … 50 51 52 A 1`

4. Mira la última carta. Conviértela a un número de 1 a 53 (usa el orden normal: tréboles, diamantes, corazones y picas. Si la carta es un trébol, toma su número tal cual. Si es de diamantes, suma 13 a su valor. Si es de corazones, súmale 26. Si es de picas, súmale 39. Ambos comodines suman 53). Cuenta el valor obtenido empezando en la carta superior (normalmente yo cuento de 1 a 13 una y otra vez, si es preciso; es más fácil que contar hasta un número alto de forma secuencial). Corta tras esa carta, dejando la última carta de la baraja a final.

   En este caso concreto, La última carta es un 1, lo que significa mover una carta. Recuerda que el 1 debe quedarse donde está, al final de la baraja. Tras hacer esto, la baraja debería quedar:

   `2 3 … 50 51 52 A B 1`

   Como vemos, el comodín `B` lo hemos movido una posición hacia abajo (respetando la última carta de la baraja, que era el 1).

5. Este último paso no modifica el mazo. Lo que tenemos que hacer es mirar la primera carta. Conviértela en un número de 1 a 53, de la misma manera que en el paso 4. Cuenta esas cartas desde la parte superior. Escribe la carta tras la que hayas terminado en un papel y no la quites de la baraja.

   Como la primera carta es un 2, contamos dos cartas, hasta el 4. Así que el primer número de nuestra secuencia para cifrar un mensaje será el 4. Para obtener el segundo número, procedemos a repetir los cinco pasos (recuerda, después de este paso la baraja se queda tal y como está, es decir, no hay que volver a ordenarla como al principio).

Te parecerá que es un poco tedioso conseguir sacar de esta forma los números para posteriormente cifrar el mensaje, pero en cuanto lo hayas hecho un par de veces, te saldrá solo y con mayor rapidez.

A modo de ayuda, te proporciono los diez primeros números obtenidos en un mazo sin clave como el que hemos usado en este ejemplo. Apúntalos, te serán útiles en el siguiente apartado. Los diez primeros números obtenidos si hubiésemos repetido los cinco pasos anteriores diez veces son estos:

4 49 10 (53) **24 28 51 44 6 4 33**

Nótese que cuando aparece un comodín, como el **(53)** que vemos ahí, no se utiliza para la contraseña. Simplemente se ignora y se vuelven a repetir los cinco pasos.

4.2. Cifrar un mensaje

Una vez que tenemos preparado nuestro mazo y además tenemos la contraseña que vamos a utilizar, vamos a cifrar un mensaje. A modo de ejemplo, cifremos: AAAAAAAAAA (diez letras "A". Más sencillo imposible).

1. Divide el mensaje original en grupos de cinco letras (no hay nada de especial en ello, simplemente se hace por tradición). Usa letras "X" para completar el último grupo en el caso de que faltasen letras. Así, nuestro mensaje quedaría:

   AAAAA AAAAA

   Pero si, por ejemplo, quisiéramos cifrar QUE TE DEN, nuestro mensaje quedaría:

   QUETE DENXX

2. Usa Solitario para generar una ristra de números con los que cifrar el mensaje. ¡Tachan! Esto es lo que hicimos en el punto anterior (ver Obtener la).

3. Convierte el mensaje que quieres cifrar a números. Luego como A es la primera letra del alfabeto:

   11111 11111

   Voy a dejar por aquí una tablita que nos hará falta en los siguientes pasos:

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Tabla 1: Orden en las letras del alfabeto

4. Sumamos los números de mensaje original con los correspondientes de la ristra Solitario, módulo 26. Es decir, si suman más de 26, restamos 26 al resultado. Algunos ejemplos:

   ```
   1 + 1 = 2
   26 + 1 = 27 y 27 - 26 = 1
   ```

   En nuestro caso tenemos que hacer la siguiente suma:

   ```
    1  1  1  1  1    1  1  1  1  1   <-------  Mensaje a cifrar
+
    4 49 10 24 28   51 44  6  4 33   <-------  Clave obtenida en el punto 4.1.

    5 24 11 25  3   26 19  7  5  8   <-------  Resultado de la suma
   ```

5. Por último, tan sólo queda pasar el resultado a letras para obtener el mensaje cifrado. Luego el mensaje `AAAAA AAAAA` cifrado con un mazo sin clave por el algoritmo Solitario da como mensaje cifrado:

   ```
   EXKYC ZSGEH
   ```

4.3. Descifrar un mensaje

Ahora que hemos entendido el proceso de cifrado, descifrar un mensaje nos resultará mucho más fácil de entender. El proceso es básicamente el mismo sólo que con un pequeño cambio (pongo los pasos mucho más resumidos que en el punto anterior).

