Tercera tarea examen

Sea $\pi(x) = x^{16} + x^{13} + x^{11} + x^6 + 1$, un polinomio primitivo sobre $\mathbb{F}_2$. Por lo visto en clase sabemos que si $\alpha = 2$ es una raiz de $\pi(x)$, entonces 2 es un generador de $\mathbb{F}^*_{2^{16}}$ (i.e. $< 2 >= \mathbb{F}^*_{2^{16}}$). Compruebe que el orden de 2 es $2^{16} - 1$. Tomando $a = 12345$, encuentre la llave publica $y = \alpha^a$. Mas aun, siguiendo el algoritmo de firma para ElGamal, y suponiendo que $k = 11$, encontrar la r y la s de la firma del archivo "Documento" (use "SHAfa" como algoritmo de digestion). Tambien encontrar y^r, r^s, v_1 y v_2.

Referencia: Ver Seccion 11.5.2 (pp. 454 y 455) en el capitulo 11 del libro de Menezes (mando dicho capitulo tambien como un anexo).