

CSC 405 Introduction to Computer Security

Homework Assignment #1 Solutions

3. (10 points) Decrypt the following encrypted quotation.

pbegu yymiq icuuf guuyi qguuy qcuiv fiqgu uyqcu qbeme vp

Ciphertext, followed by plaintext:

pbeguuyymiqicuufguuyiqguuyqcuivfiqguuyqcuqbemevp
thecookwasagoodcookascooksgoandascooksgoshewent

The cook was a good cook, as cooks go; and as cooks go she went.

Substitution Key:

abcdefghijklmnopqrstuvwxyz
ihgfedcbazyxwvutsrqponmlkj

6. (10 points) Decrypt the following encrypted quotation.

auqrq rkrzd dmhxx ageho kfalu hkmog rlagm hznhf fhglm hkrlh
mvzmr znvir klhgl vhwod krna przgr jozdl vzkra gmvrv almka
xomah gmvrf zbhka mtqho dwxre dzwmh mzcro imvra khqgz gwwri
zkm

Ciphertext, followed by plaintext:

auqrqrkrzddmhxkagehokfaluhkmoqrlagmhznhf
fghlmhkrhmvzmrznavirkhglvhodwkrnraprzgr
jozdlvzkragmvrvwalmkaxomahgmvrfzbhkamtqho
dwxredzwmhmzcroimvrakhqgzgwwrizkm

ifwewerealltobringourmisfortunesintoacom
monstoresothateachpersonshouldreceiveane
qualshareinthedistributionthemajoritywou
ldbeglادتotakeuptheirownanddepart

If we were all to bring our misfortunes into a common store so that each person should receive an equal share in the distribution, the majority would be glad to take up their own and depart.

Substitution Key:

abcdefghijklmnopqrstuvwxyz
zxnwruvabcmfghijklmopqsty

10. (10 points) Decrypt the following encrypted quotation.

mszcx ijddj nzatm lrkdj mlwmc qrktj tnwir zatnj bxdrj amlrs
zxrzd dbjbc wsrir mlrxc icnic qrkza tmlrb cbriz mlkco mnizx
r

Ciphertext, followed by plaintext
mszcxijddjnzatmlrkdjmlwmcqrktjtnwirzatnj
bxdrjamlrszxrzddbkbkwsrirmlrxcicnicqrkza
tmlrbcbrizmlkcomnizxr

twasbrilligandtheslithytovesdidgyreandgi
mbleinthewabeallmimsyweretheborogrovesan
dthemomerathsoutgrabe

'Twas brillig and the slithy toves did gyre and gimble in the wabe; all mimsy were the Borogroves, and the momeraths outgrabe.

Substitution Key:
abcdefghijklmnopqrstu vwxyz
zxvtrpnljhfd bacegikmoqsuwy

14. (10 points) Does a substitution need to be a permutation of the plaintext symbols? Why or why not?

No. A substitution can be to an entirely different alphabet. (As an example, read the Arthur Conan Doyle Sherlock Holmes "Case of the Dancing men.") One plaintext symbol can convert to several ciphertext symbols, or vice versa. For example, Morse code is a form of substitution of alphabetic letters to dots and dashes. Two plaintext characters could map the same ciphertext character as long as the recipient could distinguish between the two.

15. (10 points) Explain why the product of two relatively simple ciphers, such as a substitution and a transposition, can achieve a high degree of security.

Each cipher contributes its own strength, so ideally the strength of the product is at least the product of the strengths of the input ciphers. A substitution cipher contributes confusion, whereas a transposition performs diffusion. The DES and AES algorithms both use a combination of relatively simple functions. Obviously, however, just composing two ciphers is not guaranteed to result in a stronger combination.

16. (10 points) How would you test a piece of ciphertext to determine quickly if it was likely the result of a simple substitution?

Letter frequency count, followed by digram and trigram count.

17. (10 points) How would you test a piece of ciphertext to determine quickly if it was likely the result of a transposition?

Letter frequency count.

18. (10 points) Suggest a source of a very long sequence of unpredictable numbers. Your source must be something that both the sender and receiver can readily access but that is not obvious to outsiders and is not transmitted directly from sender to receiver.

Shared books, messages from broadcasts, content of (static) web pages.

19. (10 points) Given the speed of a current ordinary computer (for home or light office use), estimate the amount of time necessary to crack a DES encryption by testing all 2^{56} possible keys. Make a similar estimate for a 128-bit AES key.

Note: For this question, the exact answer is not as important as how the answer was derived. One sample solution is given as below.

We assume that the household computer has a 2GHZ processor. Also we assume that a machine takes a hundred cycles per brute force against a single 56-bit DES key or 128 bit AES key.

To crack a DES encryption, we need:

$(2^{56} \text{ key}) * 100 \text{ cycles} / 60 \text{ sec} / 60 \text{ min} / 24 \text{ hour} / 365 \text{ days} / 2000000000 \text{ hz} = 114.246566$
years

To crack a AES encryption, we need:

$(2^{128} \text{ key}) * 100 \text{ cycles} / 60 \text{ sec} / 60 \text{ min} / 24 \text{ hour} / 365 \text{ days} / 2000000000 \text{ hz} = 5.39514154 \times$
1023 years

22. (10 points) List three applications in which a stream cipher would be desirable. Are applications for block ciphers more prevalent? Why or why not? Why do you think this is true?

Note: There is no strict answer for this question. As soon as your explanation is reasonable, you will get full credit.