UNIVERSIDAD GALILEO
FACULTAD DE INGENIERÍA EN SISTEMAS, INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN

CÓDIGOS LINEALES EN CRIPTOGRAFÍA

Integrantes:

Santos Méndez, Manuel José 18001167
Palma Salvatierra, Harim Abdalá 18001882
Flores Martínez, Jair Alexander 18002715

Guatemala, 19 de septiembre de 2019

Cifrado Hill

1. Introducción

La criptografía es definida por la Real Academia Española (RAE) como: .ªrte de escribir con clave secreta o de un modo enigmático", siendo enigmático definido como artificiosamente encubierto para que sea difícil de entender o interpretar.

A pesar de que la materia es asociada con gran frecuencia con asuntos militares, la criptografía llegó a ser un área importante en los negocios. Las grandes empresas, que procesan enormes cantidades de datos computadorizados, deben protegerse constantemente contra lo que se llama .ªspionaje industrial", esto es, el robo de información importante por los competidores.

En la actualidad, existen muchas técnicas complejas desarrolladas para garantizar la posibilidad de transmitir grandes cantidades de información en forma confidencial.

1.1. Historia

En criptografía, el cifrado por sustitución es un método de cifrado por el que unidades de texto plano son sustituidas con texto cifrado siguiendo un sistema regular; las "unidades"pueden ser una sola letra (el caso más común), pares de letras, tríos de letras, mezclas de lo anterior, entre otros.

El receptor descifra el texto realizando la sustitución inversa. Existen diversos tipos de cifrados por sustitución. Si el cifrado opera sobre letras simples, se denomina cifrado por sustitución simple, si opera sobre grupos de letras se denomina poligráfico. En criptografía clásica, el Cifrado Hill es un cifrado de sustitución poligráfica basado en el álgebra lineal. Inventado por Lester S. Hill en 1929, fue el primer cifrado poligráfico que era práctico para operar sobre más de tres símbolos inmediatamente. En su época no tuvo mucho éxito por la dificultad operacional (Se diseño una máquina para este cifrado pero no pudo competir con máquinas como Enigma o Hagelin). Actualmente este sistema se puede implementar fácilmente en los ordenadores que tenemos a nuestro alcance.

1.2. Encriptación

Cada letra está representada por un número. A menudo el esquema sencillo A = 0, B = 1, ..., Z = 25 es utilizado, pero esto no es una característica esencial del cifrado. Para encriptar un mensaje, cada bloque de n letras (considerados como un vector) está multiplicado por una matriz invertible (n × n) (modular 26). Para desencriptar el mensaje, cada bloque es multiplicado por el inverso de la matriz usada para la encriptación. La matriz usada para la encriptación es la llave de cifrado, y tiene que ser escogida aleatoriamente del conjunto de matrices invertibles (n × n) (modular 26). El cifrado puede naturalmente, ser adaptado a un alfabeto representado con cualquier orden numérico y/o cambiando el número (modular 26) siempre y cuando la matriz (n × n) (modular x) sea invertible. Considerar el mensaje 'ACT', y la clave de abajo (Matriz en letras es GYBNQKURP):

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

'A' es 0, 'C' es 2 y 'T' es 19, con lo que el mensaje es el vector:

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

Por ello el vector cifrado está dado por:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} (31) mod(26) \\ (216) mod(26) \\ (325) mod(26) \end{pmatrix} = \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix}$$

El cual corresponde al texto 'FIN'. Cada letra ha cambiado, obteniendo un vector completamente distinto.

1.3. Desencriptación

Para desencriptar, transformamos el texto cifrado en un vector, entonces sólo tendrás que multiplicar por la matriz inversa de la matriz clave (IFKVIVVMI en letras). (Hay métodos estándares para calcular la matriz inversa; ver matriz invertible para detalles.). Encontramos que, módulo 26, el inverso de la matriz usada en el ejemplo anterior es:

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}^{-1} = \begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} (mod 26)$$

Tomando el ejemplo anterior de texto cifrado 'POH', tenemos que:

$$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} = \begin{pmatrix} 260 \\ 574 \\ 539 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} (mod 26)$$

El cual nos da como resultado 'ACT', tal y como esperábamos.

