Matemàtica aplicada a la criptografia

El grup de recerca de Matemàtica Aplicada a la Criptografia centra la seva activitat a l'àmbit de la criptografia i les eines matemàtiques en les quals es fonamenta. Es tracta d'un activitat de caire interdisciplinari, què inclou des de la recerca en Combinatòria o Teoria de Nombres, des del punt de vista de la seva aplicació a la Criptografia, fins a l'avaluació de les prestacions dels protocols criptogràfics, des del punt de vista de la implementació i l'eficiència. L'anàlisi rigorosa de la seguretat del protocols és una altra de les tasques de recerca del nostre grup.