



ESCUELA POLITÉCNICA
SUPERIOR DE CÓRDOBA
Universidad de Córdoba



Grado en Ingeniería Informática

Especialidad de Computación

Cuarto curso, Primer cuatrimestre

Curso académico: 2020-2021

Códigos y Criptografía

Cifra ADFGVX

Autores: Francisco Bérchez Moreno

Tomás Fernández Urbano

Diciembre, 2020



UNIVERSIDAD DE CÓRDOBA





Índice

Historia	2
Cifra ADEGVX	4
Cuadrado Polybius	4
Explicación del método	5
Cifrado	5
Primer paso, inicialización del cuadrado de Polybius.	5
Segundo paso, sustitución del mensaje.	5
Tercer paso, transposición.	6
Descifrado	7
Primer paso, descomponer el mensaje cifrado.	7
Segundo paso, deshacer la sustitución.	8

Historia

A principios de la Primera Guerra Mundial (1914-1918), los alemanes utilizaban la cifra denominada UBCHI en todos los escalones del ejército para comunicar sus planes estratégicos que fue originada en los años previos al conflicto. Sin embargo, hasta el comienzo de la guerra, los criptógrafos franceses tuvieron tiempo para hallar un método de descifrado lo que ayudó a los mismos en diversos episodios de la “guerra de movilidad” que se estableció en agosto y septiembre de 1914, especialmente en la preparación de la primera batalla del Marne, manteniendo esta ventaja hasta diciembre del mismo año.

Los alemanes al percatarse de dicha ventaja cambiaron rápidamente el método por otro conocido como ABC. De pronto, el 21 de enero de 1915, el capitán de artillería Georges Painvin encontró un nuevo método para romper el cifrado ABC debido a que este contenía defectos ocultos y de hecho empeoraba la seguridad respecto al método de cifrado anterior. Este sistema de descifrado es conocido como ARC.

En 1917 surgió la cifra KRU con curiosas similitudes a las utilizada por los propios franceses, aunque a principios de marzo de 1918 dicha cifra ya rota sistemáticamente por la “Cámara Negra” (“Bureau du Chiffre” francés), fue sustituida por la cifra ADFGX, conocida por los alemanes como “Cifra de Telegrafistas 18”, desarrollada por el coronel Fritz Nebel, perteneciente al departamento de cifra alemán.

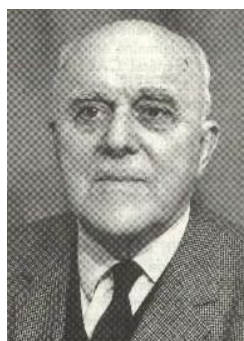



Figura 1. Fritz Nebel, del departamento de cifra alemán.



La cifra ADFGX fue originalmente usada el 5 de marzo de 1918, pero poco después fue sustituida por una cifra más compleja que incluía números. Esta cifra fue denominada ADFGVX inventada, de nuevo, por el coronel alemán Fritz Nebel que tenía por objetivo optimizar el éxito del operador de radio y la seguridad criptoanalista. En ese momento, el ejército francés ya contaba con un dedicado grupo de criptoanálisis (Bureau du Chiffre o “Cámara Negra”). El 4 de abril de 1918, el teniente Georges Painvin pudo identificar dos mensajes con cadenas y ordenaciones de texto idénticas, indicando texto plano con el mismo comienzo y claves lo que le llevó la creación del descifrado de este método. Gracias a esta hazaña el ejército francés se preparó para el ataque realizado por los alemanes el 7 de junio.



Figura 2. Capitán Georges Painvin



Cifra ADFGVX

El cifrado ADFGVX es un criptosistema clásico de clave privada que utiliza un cuadrado de Polybius, de dimensión 6x6, para cifrar un mensaje de texto plano una vez, luego usa una palabra clave para transponer letras del texto encriptado individualmente, agregando dificultad adicional al criptoanálisis. De forma general, es un método que combina un cifrado por sustitución y un cifrado por transposición.

Cuadrado Polybius

Es una especie de tablero de damas que utiliza las letras A, D, F, G, V y X en orden, como identificadores de las filas y las columnas, los cuales forman una matriz y donde cada elemento de la matriz puede ser identificado por su fila y su columna.

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

Figura 3. Ejemplo de cuadrado Polybius ADFGVX



Explicación del método

La cifra ADFGVX al ser un criptosistema de clave privada se utilizará una única clave privada que comparten tanto emisor como receptor. Por otro lado el método requerirá del mensaje que deseamos cifrar así como una clave pública que nos servirá para inicializar el método.

Cifrado

Primer paso, inicialización del cuadrado de Polybius.

Lo primero que llevaremos a cabo será la construcción del cuadrado de Polybius. Para ello, haremos uso de la clave pública establecida por el emisor y el receptor, las 26 letras del alfabeto en inglés y los números del 0 al 9. El procedimiento a seguir para la construcción de este es:

1. Comenzaremos rellenando nuestra matriz por orden de izquierda a derecha y de arriba a abajo, con las letras sin repetición de la clave pública utilizada.
 - a. No se considerará ningún carácter diferente a cualquier letra del alfabeto, así como los espacios. Ejemplo: ?, !, -, _, etc.
2. Una vez completado el paso anterior se rellenará el resto de la matriz con las letras restantes del alfabeto inglés.
3. Por último rellenaremos los huecos que queden vacíos de la matriz con los números del 0 al 9.