No hemos hablado todavía sobre las dos complicaciones que existen al elegir la matriz de encriptar. No todas las matrices tienen un inverso (ver matriz invertible). La matriz tendrá un inverso si y sólo si su determinante no es cero. También, en el caso del Cifrado de Hill, el determinante de la matriz de encriptar no tiene que tener ningún factor común con la base modular. Así, si trabajamos módulo 26 como arriba, el determinante tiene que ser no-cero, y no tiene que ser divisible por 2 o 13. Si el determinante es 0, o tiene factores comunes con la base modular, entonces la matriz no puede ser utilizada en el Cifrado de Hill y otra matriz tiene que ser escogida. Afortunadamente, las matrices que satisfacen las condiciones para ser utilizadas en el Cifrado de Hill son bastante comunes.

Para nuestro ejemplo, la matriz clave:

$$\begin{vmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{vmatrix} = 6(16*15-10*17)-24(13*15-10*20)+1(13*17-16*20) = 441 = 25(mod 26)$$

Así que, módulo 26, el determinante es 25. Éste tiene no factores comunes con 26, así que esta matriz puede ser utilizada para el Cifrado de Hill.

El riesgo del determinante habiendo factores comunes con el módulo puede ser eliminado convirtiendo el módulo en primo. Consiguientemente una variante útil del Cifrado de Hill añade 3 símbolos extras (como un espacio, un punto y un signo de interrogación) para aumentar el módulo a 29.

1.4. Ventajas y Desventajas

El cifrado de Hill termina siendo un sistema inseguro en su aplicación. Utilizando métodos de álgebra lineal en un "ataque con texto claro conocido" puede romperse el código y descubrir la matriz clave de encriptado. Un ataque con texto claro conocido significa que el analista que quiere romper el código dispone de un ejemplo de "texto en claro", es decir, de un mensaje original, con el correspondiente mensaje cifrado.

Se debe distribuir la clave en secreto y esto hace un poco inmune a este método ya que, la clave tiende a ser tan valiosa como todos los mensajes a encriptar. Si la clave se ve comprometida, queriendo decir que esta sea robada, averiguada, extorsionada, sobornada, etc...) todos los textos podrán ser desencriptados y se puede suplantar la identidad del emisor para el envío de mensajes falsos.

Las ventajas en comparación a otros métodos es que debido a que utiliza algoritmos simétricos generalmente, tiende a ser más rápido que sistemas de clave publica. Cuando el tamaño de la clave es grande y sin método para conseguir el texto original y codificado se vuelve "seguro".

Si con el sistema de Hill se cifran bloques de 8 caractéres, incluso en un cuerpo tan pequeño como n = 27 el espacio de claves aumenta de forma espectacular, comparable con DES. Si el módulo de cifra es un primo p, entonces el número de claves válidas es cercano al máximo posible de forma exponencial.

2. Referencias

Asale, Rae -. Diccionario De La Lengua Española - Edición Del Tricentenario.
https://dle.rae.es/.
Cifrado Hill. Wikipedia, Wikimedia Foundation, 9 Aug. 2019.
https://es.wikipedia.org/wiki/Cifrado_Hill.
Criptografía. Wikipedia, Wikimedia Foundation, 11 July 2019.
https://es.wikipedia.org/wiki/Criptografia
Tomé, César. "Criptografía Con Matrices, El Cifrado De Hill." Cuaderno De Cultura Científica, Patrocinado Por: Dinahosting, 11 Jan. 2017.
https://culturacientifica.com/2017/01/11/criptografia-matrices-cifrado-hill/
Grossman, Stanley I. Aplicaciones De a´lgebra Lineal. Mc Graw-Hill, 1996.