Generalised Rijndael

Sergi Blanch-Torné
Escola Politècnica Superior,
Universitat de Lleida. Spain.
sblanch@alumnes.udl.es

Ramiro Moreno Chiral
Departament de Matemàtica.
Universitat de Lleida. Spain.
ramiro@matematica.udl.es

2012-08-20

Abstract

This is the abstract

1 Introduction

2 Approach to the Rijndael Schema

3 Generalising the schema

3.1 key expansion

3.2 subBytes

3.3 shiftColumns

3.4 mixColumns

3.5 addRoundKey