ECE 40400: Introduction to Computer Security

Spring 2024

Prateek Yashwant Jannu

Purdue University, West Lafayette

Professor: Dr. Avinash C Kak

∗ **The recovered plaintext**

Charles Marc Herve Perceval Leclerc born 16 October 1997 is a Monegasque racing driver, currently racing in Formula One for Scuderia Ferrari. He won the GP3 Series championship in 2016 and the FIA Formula 2 Championship in 2017. Leclerc made his Formula One debut in 2018 for Sauber, a team affiliated with Ferrari, for which he was part of the Ferrari Driver Academy.

∗ **The recovered encryption key** – 1616

∗ **A brief explanation of your code**

Code C through Z has been taken with reference to the lecture notes from **lecture 2** and code from L through T has been removed as key_bv has already been processed in the function parameters, so now the only thing left is returning the output string which has been added at the last line of the cryptBreak.py function as return msg_decrypted_bv.get_text_from_bitvector(). First, we differentiate the first part of the message with the phrase key_bv and then the first part is xor'ed with the next N parts and so on until the whole message is decoded and in the main() function it is checked if 'Ferrari' is in the given text, if yes then the message is decoded successfully.