Name :- Ronak Kumar
Roll No :- 2015080

# FCS ASSIGNMENT-1

**A1)**

Alice :- Very weak
Qwerty1234 :- Weak
Rat$you :- Neutral
Elppa :- Very weak
Mumbai :- Very weak
Mfiical4W :- Neutral
Tif#hom&851@ :- Strong
#$\%@$^$^@$@# :- Very Strong
eclila!0987 :- Strong
45649243 :- Weak

**A2)**

**a)**

### Authentication

**Students :-**

- Any access to non-public online college IT resources like ERP, FTP, Library etc. will be achieved by individual and unique logins which are a combination of username and password. The username would consist of the user's name and roll no followed by the IIITD domain address. A seven digit roll no is assigned uniquely to each and every student of the college. Physical access to labs and using college infrastructure can be done by entering details in the ledger and by using only your username and password while using lab computers.

**Visitors :-**

- Any access to internet and online resources is blocked. Only physical resources like Library, Classrooms, Cafetaria are allowed to visit. A unique ID is assigned to every visitor which gets recorded with the name and other PPI in the ledger.

**Faculty :-**

- Any access to online IT resources like ERP, FTP etc. will be achieved by individual and unique logins which automatically grants admin rights for ERP and FTP Server. Physical access to labs and using college infrastructure can be done through your username and password.

**Employees :-**

- Any access to online IT resources like ERP, FTP etc. is not allowed except for the IT Team. IT Team can login into the system by their respective unique logins. Physical access to labs and college infrastructure for the IT team is allowed without any filling of details.

## Authorization

**Students :-**

- Any access to unencrypted services like Torrent, VPN, Telnet etc is not allowed. Traffic across the network in these channels if found may held the student guilty. Access to the database and the server of college to a student for educational purposes should be assigned by the IT Team with prior permission.

**Visitors :-**

- Only physical access to the cafeteria, classrooms and library is allowed. Any intrusion to online resources or entering into labs will held the visitor guilty.

**Faculty :-**

- Any access to ERP, FTP etc. is allowed but has to be kept confidential and need not be shared anywhere.

**Employees :-**

- Access to the resources is being assigned role wise. Any intrusion towards anything unauthorized without prior permission may held the person guilty.

## Identification

**Students :-**

- Each student is assigned a unique seven digit roll no which remains the same throughout his tenure at the college. Every student gets a unique Email ID for all accessing all the college resources (online and offline).

**Visitors :-**

- Each visitor is assigned an ID whenever he/she enters the campus gates.

**Faculty :-**

- Each faculty is assigned a unique Email ID which is different from the student's email ID for accessing all the college resources

**Employees :-**

- Each employee is assigned a unique Email ID which is different from the student's email ID for accessing all the college resources

**b)**

- Firstly, for having physical access to the labs and other resources, there is no authentication method especially for faculty and the employees. One can easily get into the labs by pretending to be a faculty or employee of IIIT Delhi and may damage the resources present there.
- Secondly, since any unencrypted communication isn't allowed and is monitored, the attacker can spoof the MAC Address of his computer and commit the malpractice using somebody else's IP. This would make that person guilty who was even unaware of the act.
- Lastly, the attacker might send phishing emails in the disguise of some faculty or trusted group to fetch your details (ex- some form). This lets the students reveal their information and they may become a victim of social engineering.

**c)**

- The solution for this problem would be to educate the guards about all the employees and the faculty of IIITD and give them a list so that they can match the person's face with that.
- The solution would be to have an expiration login time and also prevent any kind of spoofing at the router's side by relogging again. Router's also should not send the information if there are two computers with the same MAC on their network for a span to time.
- The solution for this would be to have strict domain checking whenever a new mail arrives. DKIM is here is the most effective way to automatically detect any kind of spoofed emails by authenticating the domain itself. Also, the students need to be educated to validate the email locally before giving any details.

**A3)**

a)

i) **PlainText (Also in the Q3aPlain.txt file)**
Legislatureshallmakenolawrespectinganestablishmentofreligionorprohibitingt hefreeexercisethereoforabridgingthefreedomofspeechoroftheressortheright ofthepeoplepeaceablytoassembleandtopetitionthegovernmentforaredressofg rievances game of thrones season eight spoilers jon snow and daenerys targaryen to kill each other

ii) The working code in C++ is attached in the folder with file name as Q3a.cpp

iii) I used the caesar cipher method to decrypt the given ciphertext into plain text. I chose the shift to be 7 if I decrement each character or 19 if I increment each character keeping the modularity of the number of characters. Therefore, for every character i in the cipherString, I increment the character with the key and then subtract the starting ASCII value depending on the case of the character (i.e 97 for small alphabets and 65 for large alphabets). Then I take the modulo with total number of alphabets (i.e 26) and then add the starting offset and append the character to the output string. Finally I return the output string. I used hit and trial way to determine the shift.

iv) **Random Text**
spoilers jon snow and daenerys targaryen to kill each other

Integrity is violated when the TA appends random cipher text in the end. This is because whenever a person deciphers a piece of text, then it is done completely and he may also include the random text in its text although it shouldn't be included. This causes data manipulation and effect the system since wrong text is being passed into it as input. Either random text should be completely avoided or there should be a way to tell the person that this part of text shouldn't be included in the original text.

b)

The working code in C++ is attached in the folder with file name as Q3b.cpp

**A4)**

Let's take an example of an authentication system for people entering into IIITD's campus. The security guards at the gates allow anyone to enter into the campus as long as they fill their details in a register. This practice is quite convenient and very usable but it becomes highly insecure when considering the entrance of any intruder or adversary. By this any person can just only pen down a few details which might be fake as well to get inside the campus. Some of the usability issues persisting include the showcasing of ID cards of students while entering the college. This may improve the security but overall it decreases the usability for the student since most of the malpractices are committed by people outside the campus. Also, in certain conditions when a student forgets his/her ID card then he/she has to wait to enter the details which creates a lot of inconvenience and makes the system less usable. My suggestion towards improving the usability as well as the security of the system would be to introduce the ability of face recognition at the campus gates. The faces of all the students, faculty and staff should be recorded into the database. Whenever any person enters the gate, if the profile matches with the database then the guard can easily send him inside without any worry. By applying face recognition technique, this system would become highly usable especially for students/faculty and the staff. Another improvement if face recognition fails can be done is to introduce fingerprint biometrics for everyone entering the campus. This method will store the fingerprints of any person who is either a student/faculty/staff/intruder so that whenever any malpractice happens the person can be held accountable for the act. Also, daily log should be maintained securely by storing PPI for a visitor like phone number, name etc. The system would become less usable for outsiders like delivery person etc. but that compensates for the increase in security the campus would have then keeping in mind of the usability of employees and students. Also, in case of vehicles, the system should have the ability to record the plate numbers of all the vehicles entering and leaving the campus to further strengthen the level of security.