Question Number 1

Capture The Flag

Demonstrate how you solved the CTF that lead you to this Assignment? If your group is among the first three teams then, you will receive bonus points. However, every group must justify how they got hold of this pdf file.

Note: *If you are unable to justify this then the rest of the solutions will not be accepted.*

Solution. Procedure to get final keys:

a) **Collect message-cipher pairs** using `Utils.getPairs()` for cryptanalysis.

b) **Guess the second-round key** (k_2) by analyzing T_1 and T_0 counters from linear relations.

c) **Select likely k_2 candidates** based on the highest imbalance in T_1 and T_0.

d) **Refine the key search** for k_0 and k_1 using the Linear Approximation Table (LAT).

e) **Eliminate incorrect keys** and find the final key triplet $[k_0, k_1, k_2]$ using the `solver()` function.

f) **Initialize the full key space** for (k_0, k_1) as all possible 32×32 combinations of 5-bit keys.

g) **Filter keys iteratively** by checking the XOR relations $(\alpha_{k_0} \oplus \beta_{k_1})$ with T_1 and T_0 values.

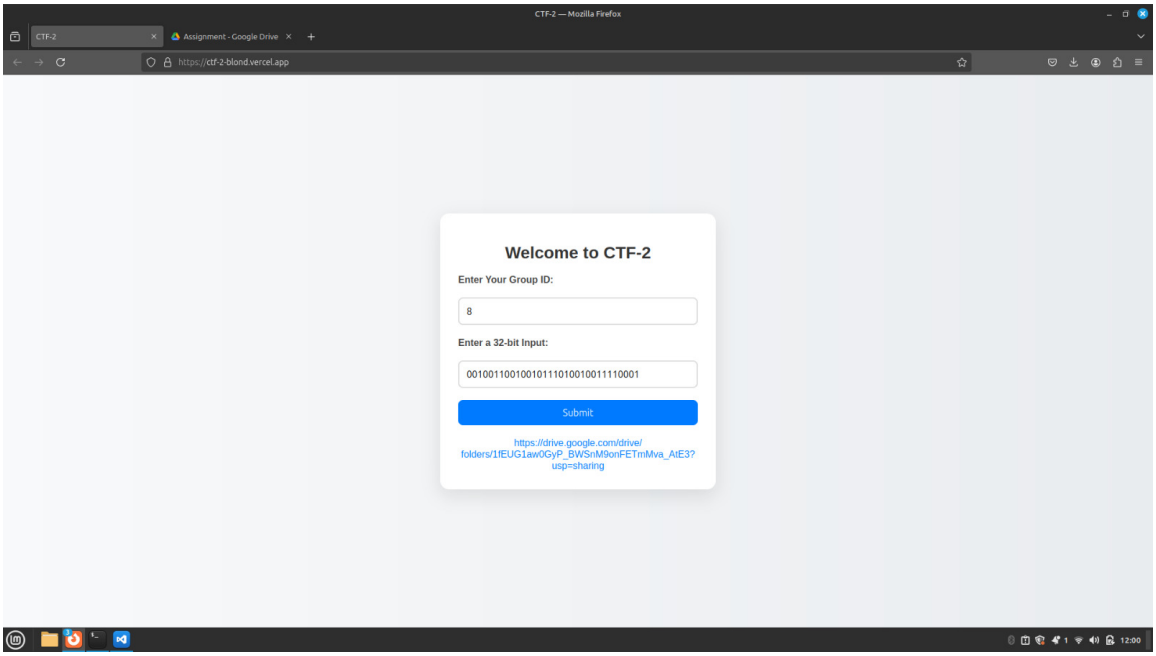
h) **Remove keys** where the XOR result does not match the expected output for $T_1 > T_0$ or $T_1 < T_0$.

i) **Continue refining keys** until only one pair (k_0, k_1) remains that satisfies all conditions.

j) **Pass the master key into** `keyExpansion()` to expand the key and generate the full 44-word key schedule.

k) **Combine 15 bits from** `k0`, `k1`, **and** `k2` with 17-bit portions from the key expansion to form the final 32-bit key guess.

Images




```
karan BR main ... | Crypto | assignments | OpenSSL openssl pkeyutl -decrypt -inkey 8.key -in 2d8a1997.bin -out decrypted_file.bin
Enter pass phrase for 8.key:
karan BR main ... | Crypto | assignments | OpenSSL cat decrypted_file.bin
https://drive.google.com/drive/u/1/folders/1NCi1PUWuODnBnkeHdqVE3vDOzmdrOdgt
karan BR main ... | Crypto | assignments | OpenSSL
```