**Applied Cryptography CS 428**

**Implementation /Programming Projects:** The project should involve implementation and study of algorithms or techniques.

Project topics:

* CBC
* CTR
* CFB
* HMAC
* Diffie-Hellman key agreement
* DES
* AES
* RSA
* Secure chat using AES, RSA
* Picture based authentication
* Side-channel attacks (since I have only one board, only one group can do this project, first come first serve)
* [Heartbleed Attack SEED LAB (](https://seedsecuritylabs.org/Labs_20.04/Files/Heartbleed/Heartbleed.pdf) individual project)

|  |  |  |
| --- | --- | --- |
| Deliverables | Due | Points |
| One member of your team, email me a Topic Description at most one page giving me title of your project, identifying the members of your team and short **description of what the teams proposes to do**. | Friday 8th April 2022 at 11:59 pm | 10 points |
| Write a project report (2-4 pages excluding references and code) describing what you did, your results and any problems you encountered. | Thursday 28th April 2022 at 11:59 pm | 25 points |
| Code (correct implementation of encryption, decryption, and key generation).  Your code should accept input/plaintext from the user. | Thursday 28th April 2022 at 11:59 pm | 65 points |

**Your project will be graded based on clarity of explanation & write-up of what was done, completeness and depth of the programming and project work.**