PROYECTO

CRIPTOGRAFÍA

La criptografía se trata del envío y recepción de mensajes codificados. El mensaje puede ser decodificado por el receptor solo si conoce el algoritmo con el cual fue codificado. Uno de los modos más antiguos es convertir las letras del mensaje en un número representando su posición en el alfabeto (en español hay 27 caracteres):

HOLA = 816121

Sin embargo luego de varios intentos, cualquiera podría darse cuenta del modo en el cual se codificó. La dificultad podría aumentar si sumamos una cantidad fija al código de cada letra y escribimos el respectivo mensaje. Por ejemplo, si sumamos 5 a cada código:

HOLA = 1321176 = MTPF

Aritmética módulo n

Este último método tiene el inconveniente que se sale del rango de códigos del alfabeto, por ejemplo, la letra Z con código 27, al sumarle 5 se obtiene 32. ¿Con qué letra asociamos el código 32? Esto se puede resolver utilizando la aritmética módulo-n, en este caso, módulo 27:

$$x \equiv y \Leftrightarrow \exists k \in \mathbb{Z} \ \ |x - y| = 27k$$

Así, 31 es equivalente a 4, ergo corresponde al caracter D.

Proposición:

Sea $\mathbb{Z}_K$ el conjunto de números enteros no negativos comprendidos entre el 0 y el K–1.

Si los escalares α los tomamos del mismo conjunto $\mathbb{Z}_K$, entonces el conjunto $\langle \mathbb{Z}_K, \oplus, \alpha \odot \rangle$ con las operaciones de suma y multiplicación por escalar convencionales constituyen un espacio vectorial.

Ejercicio:

Demuestre la validez de la proposición dada.

El Codificador de Hill

Suponga que se desea codificar los caracteres no de uno en uno sino agrupando de par en par:

HOLA = HO - LA

Entonces se puede construir una matriz A de 2x2 tal que

$$\mathbf{c} = \mathbf{H}.\mathbf{l}\text{, o}$$

$$\begin{pmatrix} c1 \\ c2 \end{pmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{pmatrix} l1 \\ l2 \end{pmatrix}$$

donde el par ordenado $\mathbf{l}=(l1, l2)^T$ corresponde a un grupo de 2 letras originales $l1$, $l2$; y el resultado del la multiplicación matricial es el par de letras codificadas $(c1, c2)^T$.

Si la matriz **H** es invertible, entonces la decodificación se puede obtener como:

$$\mathbf{H}^{-1}\begin{pmatrix} c1 \\ c2 \end{pmatrix} = \begin{pmatrix} l1 \\ l2 \end{pmatrix}$$

De este modo, intentar romper el código significa intentar adivinar la matriz invertible A.

Ejercicio:

Investigue cómo se soluciona el inconveniente de una palabra que no tiene un número par de letras, si la matriz $\mathbf{H}_{2X2}$ puede codificar solo pares ordenados de letras.

CODIFICADOR DE HILL, 1929

De acuerdo a lo estudiado, para diseñar un codificador de Hill, se requiere que la matriz **H** sea invertible, además los elementos de los vectores perteneces a un espacio $\mathbb{Z}_K$ convenientemente elegido para representar a todos los caracteres necesarios para una transmisión. Por ejemplo, si **H** es de 2x2, pueden existir 27^4 modos de construir **H** con elementos de $\mathbb{Z}_{27}$.

REFERENCIAS:

L.S. Hill Cryptography in an algebraic alphabet. *American Mathematical Monthly*, **36** (1929), 306-312.

Entregables:

- Se debe presentar dos secciones. La primera parte consta de la resolución de los ejercicios planteados, respondiendo a las preguntas dadas.
- En la segunda sección debe constar exclusivamente el análisis del problema del Codificador de Hill, 1929, proveyendo respuestas a las siguientes cuestiones:

1. Calcular las condiciones que debe cumplir la matriz **H** para que sea invertible, considerando que sus elementos provienen de $\mathbb{Z}_K$.
2. Si modificamos el espacio $\mathbb{Z}_K$ para incluir caracteres mayúsculos, minúsculos, diez dígitos y el espacio, ¿Cuántos modos de construir H existen? De estas, qué porcentaje es invertible?
3. Si un cliente le pide que diseñe un codificador de Hill pero utilizando una matriz

$\mathbf{H}_{3X3}$, ¿considera usted más seguro o menos seguro que con una matriz $\mathbf{H}_{2X2}$? Justifique su respuesta.

4. Diseñe un ejemplo de codificador de Hill con $\mathbf{H}_{2X2}$ y con $\mathbf{H}_{3X3}$, y codifique en ambos casos la frase:

   Hola mundo

   Y utilice las respectivas inversas para decodificar el resultado.
5. Suponga que usted conoce la frase original "Hola mundo" y también conoce su codificación, pero no conoce la matriz **H**, ¿es posible determinar **H** utilizando esa información?
6. Diseñe un diagrama de flujo de trabajo para un codificador de Hill que utilice el espacio $\mathbb{Z}_K$ del numeral 2), y que procese los caracteres en grupos de 3.
7. Basado en la información dada, y en información adicional que usted investigue, ¿Cuán factible es para usted construir o programar un codificador de Hill?
8. Si leyó o consultó un libro o artículo, debe poner al final del documento una sección Bibliografía o Referencias y hacer una lista de cada trabajo consultado, incluyendo título, autor(es), Capítulo/Volumen, páginas.

NOTA: Es lícito apoyarse en la tecnología, pero si necesita utilizar un software o calculadora (Matlab®, Phyton, etc), o algún sitio de resolución de matrices online (Online Matrix Calculator de blue-bit), debe ser indicado en el documento a entregar, planteando la fórmula teórica, e indicando si se utilizó para resolver esa ecuación; y repitiendo la indicación para cada una de las ecuaciones así resueltas.