Introducción a la criptología

Diego Prieto Gual
Universitat de València
dieprie@alumni.uv.es

December 13, 2017

La criptología (del griego krypto: 'oculto' y logos: 'estudio') es la disciplina que se ocupa de los problemas teóricos relacionados con la seguridad en la transmisión de mensajes en clave. Durante muchos años ha sido necesario emplear métodos de cifrado para comunicarse.

En este trabajo vamos a ver las matemáticas que hay detrás de esta disciplina, así como las diferencias entre los llamados 'Criptosistemas clásicos' y los sistemas de clave pública, que son los que se utilizan hoy en día para garantizar la seguridad informática.

References

[1] E. García, M.A. López. y J.J. Ortega, *Una introducción a la criptografía*, Universidad de Castilla la Mancha (2005).

[2] S.I. Grossman, *Aplicaciones de Álgebra Lineal*, Grupo Editorial Iberoamericana (1988).

[3] J. Ramió Aguirre, *Introducción a la seguridad informática y criptografía clásica*, Universidad politécnica de Madrid (2016).