Práctica 2 de Criptografía y Computación

Carlos Núñez Molina
Alessandro Zito
Gabriela Antolinez

1 Análisis tiempos Factorización

En esta sección vamos a analizar como tarda el algoritmo de Factorizacion por números grandes. Utilizaremos los tres metodologías que tiene ese algoritmo: Fuerza Bruta, Fermat y Ro de Pollard. Hemos hecho los análisis de frecuencias con números al azar y con números productos de primos. Empezaremos comentando con los números al azar.

Empezando con el algoritmo de Fuerza Bruta, sabemos que este algoritmo va intentando hasta que no factoriza el numero. Podemos ver en la primera imagen, como el algoritmo va a tardar mucho desde números de 28 cifras; va a crecer exponencialmente el tiempo que tardará el numero a factorizarse hasta un tiempo que es de 10^2

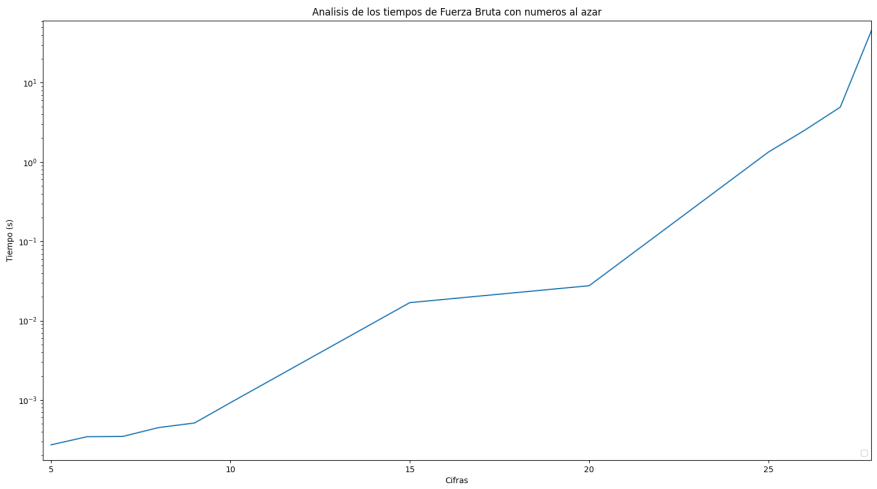

Figure 1: Análisis de los tiempos de Fuerza Bruta con números al azar

Después siguiendo con el algoritmo de Fermat, sabemos que este algoritmo va a resolver la ecuación $y = x^2 - n$ para factorizar el numero. Podemos ver en la primera imagen, como el algoritmo va a tardar mucho desde números de 10 cifras; claramente será el peor de los tres, porqué si los factores no son primos, tardará mucho en resolverlo.

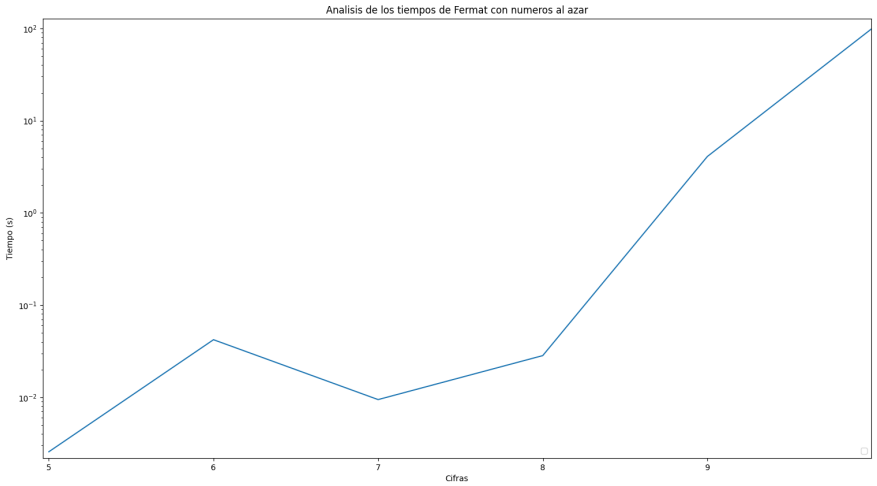

Figure 2: Análisis de los tiempos de Fermat con números al azar

El ultimo de los tres el algoritmo de Ro de Pollard, que tiene el nombre de el matemático que lo inventó. Se trata de construir una sucesión $x_1, x_2, ..., x_n$ y encontrar dos términos de la sucesión x_i, x_j tales que $mcd(x_i - x_j; n) \neq 1$. Podemos ver que este algoritmo es el mas eficiente de los 3, porqué se tardará "solo" 100 segundos con numerosa de 42 cifras!

