



UNIVERSIDAD DE SEVILLA

Dpto. Matemática Aplicada I

# Criptografía

Optativa de 5º curso

2º Cuatrimestre

INGENIERO EN INFORMÁTICA

## Introducción

Uno de los temas que ha adquirido recientemente más notoriedad es el de la seguridad y privacidad en la transmisión de datos. En especial, el auge de las comunicaciones por ordenador ha conseguido que la seguridad no solo sea un asunto militar o de organizaciones financieras, sino que interese a todo el mundo.

El objetivo del curso es introducir las técnicas básicas de *Criptología*. Se inicia con un repaso elemental de los métodos clásicos de codificación y se estudian sus debilidades. A continuación se pasa al estudio de los modernos sistemas, con especial interés en los de *clave pública* y a sus implementaciones. Se insiste especialmente en su utilidad para la seguridad en redes de ordenadores y otros aspectos relacionados.

## Programa

### Algunos criptosistemas simples

Desplazamiento. Sustitución. Claves afines. La clave de Vigenère. El método de Hill. Sistemas de permutación. Códigos '*stream*'.

### Criptografía

Criptografía de la clave afín. Criptoanálisis de las claves de sustitución. Criptoanálisis del sistema de Vigenère. Un ataque conocido usando texto fuente de la clave de Hill. Criptoanálisis del cifrado '*stream*' basado en LFSR.

### Teoría de Shannon

Secreto perfecto. Entropía. Códigos de Huffman y entropía. Propiedades de la entropía. Claves indeseadas y distancia de unicidad. Criptosistemas producto.

### El sistema DES

Introducción. Descripción de DES. Ejemplos. La controversia sobre DES. DES en la práctica. Modos de operación. Criptoanálisis diferencial. Notas y referencias.

### El sistema RSA y factorización

Introducción a los sistemas criptográficos de clave pública. Repaso de conceptos de teoría de números. El criptosistema RSA. Implementando RSA. Test de primalidad probabilístico. Ataques a RSA. El exponente de descryptación. Informaciones parciales. El criptosistema de Rabin.

Algoritmos de factorización. La factorización en la práctica.

### Otros criptosistemas de clave pública

El sistema de ElGamal y el logaritmo discreto. Algoritmos para el logaritmo discreto. Seguridad del logaritmo discreto. Cuerpos finitos y sistemas de curvas elípticas: cuerpos de Galois y curvas elípticas. El sistema de la mochila. El sistema de McEliece.

## BIBLIOGRAFIA

Stinson, Douglas R.  
*Cryptography. Theory and Practice.*  
CRC Press. 1995.

Schneier, Bruce  
*Applied cryptography.*  
John Wiley & Sons 1996.

Konheim, Alan.  
*Cryptography: A primer.*  
John Wiley & Sons 1981.

Welsh, Dominic.  
*Codes and Cryptography.*  
Clarendon Press - Oxford 1988.

van Tilborg, Henk C. A.  
*An introduction to Cryptology.*  
Kluwer Academic Publishers 1987.

Koblitz, Neal.  
*A course in number theory and Cryptography.*  
Springer-Verlag 1987.