BSCH4 - NS

Assignment 2

Crypto time!

All of the following questions have been encrypted using classical encryption techniques discussed in class. Each question is a different technique and each question contains a clue to solving another question. Oh dear it looks like I have also encrypted the instructions. Oh well, guess it means that I cannot use the standard caesar cipher in the questions now which will just make things more difficult. Bummer. I have also included some useful lists that are referenced in the questions. These are left unencrypted because that would just be too cruel. Guess I had better include a clue here so, the left rotation used in the not caesar cipher rotation encrypted question is greater than three but less than the number of Kerschoff principles multiplied by two. Enjoy and remember that your grade is based on your answers and not the decryption.

Useful resources:

A. Wordlist

1. Frozen	6. Joplin	11. Context	16. Guideline
2. Skittle	7. Offensive	12. Yellow	17. Pad
3. Abacus	8. Ingrained	13. Monitor	18. Compliant
4. Trombone	9. Ratchet	14. Fair	19. Asian
5. Chopsticks	10.Moist	15. Time	20. Anchor

B. Passwords

1. Password1

2. P4sswOrdOn3!

3. This20is21my22Passphrase23!!24

4. passcode

C. Hashes

1. 8fc42c6ddf9966db3b09e84365034357 → the

2. 32cdb619196200050ab0af581a10fb83cfc63b1a20f58d4bafb6313d55a3f0e9 → cake

3. a2a551a6458a8de22446cc76d639a9e9 → is

4. 86f7e437faa5a7fce15d1ddcb9eaeaea377667b8 → a

5. c8b1a1a3e6bcee8660ad4a4ab2e2d318295fadc325f85525285f09a16e50ebc4 → lie

6. eb0c28768b1cfe1c105a8c7a2484dd57 → tasty

7. 5ddc2ae17d5b13b4e5b3215177685116565f5058 → cake

D. Access Control

a. 140 permit tcp any any eq 23 log

b. 46 deny any

c. 45 deny host 192.168.32.4

d. 13 allow network 172.168.0.0

e. 101 deny tcp host 10.13.2.1 any neg telnet

Question 1:

Write a security guideline that would enforce the use of the second strongest password given above in password list B. If a computer system could brute force a password at a rate of two to the power of key space hour, show long would it take to brute force password number one and what reason could you give for the actual crack taking so much short. A clue to rail fence the number of rails is the number of a musical word in the word list.

Question 2:

What is involved in the monitor for compliance step of the ten-step process for security policy implementation? Give an example other than a password policy of a security concern that would be covered by a security policy. Explain how a risk assessment would be useful when deciding where to implement a policy. Clue: The column shift cipher question uses the sequence of the first seven words in the word list placed in alphabetic order.

Question 3:
What can you tell about the placement of an access control list just by looking at the number assigned to it? Name two similarities between an access control list and a standard layer three firewall. Which of the lists in given above will allow telnet to any host? The keyword for the play fair cipher is the word with the index equal to the sum of the digits in the access list number of the access list that blocks the file transfer protocol command channel.

Question 4:

Which has his the sha one hash generated from the plain text phrase that has been protected by a caesar cipher below. The plain text phrase should be converted to lower case and all punctuation and white space removed before you hash the value. You should use an online hash function or an offline utility toper form the hash for you. The last hash in the list is the hash of the keyword for question three you can decrypt it using any utility such as hash toolkit dot com. Choose the decrypt sha hash link in the top menu.

MARY HAD A LITTLE LAMB

Question 5:

What does the object identifier id made up of the numbers you get from the following word indexes in the word list above describe in the management information database

frozen abacus joplin frozen skittle frozen context