# Assignment 3

## Vulnerabilities in standard cryptographic protocols

**Introduction**:

For this assignment, your task is to choose one of the Cryptographic Protocols and study its vulnerabilities. This is an open assignment where you are free to choose any protocol.
For the submission, we expect you to submit the following:

1. A working simulation of the vulnerability
    a. A well commented code
    b. A README file explaining how to run your code
2. A report consisting of
    a. Explanation of the protocol
    b. A study of the vulnerability that you chose
    c. Whys and Hows of the vulnerability
    d. About your simulation

As the code is a simulation, it should print out the details in the command line, or you are free to use any other way of showing your simulation but printing out in the command line is the easiest option.

**Example**:

First see this video so you get the background for this example.
Suppose you choose POODLE vulnerability of SSL v3.0 protocol.

Brief - POODLE attack is a man-in-the-middle attack. When cipher block chaining is combined with SSLv3.0, padding is required to make the cipher blocks of constant size. This attack exploits the padding method to get access to 1 character from the message at a time.

For the report you are expected to write about:

- SSL in general, and about v3.0 focussing on things that causes POODLE
- About POODLE, How can it be implemented, its impacts, measures to safeguard against it.
- On paper implementation of you as an attacker trying to exploit this vulnerability, explaining your code and its nuances

For the code:
You can open up 3 ports for representing client, server and the attacker. As it is a man-in-the-middle attack, give access to all client and server messages to the attacker. Perform the SSL handshake between client and server and then send the messages between client and server which are received by the attacker as well who performs analysis of the message it received.

Complexities not relevant to the POODLE vulnerability can be ignored in the code but not in the report.
SSL/TLS itself contains a variety of vulnerabilities for you to work on but you are free to explore other protocols as well.

## **Submission**:

Submit a zip file with your entry number as its name.
On extracting, it should provide a folder with your entry number as the name.
Inside the folder should be your report in pdf format, a README file and your code.
If there are multiple files to run (as there will be one for each client, attacker and server in our example above) provide a batch file which runs all the other files.

## **Marks distribution**:

- Report (30 marks)
    - Protocol explanation / 1 pages / 5 marks
    - Vulnerability explanation / 1 pages / 10 marks
    - On paper implementation of all the steps that you as an attacker will take to try to exploit it. / 1-2 pages / 10 marks
    - About your code / 1 page / 5 marks
- Code (20 marks)
    - Readability and comments / 5 marks
    - Core logic, closeness of simulation / 15 marks

## **Deadline:**

15th June '20