CP4: Daniel Penazzi (UNC).

Aplicaciones de los cuerpos finitos a la criptografía de clave simétrica.

Luego de una introducción a la criptografía de clave simétrica y cifradores de bloque, se explicarán algunos métodos de construcción de cifradores de bloque y cómo los cuerpos finitos ayudan para proveer resistencia contra ataques poderosos como el criptoanálisis diferencial, el cual también será explicado brevemente.