CSE 345/545: Foundations of Computer Security
HOMEWORK ASSIGNMENT 1 (TOTAL OF 25 POINTS)
The assignment should take about 15 hours.
Do not wait until last minute. Submissions over Backpack ONLY. Some questions are open ended. Be creative!

1. Research and formulate two(2) experiments through which you can glean the PPI (Protected Personal Information) of the faculty and staff of IIIT-Delhi. [4 marks]

2. How would you design a study to measure the 'strength' of passwords? What good practices should be followed while creating a password? How do you encourage people to follow these? [4 marks]

3. Take a Privacy Policy and mark various points of OECD and FTC Principles into it. Assume that you are the security / privacy expert in a e-commerce organization, you have been asked to prepare the privacy policy of your organization. Do a comparative study of 3 different privacy policies of organizations, and show the similarities and difference. Keep the context within OECD and FTC principles. [1+3 marks]

4. a) The Vigenere cipher is a variation of the Caesar cipher. List one similarity and one difference between the two ciphers. Explain why the Vigenere cipher is more difficult to decode. b) What is a Feistel Cipher? Code one round of the Feistel Cipher in any programming language of your choice. [4+5 marks]

5. The guards at IIIT Delhi allow anyone to enter the college premise without a IIITD ID card as long as they enter their details in a Ledger. Do you think this practice is secure? Do you think it is usable? Propose an alternate system for entering the college. In your proposed system, please discuss:

   • What usability issues you feel need to be addressed?
   • Include some suggestions to improve the system. [4 marks]