

# TERM PAPER

Requirements (weightage - 30% roughly)

Abstract – Introduction – Algorithm – Attacks – Conclusion – Brownny point

- ✓ Understanding Algorithm
- ✓ What is a security claim (128bit or whatever)
- ✓ draw.io for drawing diagrams
- ✓ Another aspect - Implementing Algorithm
- ✓ Look at various attacks
  - Differential Cryptanalysis, Linear Cryptanalysis, Basic attacks
  - Another new attack can be drawn(Appreciable)
- ✓ Abstract - Summary of the work
- ✓ Documented piece of code, quoted (which we have done ourself)
- ✓ Last Section after conclusion
  - Brownny point - Something we think is new we can highlight
  - From any part of the term paper
  - We have to nominate some part part of our work
  - Like - This point I am nominating + why
  - Then implement Algorithm
- ✓ Reference section
  
- ✓ Requirements
  - Use template
  - Presentation Video
    - It can be about 30 minutes of video where along with slides we also have to visible in the video
    - All of us have to contribute (roughly 10 minutes each)
    - We can use either any platform(gmeet or anything) or separately we can record
  - Implementation of the Algorithm
  - Documented piece of code with readme file required to upload to github repository & share the link

Plagiarism will strictly be checked (automatically be checked with the platform where we have to upload the content) and we will get One chance to be explained why plagiarism is there

➤ We have to Encrypt the submission by key given by Dhiman Saha