CSE 345/545: Foundations to Computer Security
HOMEWORK ASSIGNMENT 2 (TOTAL OF 100 POINTS)
The assignment should take about 10 hours.
Do not wait until last minute. Submissions over Backpack ONLY. Some questions are open ended. Be creative!

1. Differentiate between Stream Ciphers and Block ciphers. Encrypt the following plaintext "FOUNDATIONS TO COMPUTER SECURITY IS A COURSE AT IIITD" using a) block cipher of your choice b) Stream cipher of your choice. Choice of keys, modes or base (if any) is left to you. [10 marks]
2. Install NMap on your computer (http://nmap.org). Make sure that the default firewall on your computer is turned off. Now perform a full scan on your computer using NMap. Document the results (including all open ports and services running on those ports). Turn your default firewall ON. Now perform a full scan again and report the difference in results. Also mention what operating system you used. **Write a report documenting the whole process with instructions for each step and output screenshots.** [25 marks]
3. What is the Heartbleed Bug? Detect whether a website is vulnerable to it using NMAP. **Document every step of the process with the commands and screenshots.** [15 marks]
4. Consider the following systems:

    a. IIIT-Delhi Library
    b. IIIT-Delhi ERP

    Do a comprehensive Threat Model of both of the above. Identify assets, points of attacks and threats. Categorize and rate threats. Identify ways of mitigating them. Note if the mitigations lead to any tradeoffs in usability. [20 marks]
5. The given ciphertext

\xc5\x81\x97~\xb4\x0b:U\x13^\x9c\xb2:\xedcC\xe5\n\xab\xb2\xbas\xbe/\r\xa8\x00'\x87\x91Ch\xb8\x060\xfb\xf8V\xf7)\x1d\xfb\x12\xe7\x16\xf0\x12\x1dQ\x99Gs`\xf5qZjQL\xe1\x1f\xfd\x90E

was obtained by encrypting a quote by Oscar Wilde (excluding punctuation if any) using DES in ECB mode. The key is numerical. Assume the role of a cryptanalyst and obtain the key as well as the plaintext. You are welcome to use any existing cryptographic libraries as long as you put them up as references. Document your approach (programmatically, manually, etc) with code(if you write any). [30 marks]
Hint: The key length is 8 bit and the key itself varies from 00000000 to 99999999

Here is an example of encryption and decryption through DES using the Crypto library in python (https://www.dlitz.net/software/pycrypto/)

```
from Crypto.Cipher import DES

Key = '01234567’
des = DES.new(key', DES.MODE_ECB)
plain_text = "abcdefgh"
#encryption
cipher_text = des.encrypt(plain_text)
#decryption
decrypted_pt = des.decrypt(cipher_text)
```