MATEMÁTICA DISCRETA (MI)
TRABAJOS EN GRUPO

CRIPTOGRAFÍA

La criptografía (del griego κρύπτω krypto, «oculto», y γράφω graphos, «escribir», literalmente «escritura oculta») es el arte de escribir con clave secreta o de un modo enigmático.

Las comunicaciones confidenciales o secretas se han utilizado desde tiempos antiguos, creándose procedimientos (sistemas de cifrado) para ocultar información de forma que sólo pudiera ser leída correctamente por aquellos a quienes se dirige. También se han ideado sistemas (criptoanálisis) para descifrar los mensajes interceptados.

El objetivo de los trabajos es presentar una breve historia de la criptografía. El primer tema abarcará la historia desde la Antigüedad hasta 1900. El segundo tema la criptografía durante las Guerras Mundiales y el tercer tema presentará los avances criptográficos de los últimos sesenta años

Los temas son amplios por lo que precisamos algunos de los puntos que necesariamente deben aparecer en los trabajos:

- Métodos de transposición y de sustitución.
- Julio César
- Análisis de frecuencias.
- Cifrado polialfabético (Vigènere)
- Criptoanálisis del cifrado polialfabético (Babbage y Kasiski)

- ❖ Criptografía en la Primera Guerra Mundial.
- ❖ Segunda Guerra Mundial.
  - o Máquinas mecánicas y electromecánicas de cifrado
  - o Enigma
  - o Criptólogos polacos y británicos. (Bletchley Park)

- ▪ Teoría de la Comunicación. (Shannon)
- ▪ DES y AES
- ▪ Claves públicas versus claves privadas (Diffie y Hellmann)
- ▪ Funciones de un sólo sentido.
- ▪ Sistema RSA
- ▪ Firma digital.
- ▪ PGP
- ▪ Criptografía cuántica

Referencias

S. Singh, “Códigos secretos”, Debate, 2000.
Las aplicaciones de las congruencias y los números primos a la criptografía aparecen en casi todos los textos de Matemática Discreta, por ejemplo, en los indicados en la bibliografía de la asignatura MD I.

Páginas web

Página web del libro citado de Simon Singh: https://simonsingh.net/books/the-code-book/the-book/
“The Code Book” en CD-Rom https://simonsingh.net/cryptography/crypto-cd-rom/

http://en.wikipedia.org/wiki/Cryptography
http://es.wikipedia.org/wiki/Historia_de_la_criptografía
http://en.wikipedia.org/wiki/Quantum_cryptology