FCS - Monsoon 2020
Assignment - 1

1. Assumptions:-

- Given that we have to follow base 12. So the total numbers will be 12 from digits 0 to 9 and + as 10 and * as 11. This is our assumption that how we will be representing 10 and 11. As we are considering + and * here, we cannot consider them as special characters.
- Lowercase alphabets: 26
- Uppercase alphabets: 26
- We consider 10 special characters in our system. This completely depends on our assumption and this 10 characters do no include + and * as we already used them for numbers representation.
- Our task is to find the number of distinct passwords of length 6.
    - ❖ Given that the first character in password cannot be a special character and password, so this can be filled in **52** ways..
    - ❖ Out of these five characters, there should be at least one special character, so this can be done in (**5C1*10).** This 5C1 is for selecting one place out of the five available places and 10 is for available special characters.
    - ❖ Now, for at least one number, this can be done in **(4C1*12)** ways. This 4C1 is to select one out of 4 available places and this 12 is for choosing any of the numbers available.
    - ❖ Next character, in **(3C1*74)** ways. The 3C1 is to select one place out of 3 places and 74 is for the number of total ways we have to fill this place.(This includes lowercase alphabets, uppercase alphabets, numbers and special characters too).
    - ❖ Similarly, **(2C1*74)** ways.
    - ❖ Final place in 74 ways.

Final answer would be, = (52) * (5C1*10) * (4C1*12) * (3C1*74) * (2C1*74) * (74) ways
= (52) * (50) * (48) * (222) * (148) * (74) ways
= 303431731200 ways.

****

2.

a. The idea of encryption is based on ASCII values. The logic for the characters at the even positions in the string and the characters at the odd positions in the string are different.

For suppose, i is an index of a character(whose ASCII value is ‘n’) in password and i is even, this character is being replaced with a character whose ASCII value is n+i.

For suppose, i is an index of a character(whose ASCII value is ‘n’) in password and i is odd, this character is being replaced with a character whose ASCII value is n-i.

b.The list of words is taken from the web. The encryption algorithm followed in 2(a) is run on these words and obtained into a .txt file.

****

3.

1. 1q2w3e4r5t - Neutral - Password containing only small letters and numbers, so it may be easy to guess in some cases.
2. Football - Very Weak - Password is a commonly known word and can be easily guessed using dictionary attack or brute force attack.
3. 983749587 - Neutral - Password contains only numbers and also it is not a phone number as it is not containing 10 digits.
4. 4><8mM% - Strong - Password contains special characters, numbers, lower case letters and uppercase letters. But the password length is short so it may be cracked but may take a long time.
5. FCSPassword1 - Weak - Dictionary words are combined to form this password.
6. &*^)&@_(%$ - Strong - As it contains only special characters, can be made more strong by adding some letters and numbers.
7. SecurePassword@123 - Strong - It contains special characters, numbers, lowercase letters and uppercase letters.
8. monkey - Very weak - can be cracked easily using a dictionary attack.
9. Hello! - weak - looks like a dictionary word with a special character at the end.
10. Qwertyuiop - Weak - As it is one among the most commonly used passwords.

****

4. *Reference :- Olayemi Mikail, Olaniyi. (2013). Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions. International Journal of Computer and Information Technology (ISSN: 2279 – 0764). 2. 1122-1130.*

a. The security concepts which have to be included in an online voting system are:
   - **i.** Confidentiality :- Ensuring that no one can read the message except the intended user.
   - **ii.** Availability :- Ability to use information or resources desired.
   - **iii.** Integrity:- Votes should not be modified, deleted or forged without detection
   - **iv.** Usability:- How easy it is to users to use the system.
   - **v.** Authentication:- Only the authorized users can vote through the system.

b. Authentication mechanism in online voting system:-
   - We have to make sure that only the authorized users are allowed to vote. In order to make sure that, only the people having accounts in the system can vote.
   - Firstly, everyone who belongs to the institute has to register with their mail id into the system. During registration, there will be a verification email sent which is to be verified, and also we have to make sure that each mail will be registered only once.

- When an individual wants to vote, along with the option to select his preferred choice, we can still achieve another level of authentication using an OTP mechanism.
- Like, whenever anyone wants to vote, we can send an OTP to his/her registered email id. So that only with that OTP one can complete their process of voting.

c. Ensuring Confidentiality and Integrity in voting system:-

- Confidentiality is to ensure that no one can read the message other than the expected.
- We can ensure confidentiality by making the system secure enough that no outsider would be able to access the information of votes.
- We can use the encryption kind of techniques here, though it is not a text message which is being passed, we can come up with some kind of encryption which can be decrypted and read only with the key which the sender has securely transmitted to the recipient.
- This key transfer mechanism is very important thing to be looked after and there are lot of famous algorithms which securely does this,
- Integrity ensures that votes are not modified and deleted.
- To some extent, integrity can also be achieved using an encryption mechanism, and there must be no other person while an individual is casting his/her vote.
- We can also come up with any of message passing techniques which ensures an acknowledgement is received soon after a person casts his vote. With the help of this we can make sure that the votes are not deleted.

****

5. The series of questions can be in this way:-

- Question;- “You look so young and great, what's your date of birth?
  - From this we can try with his DOB and combinations..
- Question:- “You look so fit.! Do you play any games? What are your hobbies?”
  - From this we can try with his hobbies and combinations.
- Question:- “What’s your favorite movie or shows?”
- Question:- “Whom do you look up to?”
- Question:- “May I borrow your mobile once?”
  - If he/she gives his/her mobile, we can get lot of clues using which we can break the vault.