Ejercicios de repaso SSI Módulos I y II

1. Cifra con Vigenère el mensaje DESASTRE, escrito usando un alfabeto con Ñ con W, y usando la clave SOS
2. Usando dos polinomios de realimentación distintos de dos LFSRs: $x^5 + x^4 + x^2 + x + 1$ y $x^5 + x^4 + x + 1$ y con cada uno de ellos las semillas 10101 y 00111, calcula en cada uno de los 4 casos las secuencias de salida completas.
3. Calcula el resultado de la operación en AES 11011011 x 01001001
4. Aplica el algoritmo de Diffie-Hellman con los valores: p=13, α=2, xA=87, xB=143
5. Calcula 3^{399} (mod 29)
6. Supón que tenemos una red con 1000 usuarios en la que cada participante se quiere comunicar de manera secreta con cada una de los otros participantes ¿Cuántas claves en total se requieren entre todos los usuarios, si se usa criptografía simétrica?
7. Supón que tenemos una red con 1000 usuarios en la que cada participante se quiere comunicar de manera secreta con cada una de los otros participantes ¿Cuántas claves se requieren si se usa criptografía de clave pública?