

# **Practico 1 de Criptografía 2016**

## **Ejercicios Elegidos para el Practico Final:**

1) Ud. intercepta un mensaje escrito por alguien que Ud. sabe esta usando un Código Hill 3 x 3.

El mensaje interceptado es:

XFW SRG YAY XTM LKD UZI CHI S XK ÑDE RIS ÑKL LBU NTB EJB OBB  
UTO AU Y

Un colaborador suyo encuentra en el lugar de transmisión la primera parte del mensaje, que comienza:

NOS DESCUBRIE

¿Que dice el resto del mensaje?

6) Tomar alguno (o varios, si quiere) de los S-boxes de Serpent (leer el paper en mi pagina) y encontrar una representación del mismo con operaciones booleanas.

7) Escribir un programa que tome como input un S-box y le calcule la tabla de diferencias y la máxima diferencia. Usar este programa con los S-boxes de Serpent.