Security Project

Mostafa Osama AbdelZaher	*1190173*
Yomna Osama Hussien	*1190203*
Amr Yasser SalahElDin	*1190380*
Khalid Mamdouh	*1190321*

CTF Part solution:

1. SUPER SECRET MESSAGE
2. THM{d0_n07_574lk_m3}
3. CMP {Turn Lights OFF}, CMP {Yellow Joy}, CMP{You_Catched_ME}
4. CMP{Mara Sabetny A3az 7abiba :(}
5. CMP{Abyusif_Or_Marwan_Moussa}, key = 15
6. CMP{30_Pounds}
7. CMP 17TOKA2023
8. CMP{Shababik81}
9. THM{y0u_w4lk_m3_0u7}
10. THM{7h3r3_15_h0p3_1n_7h3_d4rkn355}
11. COMPUTERS{ D0neD0ne} (Script included)
12. soundingqr
13. THM{500n3r_0r_l473r_17_15_0ur_7urn}

Algorithms part:

We figured out the three algorithms as follows:

Algorithm 1:

The only option for this algorithm is to be a one-time pad. One-time pad is mostly known for having a key as long as the plaintext with being perfectly secret due to relying completely on a random sequence of bits.

Algorithm 2:

There are only two algorithms that take a single number as a key, which are Caesar cipher, and Rail Fence. Since Caesar was excluded in the question, this leaves only one option, which is the Rail Fence.

Algorithm 3:

There are only two key-exchange algorithms, Diffie-Helman, and El-Gamal algorithms. Only El-Gamal algorithm produces 2 ciphertexts.