INFORME DE TALLER 1

Métodos criptográficos de sustitución

García Grimaldos, Alberto Manuel; Álvarez Caballero, Hernán David
alberto.garcia.2016@upb.edu.co; hernan.alvarez.2014@upb.edu.co
Universidad Pontificia Bolivariana
Seccional Bucaramanga
Octubre 6 de 2019

I. *OBJETIVOS DE DESARROLLO*

Objetivo General

- *Identificar y comprender los procedimientos de criptoanálisis por sustitución que están enmarcados dentro de los métodos criptográficos clásicos, mediante la práctica de ejercicios manuales y algorítmicos, con el fin de sentar una base teórico-práctica para los protocolos de cifrado modernos.*

II. *INTRODUCCIÓN*

En criptografía, un cifrado de sustitución es un método de cifrado mediante el cual los caracteres de un mensaje se reemplazan con texto cifrado, de acuerdo con un sistema fijo; las unidades de caracteres pueden ser letras simples, pares de letras, trillizos de letras, mezclas de las anteriores, etc. El receptor descifra el texto realizando la sustitución inversa. Es importante resaltar que en un cifrado de sustitución las unidades del texto sin formato o mensaje sin cifrar se mantienen en la misma secuencia en el texto cifrado, pero las unidades mismas se alteran.

Cuando hablamos de cifrado por sustitución existen varios tipos, los cifrados monoalfabéticos utilizan una sustitución fija en todo el mensaje, mientras que los cifrados polialfabéticos utilizan una serie de sustituciones en diferentes posiciones en el mensaje, donde se utilizan múltiples alfabetos cifrados.

Para este laboratorio se van a considerar el cifrado Afín, el cual es de tipo monoalfabética-monográfica en el que cada símbolo del alfabeto en el texto en claro es sustituido por un símbolo del alfabeto cifrado, siguiendo la función $(a*m+b)mod(n)$, donde a se la llama constante de decimación, b se la llama constante de desplazamiento, m representa el símbolo del texto y n es el número de símbolos del alfabeto de cifrado; cuando la constante de decimación es uno se puede afirmar que es un cifrado por desplazamiento puro o cifrado de césar.

Además se analiza el cifrado de Playfair que utiliza una matriz de 5 x 5 la cual contiene las 26 letras del alfabeto inglés y comenzando la matriz se encuentra la secuencia correspondiente a la palabra clave.

También trabajos con el cifrado de Vigenere, el cual es polialfabético con una clave k de cifrado y descifrado periodica, se dice que su debilidad es que lo ideal es que el mensaje de texto claro sea igual de extensa a su calve. Utiliza el mismo método que el cifrado de César, agregando una clave k de cifrado y descifrado, que se escribe cíclicamente sobre el mensaje en texto claro.

Sumado a los tres métodos anteriores se aplica el cifrado de Vernam, el cual se basa en la libreta de un solo uso para ejecutar el cifrado, el texto en claro se combina mediante la operación XOR con un flujo de datos aleatorio (idealmente) o pseudoaleatorio del mismo tamaño, para generar un texto cifrado. El uso de datos pseudoaleatorios para generar la clave se presenta como una manera común y efectiva de construir un cifrado.

III. *PROCEDIMIENTO*

Para punto uno, se realiza el cifrado afín con los ***a*** y ***b*** solicitados en el enunciado, rotando los caracteres **b%26** veces, después de haber realizado al decimación (cambiar el carácter original con base en una constante **a**, que altera el código del carácter a rotar .

El punto dos se realiza rotando **-b**, con un coeficiente de decimación de a^{-1} **,** pues esta es la manera correcta de obtener el inverso multiplicativo modular de a.

Para el numeral tres, se asigna el **a** mencionado (59), y se realizan todas las rotaciones posibles (26) para el criptograma.

En el punto cuatro, se asigna la **b** y se opera por fuerza bruta todas las posibles **a** (deben ser impares y coprimas con **n=26**) hasta llegar al resultado por inferencia.

Para el numeral 6 y 7, teniendo las **k** de cifrado, se escriben sin repetir caracteres sobre la matriz del abecedario 5x5 en ese orden específico, luego se escribe el resto del abecedario debajo de la clave ingresada en la matriz.
Se operan las reglas del cifrado de playfair (cuando una tupla de letras está en una misma fila, se selecciona para cada una la letra de la derecha, se selecciona la de abajo si están en la misma columna, se selecciona la que coincide con su fila y la columna de la letra que le acompaña, en caso de no estar en la misma fila ni columna).

En el punto 8, tenemos $C_6^3 = \frac{6!}{(6-3)!\,3!} = \frac{6!}{3!\,3!} = 20$ posibles combinaciones para la clave, pues se deben tomar tres de las seis letras faltantes de la matriz {K, L, T, U, X, Y}.

Para los puntos 9 y 10, se crea la matriz de 26x26 (abecedario x clave cíclica) escribiendo en cada fila el abecedario de forma cíclica, cada vez comenzando en abecedario[numeroDeFila], y se selecciona un carácter de la forma matriz[abecedario][clave], para tomar en orden un carácter que hará parte del criptograma.