Segundo paso, sustitución del mensaje.

Una vez obtenido el cuadrado de Polybius, que en nuestro caso será una matriz cuadrada de dimensión 6x6, sustituiremos cada letra del mensaje por la pareja de letras, fila y columna, que la identifica dentro de la matriz. Por ejemplo, utilizando la matriz representada en la *Figura 3*, la letra A sería sustituida por la pareja de letras VG. Como ejemplo inverso, la pareja de letras AD están sustituyendo a la letra K.



De forma general, usando de nuevo la *Figura 3*, el mensaje “CIFRADO” es sustituido por la cadena “FGDXVVDFVGGFAA”.

Tercer paso, transposición.

Para hacer el cifrado más seguro, una vez sustituido nuestro mensaje utilizaremos una transposición por columnas. Para poder aplicar esta transposición vamos a crear una matriz que tenga tantas columnas como caracteres tenga la clave privada sin repetición.

Una vez creada la matriz deberemos rellenarla introduciendo por filas cada carácter del mensaje sustituido hasta que introduzcamos todo el mensaje. Puede darse el caso en el que nuestro mensaje no sea capaz de completar todas las celdas de la matriz, en caso de que esto ocurra la solución será añadir algún carácter no relevante, en nuestro caso la X, por celda hasta completar toda la matriz.

Una vez completa la matriz haremos una ordenación por columnas en base al orden alfabético de la clave privada utilizada. Posteriormente, reescribiremos de nuevo el mensaje, leyendo por columnas los caracteres resultantes en la matriz (de izquierda a derecha). El mensaje resultante será el mensaje completamente cifrado por el método ADFGVX.



Descifrado

Primer paso, descomponer el mensaje cifrado.

Una vez tenemos nuestro mensaje cifrado para descifrarlo comenzaremos haciendo uso de la clave privada para rellenar una matriz por columnas con el objetivo de deshacer las permutaciones que se le aplicaron al cifrar el mensaje original y por último deshacer la sustitución aplicada al mismo.

Lo primero que haremos será calcular un tamaño de bloque que indicará el número de caracteres con los que rellenaremos cada columna de la matriz. Este tamaño de bloque se calculará como la división de la longitud del mensaje cifrado entre la longitud de la clave privada. Una vez calculado el tamaño de bloque, rellenaremos por columnas la matriz de izquierda a derecha sabiendo que la permutación de las columnas fue realizada en base al orden alfabético de la clave privada. Por tanto, para deshacer dichas permutaciones deberemos permutar de nuevo las columnas para obtener la clave privada. Por ejemplo:

- Clave privada usaremos “SOL”.
- Mensaje cifrado usaremos “FXDFFXXDDXXX”.

L	O	S
F	X	D
F	F	X
X	D	D
X	X	X

Matriz permutada

S	O	L
D	X	F
X	F	F
D	D	X
X	X	X

Matriz con permutaciones deshechas

Una vez deshacemos las permutaciones en base a la clave privada, leemos la matriz por filas reconstruyendo de nuevo el mensaje el cual sería “DXFXFFDDXXX”.



Segundo paso, deshacer la sustitución.

Una vez deshechas las permutaciones llegamos al punto donde tenemos una cadena de caracteres cifrados por sustitución. En este paso necesitaremos construir la matriz de descifrado a partir de la clave pública para deshacer la sustitución realizada en el cifrado. Es de relevancia recordar que se debe construir con la misma clave pública que el emisor ya que por el contrario el mensaje descifrado que obtendremos no tendría que ser el correcto.

Una vez obtengamos esta matriz de descifrado recorreremos el mensaje cifrado por parejas de letras, las cuales identificarán la fila y la columna de la matriz respectivamente, el proceso consistirá en sustituir cada pareja de letras por el carácter que identifiquen en la matriz de descifrado, reconstruyendo así el mensaje original. De forma general, usando de nuevo la *Figura 3*, el mensaje cifrado “FGDXVDFVGGFAA” se corresponde con el mensaje “CIFRADO” ya que “FG” han sustituido a “C”, “DX” han sustituido a “I”, etc.

Además, deberemos tener en cuenta que el mensaje obtenido podrá contener caracteres irrelevantes como pueden ser, por ejemplo, números. Esto es debido a que en el cifrado se podían introducir caracteres adicionales para completar la matriz de permutaciones basada en la clave privada.



Bibliografía

<http://justinkulp.com/wp-content/uploads/2018/07/The-ADFGVX-Cipher.pdf>

<https://www.nku.edu/~christensen/1402%20ADFGVX.pdf>

https://en.wikipedia.org/wiki/ADFGVX_cipher

https://www.acta.es/medios/articulos/comunicacion_e_informacion/052063.pdf

<https://sites.google.com/site/anilandro/06120-adfgx-01>