CSE 345/545: Foundations to Computer Security

HOMEWORK ASSIGNMENT 1 (TOTAL OF 100 POINTS)
Due by 2100hrs on Sept 5, 2018

Plagiarism policies will be strictly enforced.

Part I [10 points]
Classify the below mentioned passwords as very strong, strong, neutral, weak, very weak and also, justify your reasoning. Please keep the response within 20 words for each.
1. Alice
2. Qwerty1234
3. Rat$you
4. Elppa
5. Mumbai
6. Mfiical4W
7. Tif#hom&851@
8. #$\%@$^$^@$@#
9. ecila!0987
10. 45649243

Part II [30 points]
Design an authentication, authorization and identification scheme for visitors, students, faculty, and employees of IIIT-Delhi.

- Describe the complete design of the system and how each of the components will be incorporated?
- Discuss various (at least 3) ways in which attacker might try to spoof the system.
- Give countermeasures that you have taken to avoid the spoofing and other attacks.

Please keep your complete response within 600–900 words.

Part III [45 points]:

a) [30 points] Decipher the following Ciphertext
Slnpzshabylzohssthrluvshdylzwljapunhulzahispzotluavmylspnpvuvywyvopipapunaolmylllelyjpz laolylvmvyhiypknpunaolmyllkvtvmzwlljovyvmaolwylzzvyaolypnoavmaolwlvwslwlhjlhisfavhzz ltislhukavwlapapvuaolnvclyutluamvyhylkylzzvmnyplchujlz nhtl vm aoyvulz zlhzvu lpnoa zwvpslyz qvu zuvd huk khlulyfz ahynhyflu av rpss lhjo vaoly

- Provide the plain text
- Provide working code for reversing this. (Any language)
- Describe the methodology, in detail, used for reversing the cipher text
- The original cipher-text in this question was modified by a TA by appending some random cipher-text at its end. Identify the randomly added **cipher-text**. Which security policy is violated in this case? Explain how.

Hint: It's one of the ciphers covered in class.
Please keep your complete response concise and to the point.

b) [15 points] Write a program (in any language) to decrypt the below cipher-text which was encrypted using Substitution cipher with key - BIRDWATCHNGEFJKLMOPQSUVXYZ

Qcw Hjdhbj lbobdhpw aeyrbqrcwo (Qwolphlckjw lbobdhph) hp b fwdhsf-phzwd lbppwohjw ihod jbqhuw qk Bphb qcbq hp vhdwey dhpqohisqwd. Bp qcw tekibe lklsebqhkj hp rkjphdwowd pqbiew, hq cbp iwwj ehpqwd bp Ewbpq Rkjrwoj kj qcw HSRJ Owd Ehpq phjrw 2004. Hq hp jbqhuw qk qcw Hjdhbj psirkjqhjwjq, Rwjqobe Bphb bjd Fybjfbo

Part IV [15 points]

Pick a secure system (email authentication, etc.) that you are using in everyday life and suggest ways to make it usable. Address the topics that we discussed in class. Keep the answer less than 450 words. In your proposed system, please discuss:

- What usability issues you feel need to be addressed?
- Include some suggestions to improve the system.

Remember there is a trade-off, the scheme should provide reasonable security at least.

Submission guidelines (points will be deducted if not followed):

All the codes/pdf files must be compressed in a zip file which is to be uploaded to Backpack by the deadline. Instructions to run the code must also be included. Do not send assignment by email! No email submissions will be entertained.

FileName : A1_ROLL_NO.zip