Part 1

Encrypted text:

5794d0da2de74c58cae4959f4df22c3f824c45696c21707c5a03645e2e5b1c4dc2285609083d80354a2befc
ed1edca573115bcdd5ab634295d46645d19c347213a10441f1b2196dfae8c88f13a873cbb56f5debf2a64a
102e8a6fc908991a11e8a52e8b8197581aa4cc8dbab2c987659498b2c0cb39085b0ce579d916669663494
28e337e8a7d63ea27abbf75b85347c025fe39e8ab2422a770c48900210748cbaf406182119eed41fd36c2f
b266aa0f32b946b1c2c47783915f28be62659d2f635311ec8f1062d27cd94c460c1d964c8f94257aa8d5f23
2442bed6f349603c43dc32eb3d6101f3a1974a8bc4b42d14ecc8c8f51a5ed7d69c406ccfaa9a808cf35ac5c
b76bd9bf94c7b72ff7964b7a05c0170f6132c19e02088c01b5c450b5ba13b960f8eaaf727b5e16fe6e67cd8
9f3974449592e7b2129ca7db380fbeadc497c8e4ab80beddad0ec54face12781e4fd6d41f8b297a117083e
0ab11bea6088528edbae36020332cc86913c6fb1880bef47a941d8f98b39192533f3883d73d644f9823a0d
0dbed50641666804848b43427a7326f0934d311df014cb5102f58da30798fc4e8cd8c096b4f463e124c589
8c04b00bd80ba2ebd972ab96c727f8a1498337d10515684587ae45d836113f69ba0e32528e6b25ede4e97
12d61ee5ad9b698020255b7b57005d5c8f65337abdf19bb8ac1776a4bd3b9336733c9174737c5ac12050c
4b3efe5607d4a36bb2cd9c90c7a31ac6ff4bd2b0d9d40314b9ff09f9f8196f1600d1f32a13b6941e108f38f9
7f4583fb28531eecfa46b5265a8b260a072af5590b5a397afedd530db823855da5581940d444a9b3f9e135
4610c0853632ea94a58ac4285dcd892f05ca922b1376e1333e56dc16b91398f5cd376d056881496ce8f812
c5eb388ba7b37402a257ee5b3a343b7591e21dbdca35460c93294e5bfdf33ddd379702f00b75f9d686f556
fe233e222aabf076e745e089aa499058a2371d697170a7bc359b82e4cd85c41c4a4cb0970302eb966909e
0f4492865d0d935e4f4ab4e99ea833cc2c710eaaf6491559e292db63b28981fe37397db813ea9f1d9d7b4d
a91c475ed78e5419799d7c5df44be35ff49751796130f98b355cba96666c11fa360e5a372a30d3f5c8ae0f2
bd575443d8975543aaaaaea6bb03a8985177f9487f382c9ea76529154ee80f88e6d211be998ab2918b2ef
bb629243110487e2d9c895e36d076b586ecd3c961592e007984b2294dbb8ade05d5f4fab75f906d9771a3
d5bc8a25218be02eb2259f81cf996ce6cb65dfa7d09d6461e9ebc5f51670164ca5d167fd1a785cf2847726d
bd6fced35fca4ddb686f19ddb6290e4f010bf6f1c2f0194c59a4c247d9fc182b67a820fe0cad02ff9db3e45ee
e54c67dac2791099b429af5b4ef43f24bd771f3c364b1fabb8d146f95c90dd16e0f6ec44f1281cdf46cf63a9
2ff6e8f733d37bc292e3489826a26448d32b174b3020e913466562b7f875f757ff03d1915d6036d3561234
91b1be7cc57f6c261ff65dbf797cf8616e302018bccc81777a6fac6402e10ac5ce404bd796887ae840e3f49a
1643fb9b8173e6ea92d1421bea0f6da03025b6dee1a2475ca877fd24ede647cacce93df5ae5c1820426263
9c2c9e4da59f723b1a84dfb9e8fc54e7188163528b580c0c40ecd767cf9051ed1adb283fb37e4500412d6d
82e479290c3321d05d6535725d4b19be95421fb8cf0661bff980b860243b95ed13e59e602473f1f

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.