Este trabalho tem por objetivo mostrar um algoritmo utilizado para fatoração de polinômios univariados sobre corpos finitos. Esse algoritmo é dividido em três etapas: fatoração livre de quadrados, fatoração em graus distintos e fatoração em graus iguais. Seja f(x) um polinômio com coeficientes em Fq[x], onde Fq é um corpo finito. A fatoração livre de quadrados elimina os fatores repetidos de f. A fatoração de graus distintos separa f em blocos de polinômios de graus menores agrupados de acordo com o seu grau e assim, pode-se escrever f como $f = f_1 f_2 f_3 ... f_k$ onde cada f_i, i = 1,...,k é um bloco de polinômios irredutíveis de grau i. O trabalho focará na última etapa que é a fatoração em graus iguais e esta consiste em fatorar cada bloco f_i, i=1,...,k, que é um produto de polinômios irredutíveis de grau i, em blocos de polinômios de mesmo grau. Para tal, utiliza-se o separador chamado Cantor e Zassenhaus, que consiste em tomar um polinômio a(x) Є Fq[x] aleatório, cujo grau é menor que o grau de f_i e um inteiro d que seja divisor do grau de f_i e analisar o mdc entre a e f_i, obtendo assim um polinômio g_1; se $g_1 \neq 1$ dividir f_i por g_1 e assim obter um fator de f_i; calcular, através do algoritmo de Euclides, o resto da divisão de f_i por $a^{\frac{(q^d-1)}{2}}$ e, por fim, calcular o mdc entre $a^{\frac{(q^d-1)}{2}} - 1$ e f_i, obtendo assim g_2; se $g_2 \neq 1$ e $g_2 \neq f_i$ dividir f_i por g_2 para se ter um fator de f_i. Assim, para cada escolha do inteiro d e do polinômio a(x) obtém-se a fatoração de f_i como produto de polinômios mônicos irredutíveis de grau d e mostra-se que a probabilidade de o algoritmo devolver os fatores de f_i procurados mesmo utilizando um polinômio a(x) aleatório é satisfatória, o que completa o algoritmo.