En el punto 14, se deben convertir tanto la clave como el mensaje a binario, y pasarlas por una compuerta XOR para generar nuestro criptograma, que será devuelto en hexadecimal para su más fácil lectura. Este método es el único método de cifrado que se puede demostrar matemáticamente seguro, pues al su clave ser igual o más larga que el mensaje original, además de tener una probabilidad de 50/50 de descubrir un bit de la clave, se vuelve incondicionalmente seguro, pues conocer una parte de la clave no significa que esta pueda descubrirse por completo.

El punto 15 se realiza de igual forma que si de cifrar (en lugar de descifrar) se tratase, justo de igual forma que en el punto anterior.

Para el punto 16 se debe realizar el paso a través de la compuerta XOR del criptograma y el mensaje en claro, para hallar la clave.

IV. *ANÁLISIS DE RESULTADOS Y CONCLUSIONES*

Método de Afin

Teniendo en cuenta que la fórmula de cifrado es: $Ci=a\cdot Mi+b \bmod(n)$, y la constante de decimación no cumple la condición de ser impar, al ser cero (cero es un número par), convierte la variable en cero y queda solo los caracteres de desplazamiento, haciendo que el mensaje “ATACAR PREARL HARBOR AHORA” se transforme a: “WWWWWWWWWWWWWWWWWW

WWW" ademas de la necesidad de que a sea diferente de cero también está la limitante que debe ser impar haciendo que (a,b) = (6,0) tampoco sea viable.

Para (a,b) = (3,92), se obtiene el criptogramas C2 = OTOUONHNAONVJONRENOJENO.

Se puede evidenciar el descifrado del criptograma "WXANVVWRFWFJEPEZC" del enunciado dos, con **a=11** y **b=56**, que arroja como resultado "EXCELLENTE TRABAJO".

Realizando el descifrado con el **a** dado, y con todas las posibles rotaciones, se encuentra el mensaje "**ATACAREMOSHOY**", con a = 59 y **b = 16,** c= QTQEQFSWKMNKC.

Realizando el descifrado con un b dado, y con todas las 12 posibles números impares hasta el 26 para a se llegó al mensaje "HOY HAY QUE ATACAR" con a = 17 del criptograma c = HWKHSKEUISDSASV.

Método de Playfair

Después de cifrar mediante las reglas de playfair, se puede ver que la cadena cifrada "**LAAUREIN FUE ARRESTADO"** cambia su resultado si se cifra con las llaves "**JACOME**" y "**CRIPTOGRAFIA**", pues estas no tienen los mismos caracteres ni su mismo orden. Se puede decir que cifrar con la clave "claaaaaaaaaaaaaaaaaaaaaaaaaaaaveeeeeeeeeeeeeeee" arrojaría el mismo resultado que cifrar con la clave "clave" o "clalalalalalalaveveveveveve", ya que para la matriz del abecedario solo importan los caracteres sin repetición, ya que estos darán el orden de la matriz, pero no cambiarán la ejecución de las reglas criptográficas. Es así que podemos decir que cifrar con las claves "abcdefghijklmnopqrstuvwyxz" arrojará el mismo resultado que dicha clave con repeticiones de los caracteres de la misma.

```
Enter the key: CRIPTOGRAFIA
Enter the text to be encrypted: LAAUREIN FUE ARRESTADO
Playfair encryption result: HBIHNTHR SGNLGIWI KNIBMD
```

```
Enter the key: JACOME
Enter the text to be encrypted: LAAUREIN FUE ARRESTADO
Playfair encryption result: KCWCQSHE TNQGBWWS DQROFC
```

De esta forma obtenemos el criptograma "KCWCQSHE TNQGBWWS DQROFC" y "HBIHNTHR SGNLGIWI KNIBMD" con las claves "JACOME" y "CRIPTOGRAFIA" respectivamente.

Se puede observar el texto siendo descifrado con la clave curriculo, lo que nos deja el mensaje en claro "APRENDILOCORXRECTO", la cual posteriormente cifraremos de nuevo con distintas claves para demostrar parte de las fallas de este método de cifrado.

```
Enter the key: CURRICULO
Enter the cryptogram to be decrypted: GWLBSOLC FOBCRBOL NE
Playfair decryption result: APRENDILOCORXRECTO
```

Para el numeral 7, se usó la clave "curriculo", pero añadiendo repeticiones del caracter "c" al final de la misma, para crear claves que generen el mismo criptograma.

```
Enter the key: curriculoc
Playfair encryption result: GWLBSOLC FOBCRBOL NE
Enter the key: curriculoccccccccccccccccc
Playfair encryption result: GWLBSOLC FOBCRBOL NE
Enter the key: curriculoccc
Playfair encryption result: GWLBSOLC FOBCRBOL NE
Enter the key: curriculocccccc
Playfair encryption result: GWLBSOLC FOBCRBOL NE
Enter the key: curriculocccccccccc
Playfair encryption result: GWLBSOLC FOBCRBOL NE
Enter the key: curriculocccccccccc
Playfair encryption result: GWLBSOLC FOBCRBOL NE
Enter the key: curriculocccccc
Playfair encryption result: GWLBSOLC FOBCRBOL NE
Enter the key: curriculocccccccccccccc
Playfair encryption result: GWLBSOLC FOBCRBOL NE
Enter the key: curriculocccccccccccccc
Playfair encryption result: GWLBSOLC FOBCRBOL NE
Enter the key: curriculocccccccccccccccc
Playfair encryption result: GWLBSOLC FOBCRBOL NE
```

