

The decrypted plaintext is: Sir Lewis Carl Davidson Hamilton (born 7 January 1985) is a British racing driver currently competing in Formula One, driving for Mercedes-AMG Petronas Formula One Team. In Formula One, Hamilton has won a joint-record seven World Drivers' Championship titles (tied with Michael Schumacher), and holds the records for the most wins (103), pole positions (103), and podium finishes (191), among many others. Statistically considered as the most successful driver in Formula One history.

The key (as an integer) is: 4040

Explanation: As expected, this code is taken from “decryptForFun.py,” the decryption script provided from the Lecture Notes. The only functional changes were that I deleted the code related to turning the user input “key” string into the BitVector “key_bv” and changing the value of BLOCKSIZE from 64 to 16.

This decryption works on the principle of “differential XORing” which uses a bitwise XOR operation on every ciphertext (encrypted_bv) block of length “BLOCKSIZE” (bv) with the previously decrypted block (previous_decrypted_block) AND the key as a bitVector (key_bv)