# Homework - 1

**Kaustav Vats - 2016048**

01-Sep-2018

## Part I

1. Alice - **Very weak**
    - One uppercase letter used.
    - Only letters included, consecutive lowercase used, name should not be used as a password, Length too short(less than 7), Numbers & symbols not used, Need more randomness.

2. Qwerty1234 - **Neutral**
    - One uppercase used, Numbers used.
    - No symbols used, Consecutive numbers and consecutive letters used. Qwerty...,123... common pattern used, Need more randomness.

3. Rat$you - **Strong**
    - One uppercase used, one special character used. Seven letter password.
    - Numbers not included, only one uppercase used.

4. Elppa - **Very weak**
    - One uppercase used.
    - Only one uppercase used, consecutive letters used, No numbers used, No special character used, name should not be used as a password, Length too short, Need more randomness.

5. Mumbai - **Weak**
    - One uppercase used.

- Only one uppercase used, consecutive letters used, No numbers used, No special character used, name should not be used as a password, Length short, Need more randomness.

6. Mfiical4W - **Neutral**
    - Two uppercase used, One number used, Length greater than 7.
    - No special character used.

7. Tif#hom&851@ - **Very strong**
    - One uppercase used, special character used, numbers used, length greater than 7.
    - Consecutive letter and numbers used (Advisory).

8. #$\%@$^$^@$@# - **Very strong**
    - Special character used, length greater than 7.
    - No numbers used, No letters used, special character repeated.

9. ecila!0987 - **Strong**
    - One special character used, numbers used, length greater than 7.
    - No uppercase used, consecutive letters and numbers used.

10. 45649243 - **Very weak**
    - Numbers used, length greater than 7.
    - No letters used, No special character used, consecutive numbers used, only numbers used.

## Part II

Many online system services are offered in IIITD. Erp is used for course registration, Fee payment, Hostel request etc. IIITD network login is used to access Internet in campus. Backpack is used to access course material, submit deadlines, etc. In the new System OTP and alternate mail can be used as 2$^{nd}$ step

for identification or USB signature device. To avoid any usability issue, this 2nd step can be used as a surprise check.

1. IIITD Mail System:
    - Students, Faculty & Employees has an email id and a password for their identification. They will also have their mobile device and alternate email for 2nd step verification. Visitors don't have a institute email id.
    - System take their email id and password to authenticate the user. If hashed password matched with the password store in the database, then user is allowed to access the mail.
    - Students, Faculty & Employees have different authorization. Eg- Admin can send a mail to any mailing list/user. Student are not authorized to send a mail to student list/group or any other official mailing list(list that are used by employees for official purpose). Similarly Employees and Faculty has access to limited mailing list.

    This service is available for both On Campus and Off campus.

2. ERP: It's a registration portal; to register courses, to register for hostel, to register for projects and TAship for a particular course.
    - Students, Faculty & Employees can use their institute id and their password for their identification. They will also have their mobile device and alternate email for 2 step verification. Visitors don't have any access to this service.
    - System take their email id and password to authenticate the user. If hashed password matched with the password store in the database, then user is allowed to access ERP.
    - Students, Faculty & Employees have different authorization and purpose for this service. Students are given access for course registration only for small duration. Same for hostel registration. Admin can change access rights for all student and can also update their grades. Few employees are given access to verify the payment made by each student and for hostel registration requests.

This service is available for both On Campus. VPN can be used for Off campus. VPN requires user credentials. Then credentials are verified with the data stored in database.

3. IIITD Network Login:
    - Students, Faculty & Employees can use their institute id and their password for their identification. Everyone need to get their mac address registered by IT helpdesk. They are using two step verification to identify the user. Visitors are given restricted access to the networks. They only need to connect to the network and the rest is handled by networks policies.
    - System first check for the mac address of the user. If it's registered only then give access to the login page. In Login page user enter their email id and password to get authenticate. If hashed password matched with the password store in the database, then user is allowed to access Internet.
    - Some restricted internet access should be given to students.

4. Backpack:
    - Students & Faculty need to identify themselves by entering their email id and password. They will also have their mobile device and alternate email for 2 step verification.
    - Then backpack will authenticate by hashing the entered password and comparing it with password stored in the database.
    - Faculty is given full access to the backpack. They can create an announcement, delete it, etc. Whereas student should only view the announcement. They should be given restricted access to backpack.

5. Entry to the College:
    - Students, Faculty & Employees they all need to identify themselves using their institute ID's before entering the campus. Visitors can use any other Govt ID to identify themself.

- Guard authenticate the ID's they have provided and should only allow after complete authentication.
- Restricted access is given to the student. They are not allowed to enter Faculty building. They are not allowed to enter hostel depending on their gender.

6. IIIT LIbrary:
    - Student, Faculty & Employees they all need to identify themselves to use Library service. They will also have their mobile device and alternate email for 2 step verification. Visitors can't access any library service.
    - Library service will authenticate user by hashing the entered password and comparing it with password stored in the database.
    - Student, Faculty & Employees they all are given different access. Student & Faculty can hold a book in library. Library employees can allot a book to a person, they can cancel their booking etc. So each user is given different authorization.

Ways in which attacker might try to spoof the system.