Lo que nos da las siguientes claves:
curriculo
curriculoc
curriculocc
curriculoccc
curriculocccc
curriculoccccc
curriculocccccc
curriculoccccccc
curriculocccccccc

Esto ocurre porque la clave solo altera la matriz del abecedario una vez por cada caracter, es decir, los caracteres repetidos en la clave no alterarán el método de cifrado.

Método de Vigenere

Para el numeral 9 se cifró el texto mediante el cifrado de Vigenere " *WE ARE THE CHAMPIONS* ", el resultado con la clave

- *K*= "*SEDENTARIO*" fue *C*= OIDVRMHVKVSQSMBGS
- *K = "ARCHIVO"* fue *C*= WVCYMOVETJHUKWOEU
- *K = "ARAR"* fue *C*= WVAIEKHVCYADPZOES

En el numeral diez con *K= "LLAMARADA"* y *C= "ACEBAIARSALRMLRPHLPL"*, se obtiene el mensaje *"PREPARAOS PARA LA PELEA"*.

Dado que la clave es cíclica la llave "ARAR" contiene la clave "AR", por ende, es indiferente usar una o la otra; siempre se obtendra el criptograma "WVAIEKHVCYADPZOES".

Se nos pide, en el enunciado 12, comprar el cifrado de Cesar con k = 19 y el de Vigenere con k = T, el mensaje que se utilizó es "PRUEBADECOMPARACION", para los dos metodos de cifrado se obtiene IKNXUTWXVHFITKTVBHG; el resultado se debe a que el cifrado Vigenere utiliza como la clave un solo carácter que equivale a 19, entonces se puede ver como un cifrado Cesar.

Numeral 13, tanto Vigenere utilizando una clave de longitud uno como el cifrado Afin por desplazamiento puro se podrían llamar cifrado de Cesar, esto debido a que se convierten en algoritmos de sustitución simple, cada carácter está siendo desplazado unas cantidad k o b veces.

Método de Vernam

Para el numeral catorce se cifró el texto mediante el cifrado de Vigenere " *SOMOS LOS REYES DE PERSIA* ", el resultado con la clave

- *K*= "*ESTA ES LA PRIMERA LLAVE1*" fue *C*= 161C 190E 161F 0312 0217 1008 1616 041C 0913 050C 70
- *K = "LA SEGUNDA LLAVE2 ES ESTA"* fue *C*= 1F0E 1E0A 1419 0117 1309 1504 0501 7715 1617 001D 00

En el numeral quince con K= "VIVAELREINODEARISTOTELA" y C= "171D1702041E1708061D0A0A09001F081 7061A13040800", se obtiene el mensaje "ATACAREMOS EN LA MADRUGADA".

Finalmente en el numeral 17 se dice que la clave tiene una longitud 3 y se compone sólo de vocales que no se repiten se puede decir que existen C(5,3)=60 combinaciones: 'aei','aeo','aeu','aie','aio','aiu','aoe','aoi','aou','aue','aui','auo','eai','eao','eau','eia','eio','eiu','eoa','eoi','eou','eua','eui','euo','iae','iao','iau','iea','ieo','ieu','ioa','ioe','iou','iua','iue','iuo','oae','oai','oau','oea','oei','oeu','oia','oie','oiu','oua','oue','oui','uae','uai','uao','uea','uei','ueo','uia','uie','uio','uoa','uoe','uoi', probando las posibles claves se encontró el mensaje: VOLAR EL OLEODUCTO A LAS 0600 con la clave "UAIUAIUAIUAIUAIUAIUAI".

V. *CONCLUSIONES*

Cifrar con el método de playfair tiene la desventaja de que la alteración de la clave utilizando repeticiones de sus caracteres, no altera el resultado del criptograma final (poca propagación).

El cifrado de César puede ser cualquier método criptográfico por medio del cual solamente se realice la rotación de los caracteres por un factor **b** constante.

El carácter cíclico de las claves puede llegar a ser una vulnerabilidad en el cifrado, pues el

criptograma final podría llegar a ser criptoanalizado más fácilmente.

VI. *REFERENCIAS BIBLIOGRÁFICAS CONSULTADAS*

[1] Jorge Ramió Aguirre, Aplicaciones criptográficas. Libro guía de la asignatura de Seguridad Informática. Universidad Politécnica de Madrid. Enero 1998.

[2] Bruen, Aiden A. & Forcinito, Mario A. (2011). Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century. John Wiley & Sons. p. 21. ISBN 978-1-118-03138-4.

[3] Gaines, Helen Fouché (1956) [1939], Cryptanalysis / a study of ciphers and their solutions, Dover, ISBN 0-486-20097-3. Disponible: https://archive.org/details/cryptanalysis00hele/page/n1