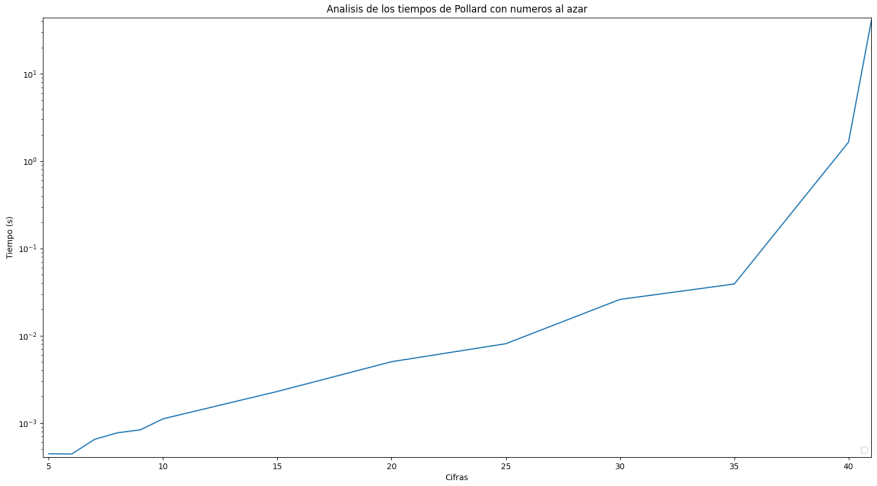

Figure 3: Análisis de los tiempos de Pollard con números al azar

Haciendo los mismos test con números productos de dos primos, podemos ver como la eficiencia de Fuerza Bruta y Pollard es menor; sobre todo la de Fermat será mayor; eso porqué Fermat va a buscar los dos factores primos y si son cerca el tiempo será menor.

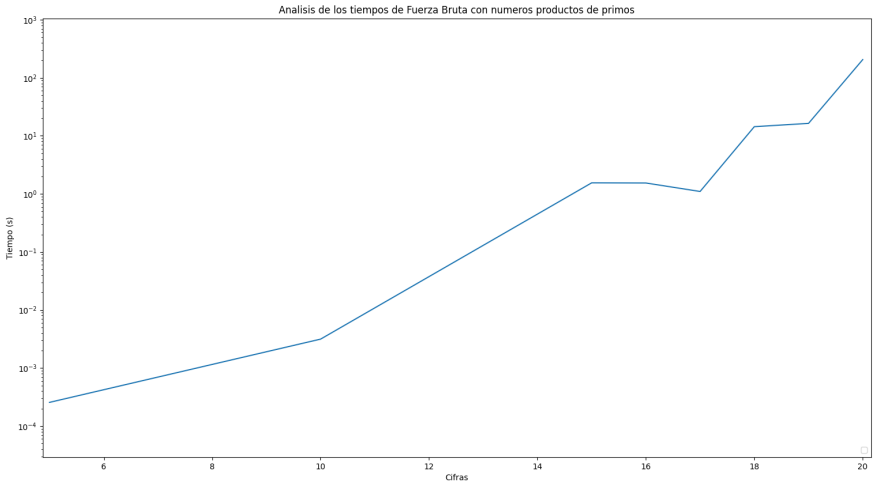

Figure 4: Análisis de los tiempos de Fuerza Bruta con números productos de dos primos

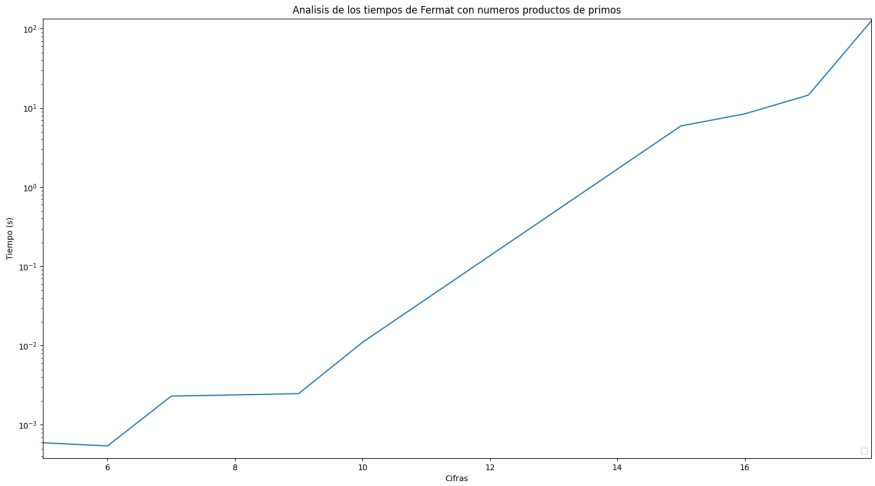

Figure 5: Análisis de los tiempos de Fermat con números productos de dos primos

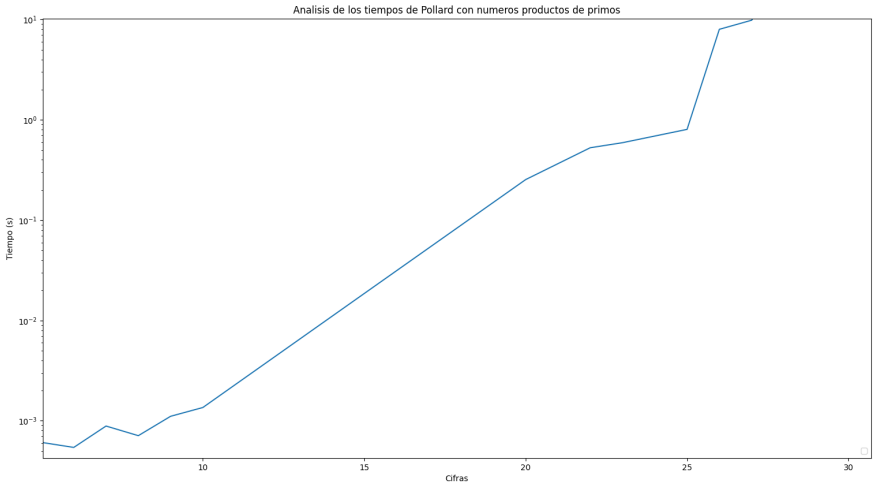

Figure 6: Análisis de los tiempos de Pollard con números productos de dos primos