- Attacker can try Email spoofing. Attacker can set email header so that the message appears to have come from the actual source. Then this can be used to extract data/phishing and spamming.
- Attacker can use his own router to exploit the network of the user. User will connect to this router thinking that it's a college router. Then the attacker can use common man in the middle attacks like Phishing, SQL Injection, Malware attacks. Attacker can exploit user device by sending packets directly with any router firewall. Attacker can monitor all conversation of the user.
- IP Spoofing attacks are also possible. If an attacker gain access to an authorized person in IIITD. Then attacker can use his/her legitimate IP address & mac address to gain access to the Network, send packets using trusted IP address.

- Attacker can also try DoS attacks using many compromised computers, causing the server to overload. Attacker can send virus, malware to other users using legitimate IP address.

How above points can be avoided.

- Institute should have strong firewall to avoid any kind of email spoofing. Packet filtering should be implemented.
- Secure encryption protocol such as SSH, TLS should be used to encrypt data. Avoid trust relationship, just only ip address verification is not enough.
- Instead of just ID card for verification. Biometric can also be used to identify & authenticate the person.
- OTP or a USB Signature device can be used to make

## Part III

A. Plain text:
Legislatureshallmakenolawrespectinganestablishmentofreligionorprohibitingthefreeexercisethereoforabridgingthefreedomofspeechorofthepressortherightofthepeoplepeaceablytoassembleandtopetitionthegovernmentforaredressofgrievances game of thrones season eight spoilers jon snow and daenerys targaryen to kill each other

Methods used: Above plain text is encrypted using **caesar cipher**.

1. Try Caesar cipher, if it doesn't work then move to Vigenere Cipher.
2. For Caesar cipher we try to find shift for each letter. Count frequency of each letter in encrypted text.
3. Then compare frequency with relative frequency of Letters in English Text.
4. Highest frequency letter in Encrypted Text: **L**
   Highest frequency letter in English Text: **E**
   2nd Highest frequency letters in Encrypted Text: **A, H, V, Y, Z**
   2nd Highest frequency letter in English Text: **T**

5. Translate each letter to a number, ‘a’ = 0, ‘b’ = 1, ‘c’ = 2, …, ‘z’ = 25. Shift in the alphabets **7.** Then shift for T should be A & A is in our 2nd Highest frequency set.
6. On assuming shift in alphabets is by 7. Try to decrypt the Ciphertext. Our KEY would be “HIJKLMNOPQRSTUVWXYZABCDEFG”.

7. *Since the Encrypted text was short in length. We can also try brute force attack. By increasing shift in every iteration and printing out the result. Since we know that the text is in english we can identify the correct plain text.*

Randomly added ciphertext is: **nhtl vm aoyvulz zlhzvu lpnoa zwvpslyz qvu zuvd huk khlulyfz ahynhyflu av rpss lhjo vaoly**

- **Data Integrity** is not maintained. Text added by unauthorized user.
- **Confidentiality** is also not maintained, Since data was encrypted so its possible that the hacker knew the key and added some encrypted data in the end.
- **Authenticity** is also not maintained, It’s possible that hacker knew the credentials of the user and modified the file by adding some text in the end.

*Note:- Text added by the TA in the end of the ciphertext is not so random. It’s easily decryptable using the key for the rest of the ciphertext. This means that the TA knew about the key and used it to encrypt the new text.*
*Program in q3.java*

B. The Indian paradise flycatcher (Terpsiphone paradisi) is a medium-sized passerine bird native to Asia that is widely distributed. As the global population is considered stable, it has been listed as Least Concern on the IUCN Red List since 2004. It is native to the Indian subcontinent, Central Asia and Myanmar
*Program attached in a q3.java*

## Part IV

Email Authentication provides a way to verify user's identity. It is used to communicate with an Organization/Party and also to get access to a system(Network/ IIITD Login). All of the service providers have different email password policies. Since email service is used very often by each user, so policies/rules used are minimal to satisfy security and provide usability to the user.

- Web browsers also provide great user experience. **Browser can save the password**. Next time when the user try to access the service it will automatically login, giving fast and easy access to the user.
- **User might also save password in plain text or use some third party software**(Keeper, KeePass,..) either on PC or Mobile. If there machines are not secure enough then they might lose their passwords.
- Some email service providers(eg:- Outlook, Yahoo Mail) validate the user, with much better security if they login from a new device. Basically they try to verify the device using one more identification step and once verified they allow the user to login using those device. But this usability feature can be misused by putting a keylogger on the device. Attacker can use that device to access mail using the user credentials.
- Many accounts are hacked using the password recovery options. **Security question are very general to the user** like "When/where were you born?", "What's your mother's name",..etc. These questions provide great usability but less security. Since these questions can easily be extracted from the user.
- When user creates an account on email service providers. They are asked to enter an alternative mail. That mail is used to verify the authenticity of the user. Suppose if that alternate mail id is compromised. Then all the accounts that used above compromised email as an alternative email can be hacked using password recovery options. This can also lead to cascade account compromise.

Some suggestions to improve the system.

- Email service providers should use OTP verification frequently and keep updating the devices allowed for auto login. New devices that are used frequently should be allowed to be added as a recognized device only after few logins.
- Better security questions should be added and user should be allowed to make their own security question(only allowed by few service provider). Account should be restricted with some security rights based upon the user activity(Like login from new device).
- Alternate mail should not be used for recovery, just only for account confirmation link.
- After some duration, Email service provider should ask the user to update the password.
- It should also use OTP for surprise verification.
- If user forgot his/her password. OTP on mobile can be used to give access to the user with some security restrictions(eg:- not allowing to change password) to increase usability.