



WRITE UP FOR SHUFFLE SQUADRON

Contact :
contact@cybercohesion.com



❖❖ Scenario :

- The participant has been given challenge.py and output.txt, and their task is to find the flag using their mathematical methods.
- The mathematical logic applied is a Permutation Group : <https://golamrabbany.medium.com/crypto-ctf-learning-permutation-4f5b85c062fd>
- Looking out for output.txt we have multiple factors of the group and applying a DLP solution should bring us a value of « $a = 939949150743981254$ » & « $b = 128039154543841453$ »

❖❖ Answer :

Cyber_Cohesion{65.476721,-173.511416}

❖❖ Ref :

- https://www.researchgate.net/publication/326514386_Cryptanalysis_of_a_Proposal_Based_on_the_Discrete_Logarithm_Problem_Inside_Sn/citation/download
- https://docs.sympy.org/latest/modules/combinatorics/perm_groups.html
- <https://github.com/ufkapano/permgroups>



WARZONE

AND THAT WAS IT

Shuffle squadron !