



## Criptografía (Spanish Edition)



**Descargar**



**Leer En Linea**

[Click here](#) if your download doesn't start automatically

# Criptografía (Spanish Edition)

*Luis Espino*

## **Criptografía (Spanish Edition)** Luis Espino

La criptografía es escribir de manera oculta, considerada un arte para unos y una ciencia para otros. Todo depende del enfoque con que se trate, si la escritura se oculta de manera peculiar sería un arte, pero si se usan los fundamentos teóricos de Shannon y los algoritmos modernos sería una ciencia.

Aunque el desarrollo de la criptografía se viene dando hace más de 4000 años, el desarrollo de la criptografía moderna tiene menos de 60 años, en los cuales, el avance ha sido muy productivo para construir los sistemas criptográficos más seguros de la historia.

La seguridad informática cubre tanto la privacidad y la integridad de los datos en un sistema de comunicación mediante la criptografía. Sin embargo, cada uno de estos elementos tiene partes, de las cuales, han sido difíciles de proteger. Por ejemplo, el intercambio seguro de llaves sucedió hace 40 años con la propuesta de Diffie y Hellman referente a la criptografía asimétrica o de llave pública. La mayoría de protocolos de seguridad surgieron en los 1990's con la aparición de Internet. En 2001 aparece AES como un estándar seguro de cifrado. Durante los últimos 15 años se han ido mejorando los algoritmos y protocolos gracias al criptoanálisis.

El futuro de la criptografía es incierto, la criptografía se ha ido desarrollando por las necesidades de los usuarios, en la actualidad, las exigencias son altas y es necesaria la búsqueda de otros mecanismos de cifrado aparte del simétrico y asimétrico. Por ejemplo, la criptografía de llave pública tiene como fundamento de seguridad que no hay algoritmos eficientes para la factorización de números grandes para quebrantar el sistema. Cuando la tecnología alcance ese nivel, se tendrán que idear nuevos mecanismos. La criptografía de curva elíptica y la criptografía cuántica han sido temas de estudio reciente.

Otro aspecto a considerar es el espionaje, hay de tipo ilegal pero también hay de tipo legal. Algunos autores afirman que con políticas de gobierno contrarias a la privacidad no tiene sentido hacer sistemas criptográficos más robustos.

En cuanto al contenido de este libro, primero se introduce el concepto de la criptografía, sus bases teóricas y una breve historia. Luego se describen los sistemas de cifrado clásicos más importantes que sirvieron como base para definir la criptografía moderna.

Respecto de la criptografía moderna, esta se separa en la criptografía simétrica y asimétrica, por el mecanismo de las llaves. En cuanto a la criptografía simétrica, se exponen los sistemas de cifrado por bloques tales como las redes de Feistel, DES y AES, también los sistemas de cifrados RC6 y Serpent. Luego, se hace una introducción a las funciones hash criptográficas y la autenticación de mensajes. En cuanto a la criptografía asimétrica, se exponen los algoritmos Diffie y Helman, y RSA.

Luego se describen los principales protocolos de seguridad en Internet, estos protocolos utilizan diferentes algoritmos, como los antes mencionados, dependiendo de las necesidades. Principalmente, la firma digital, la autenticación, los protocolos de transporte y las redes inalámbricas.

Finalmente, se hace una recopilación de la principal codificación criptográfica en los lenguajes Java, Python y PHP, tanto de la criptografía simétrica como asimétrica o de llave pública para que el lector tenga una idea de su implementación.

 [Descargar Criptografía \(Spanish Edition\) ...pdf](#)

 [Leer en línea Criptografía \(Spanish Edition\) ...pdf](#)

**Descargar y leer en línea Criptografía (Spanish Edition) Luis Espino**

---

Format: Kindle eBook

Download and Read Online Criptografía (Spanish Edition) Luis Espino #Z17TLMUIV53

Leer Criptografía (Spanish Edition) by Luis Espino para ebook en líneaCriptografía (Spanish Edition) by Luis Espino Descarga gratuita de PDF, libros de audio, libros para leer, buenos libros para leer, libros baratos, libros buenos, libros en línea, libros en línea, reseñas de libros epub, leer libros en línea, libros para leer en línea, biblioteca en línea, greatbooks para leer, PDF Mejores libros para leer, libros superiores para leer libros Criptografía (Spanish Edition) by Luis Espino para leer en línea. Online Criptografía (Spanish Edition) by Luis Espino ebook PDF descargarCriptografía (Spanish Edition) by Luis Espino DocCriptografía (Spanish Edition) by Luis Espino MobipocketCriptografía (Spanish Edition) by Luis Espino EPub  
**Z17TLMUIV53Z17TLMUIV53Z17TLMUIV53**