Part 1

Encrypted text:



Decrypted text: Ricciardo made his debut at the 2011 British Grand Prix with the HRT team as part of a deal with Red Bull Racing, for whom he was test driving under its sister team Scuderia Toro Rosso. He joined Toro Rosso in 2012 full-time after the team changed its driver lineup and drove a Ferrari-powered car for them in 2012 and 2013. In 2014, Ricciardo was promoted to Red Bull as a replacement for the retiring Mark Webber alongside Sebastian Vettel. In his first season with Red Bull under Renault power, Ricciardo finished third in the championship with his first three Formula One wins, in Canada, Hungary, and Belgium.

For this part I have implement the encryption and decryption method. For encryption I first read the file and pad zero from right if the block is not 128 bit, and then pad 129 zeros from left to get to 256 bits. Then I multiple pq to get n. and then do the encryption algorithm in rsa C = M^e mod n to get the encryption text. For decryption part I used the CRT which get the Vp Vq first and then use (Vp \* Xp + Vq \* Xq) % (n) to do the decryption.

Part 2

I first call the PrimeGenerator in order to determine generated p and q value is prime or not, and then call the encryption function I wrote earlier to encrypt the three text separately using different p and q value. Then according to CRT algorithm I to calculate each of the text’s multiplicative inverse and then use M1 \* M1 ^ inverse \*M2 \* M3 and etc and add all three conditions together to mod N, this way to get M^3, and then I called solve\_pRoot function that given to solve for M.