CRIPTOGRAFIA
MA II - FIB

Advanced Encryption Standard (AES)

Entrega

1. **AES**

   (a) Canviem la funció **SubBytes** per la identitat, i.e. **SubBytes(x)=x**.
   Sigui M_i igual a M excepte en el bit i; M_j igual a M excepte en el bit j; M_{ij} és igual a M excepte en els bits i, j; C_i el resultat de xifrar M_i amb la clau K; C_j el resultat de xifrar M_j amb la clau K; C_{ij} el resultat de xifrar M_{ij} amb la clau K.
   Feu un programa per comprobar que $C = C_i \oplus C_j \oplus C_{ij}$ per qualsevol i, j, i que això no pasa si agafen la funció **SubBytes** original.

   (b) Canviem la funció **ShiftRows** per la identitat. Quins efectes té aquest canvi al xifrar un bloc? Feu un programa que mostri aquest efecte.

   (c) Canviem la funció **MixColumns** per la identitat. Quins efectes té aquest canvi al xifrar un bloc? Feu un programa que mostri aquest efecte.

Referències

Federal Information Processing Standards Publication (FIPS) 197: Advanced Encryption Standard (AES)