Garduño Velazquez Alan

Cryptography 3CM5

## Cesar

M = laboratory

C = ODERUDWRUB

Para descifrar este criptograma, básicamente solo hay que hacer recorrido hacia la izquierda en 3 posiciones, ya que el cifrado Cesar se define como “C = p+3 mod 26”, esto implica que se hace un corrimiento a la derecha en 3 posiciones, sin embargo, no hay que olvidar la operación modulo para que tenga sentido.

## Atbash

M = laboratory

C = OZYLIZGLIB

Para descifrar este criptograma, hay que poner el alfabeto sobre el que se escribió y su inverso, ósea que la primera letra sea la última y la ultima la primera ya que este las sustituye, por ende, lo único que hay que hacer es regresar la correspondencia de cada letra.

## Affine

M = laboratory

C = INWJKNCJKV

Para descifrar este criptograma, hay que saber con qué parámetros se cifro, estos parámetros llamados “alfa” y “beta“, para este caso en particular se usó alfa = 9 y beta = 13 ya que el cifrado se define como C = alfa*n+beta mod 26 y para descifrarlo requieres el

inverso multiplicativo de alfa, el cual se puede obtener con el algoritmo extendido de Euclides, una vez conociendo este valor se pude obtener una nueva ecuación donde M = alfaInverso *n +inversoaditivobeta mod 26 y así obtienes el valor correspondiente de la letra.

## Polybios

M = laboratory

C = CAAAABCDDBAADDCDDBED

Para descifrar este criptograma requiere dividirse en dos, el primer criptograma indica la fila y le segundo la columna con la que se cifro, entonces básicamente es busca la correspondencia e ir construyendo el mensaje original.

## Playfair

M = laboratory

C = HFFSPDYFTX

Para descifrar este criptograma se requiere conocer la llave de cifrado, en este caso utilizamos “escom” como llave después construimos su respectiva matriz de cifrado, después de esto hay que buscar las posiciones de la matriz que cumpla con las condiciones para que devuelva un mensaje en claro.

## Desplazamiento

M = laboratory

C = XMNADMFADK

Para descifrar este criptograma, se requiere la llave para este caso se usó 12 y lo que hay que hacer es hacer el desplazamiento inverso, lo que sería, Pn = Cn – Kmod26, donde k es la llave, ósea es k=12, básicamente solo sería hacer un desplazamiento hacia la izquierda.

## Vigenere

M = laboratory

C = PSDCDELQFK

Para descifrar este criptograma se puede usar el análisis de frecuencias, analizando todo el texto cifrado habrá cadenas en común, lo que hay que hacer es encontrar esas cadenas y contar la cantidad de caracteres que hay entre cada una, una vez que ya se tenga eso, tendremos varias y diferentes distancias, dependiendo de cuantas cadenas hayamos encontrado, entonces de todos los valores que se tengan se obtiene su máximo común divisor, y el máximo común divisor que se obtenga es la longitud tentativa de la llave, supongamos que la longitud es de 4, entonces habrá que dividir en 4 subcriptogrmas, por el ejemplo el primeo contendrá la 1,5,9 carácter, la segunda 2,6,10,14, la tercera la ,3,7,11 y la cuarta 4,8,12 y así sucesivamente, hasta que terminemos con la longitud de la cadena , después buscamos las letras que más se repitan, y buscamos la repartición 0,+4,+11 mod 26 que son A, E y L que son las letras más comunes en el idioma inglés, esto puede variar con respecto al idioma, una vez con esto tendremos 4 tuplas, y buscaremos la palabra que tenga sentido y esa será nuestra llave., una vez con la llave podremos buscar las correspondencias respectivas.

## Vernam

M = laboratory

C = áLaD,□ìR@□

Para descifrar el criptograma requerimos conocer la llave de bits con la cual se cifro, conociendo esta lleve, procedemos a obtener los valores en ASCII de los caracteres del criptograma, luego aplicamos la función XOR entre el criptograma y la llave, esto nos dará como resultado un código binario que se transforma en números decimales de 8 bits y a su vez estos serán valor en ASCII del texto plano.

Nota: La plataforma tiene un pequeño detalle, ya que el criptograma devolvió caracteres que no pudieron ser interpretados por mi navegador.

## Hill

M = laboratory

C = XYJVXHHTK

Para descifrar este criptograma requieres conocer la matriz que se utilizó como llave para cifrar, como se sabe esta matriz requiere tener inversa, ósea su determinante tiene que ser distinto de 0, ya teniendo estos elementos obtenemos la inversa de esa matriz, cuando ya se cuente con la inversa de la llave se multiplica por la matriz del texto cifrado, aplicamos algebra modular según el alfabeto que se esté usando y esto nos dará como resultado un matriz con los valores en el alfabeto del texto plano.