1. Se coge el mensaje cifrado y se divide en grupos de cinco letras.

2. Se utiliza Solitario para generar la clave. Recordemos que antes de generar la clave, emisor y receptor se han debido de poner de acuerdo en cual será dicha clave. Y recordemos también que en el ejemplo nosotros hemos utilizado un mazo sin clave.

3. Convierte el mensaje cifrado a números.

4. Aquí viene el mayor cambio. Resta a cada número del texto cifrado el número correspondiente de la ristra, módulo 26. Algunos ejemplos:

   ```
   22 - 1 = 21
   1 - 22 = 5
   ```

   Es fácil. Si el primer número es menor o igual que el segundo, sumamos 26 al primer número antes de restar. Así, 1 – 22 se convierte en 27 – 22 = 5.

5. Por último, los números obtenidos en el resultado de la resta pásalos a letras y obtendrás el mensaje descifrado.

4.4. Introducir una clave en el mazo

Antes de empezar a generar la ristra, es necesario "introducir" una clave en la baraja. Ésta es, probablemente, la parte más importante de toda la operación, y en la que se basa toda la seguridad del sistema. Solitario es sólo tan seguro como lo sea su clave. Es decir, la forma más fácil de romper Solitario es imaginarse qué clave se está utilizando. Si no tienes una buena clave, el resto no importa. He aquí algunas sugerencias para realizar el intercambio de claves:

- **Utiliza dos mazos barajados de la misma manera.** Las claves aleatorias son las mejores. Uno de los comunicantes puede barajar un mazo de forma aleatoria, y luego copiar la distribución de las cartas en el otro mazo (para así obtener dos mazos iguales). Uno de los mazos es empleado por el emisor, y el otro por el receptor. La mayoría de la gente no son buenos barajando, así que baraja el mazo al menos seis veces. Ambas partes deben tener otra baraja adicional ordenada de la misma forma, porque si se comete algún error nunca se podrá descifrar el mensaje.
- **Usa un orden de Bridge.** La descripción de una mano de bridge en un periódico o en un libro de bridge constituye una clave de aproximadamente 95 bits. Ponte de acuerdo con el otro comunicante en la forma de convertir el diagrama en un orden concreto para tu baraja. Luego ponte de acuerdo sobre la forma de meter los dos comodines en el mazo. Una posibilidad obvia es poner el comodín A tras la primera carta que se mencione en el texto, y el comodín B tras la segunda carta mencionada en el texto.
- **Usa una "frase de paso" para ordenar la baraja**. Este método utiliza el algoritmo Solitario para crear un ordenamiento inicial del mazo. Ambos, el emisor y el receptor, comparten una frase de paso (por ejemplo, “CLAVE SECRETA”). Empezar con el mazo en un orden fijo; de la carta más baja a la más alta, con los palos en el orden visto previamente, y con los dos comodines al final, primero el `A` y luego el `B`. Ahora utilizamos Solitario, tal cual, pero al llegar al paso 5 (dentro del punto Obtener la clave) contamos según el número que corresponda a la primera letra de la frase de paso. En otras palabras: volvemos a realizar el paso 4, pero usando el número que corresponda a la primera letra de la palabra de paso (que en este caso sería la “C” de la palabra “CLAVE”) en vez de usar el número correspondiente a la última carta de la baraja. Recuerda poner las cartas de arriba justo debajo de la última carta de la baraja, como antes.

  Repetimos los cinco pasos de Solitario tantas veces como letras tenga la palabra de paso. Es decir, la segunda vez utilizaremos la segunda letra, la tercera vez la tercera letra, etc.