1. In the field of information security, Kerckhoffs' Principle is like motherhood and apple pie, all rolled up into one.

a. Define Kerckhoffs' Principle in the context of cryptography.

b. Give a real-world example where Kerckhoffs' Principle has been violated. Did this cause any security problems?

c. Kerckhoffs' Principle is sometimes applied more broadly than its strict cryptographic definition. Give a definition of Kerckhoffs' Principle that applies more generally.

a-The fundamental principle of cryptography that the inner workings of a cryptosystem are completely known to the attacker. The only secret is a key. Keeping cryptosystem secure with these conditions is known as Kerckhoffs’ principle

b-Microsoft’s Network LAN Manager (NTLM) violated Kerckhoffs’ Principle. NTLMauthentication service allowed attacker to use Rainbow attack. In this attack, even if attacker does not know the secret key, he can break the system using pre-computed directory of encrypted passwords. Hence, this violation of Kerckhoffs’ principle did causes ecurity issues in NTLM suite and another oneA house lock is an example of a mechanism whose inner workings are completely known, but this has posed a problem, as people have devised many various ways to break through the lock

c-Kerckhoff’s Principle can be applied in various aspects of security other thancryptography. The principle is taken to mean that security design is open to public scrutiny. This means people can expose security flaws in the design. If the system stands this scrutiny, it is more secure

Q2-Edgar Allan Poe's 1843 short story, "The Gold Bug," features a cryptanalytic attack.

a. What type of cipher is broken and how?

b. What happens as a result of this cryptanalytic success?

a- The cipher that is broken is a simple substitution. This cipher is broken by doing a letter frequency count. Comparing symbol frequency count with the English letter frequency count and then replacing the symbols in the cipher-text with letters by order of occurrence

or

The cypher in the story is simple substitution cypher and it is broken using frequency analysis

b- The success made it so that there are shortcuts for seemingly impossibly large amount of keys to try. Can’t just use simple substitution. Seems like there are 26 factorial keys but you need better confusion that statistical analysis cannot be useful in. And so, evolved cryptanalysis

.or

.Due to this cryptanalytic success, a hidden fortune is discovered in form of a chest filled with gold coins and jewelry

Given that the Caesar's cipher was used, find the plaintext that corresponds

to the following ciphertext:

VSRQJHEREVTXDUHSDQWU

Plaintext◊SPONGEBOBSQUAREPANTS

5. Suppose that we have a computer that can test 2^40 keys each second.a. What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^88?

2^88/2^40= 248248seconds/60/60/24/365 = 8,925,512 years. Assume 365 days, non leap-year.

b. What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2112?

c. What is the expected time (in years) to find a key by exhaustive search if the keyspace is of size 2^256?

2^256/2^40= 22162216seconds/60/60/24/365 = 3.3394309e+57 years. Assume 365 days, nonleap-year.

.

Q6-The weak ciphers used during the election of 1876 employed a fixed permutation of the words for a given length sentence. To see that this is weak, find the permutation of ( 1 , 2 , 3 , . . . , 10) that was used to produce the scrambled sentences below, where "San Francisco" is treated as a single word. Note that the same permutation was used for all three sentences.

first try try if you and don't again at succeed

only you you you as believe old are are as

winter was in the I summer ever San Francisco coldest spent

***Nahi smjh arha mjhe***

Q7-The weak ciphers of the election of 1876 used a partial codebook and a permutation of the words. Modify this approach so that it is more secure

Ans-) In election of 1876 , Partial codebook was used, Use a permutation only once or a very limited number of times. Could book could also be more comprehensive to avoid giving away too much context

8. This problem deals with the concepts of confusion and diffusion

a. Define the terms confusion and diffusion as used in cryptography.

b. Which classic cipher discussed in this chapter employs only confusion?

c. Which classic cipher discussed in this chapter employs only diffusion?

d. Which cipher discussed in this chapter employs both confusion and

diffusion?

Ans No.a

In [cryptography](https://en.wikipedia.org/wiki/Cryptography), **confusion** and **diffusion** are two properties of the operation of a secure [cipher](https://en.wikipedia.org/wiki/Cipher) identified by [Claude Shannon](https://en.wikipedia.org/wiki/Claude_Elwood_Shannon)

1. Confusion :

1-Confusion is a cryptographic technique which is used to create faint cipher texts

2- This technique is possible through substitution algorithm.

3- In confusion, if one bit within the secret’s modified, most or all bits within the cipher text also will be modified.

4- In confusion, vagueness is increased in resultant.

5- Both stream cipher and block cipher uses confusion

6- The relation between the cipher text and the key is masked by confusion

1. Diffusion

1-diffusion is used to create cryptic plain texts.

2- While it is possible through transportation algorithm.

3- While in diffusion, if one image within the plain text is modified, many or all image within the cipher text also will be modified

4- While in diffusion, redundancy is increased in resultant.

5- Only block cipher uses diffusion

**Ans No.b**

One-time pad

**Ans No.c**

Double transposition is the example of classic cypher which employs only diffusion.Plaintext is arranged in matrix form and rows and columns are shuffled to get the cipher text

**Ans No.d**

Ciphers of the Election of 1876 are examples of cypher which employ both confusion and diffusion. Codebook is used as confusion step and permutation of words is used as diffusion step

10. Determine the plaintext and key for the cipher text that appears in the *Alice in Wonderland* quote at the beginning of this chapter. Hint: “The message was encrypted with a simple substitution cipher and the plaintext has no spaces or punctuation.”

MXDXBVTZWVMXNSPBQXLIMSCCSGXSCJXBOVQXCJZMOJZCVC

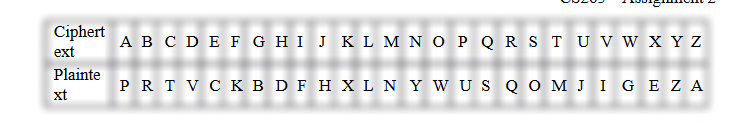
TVWJCZAAXZBCSSCJXBQCJZCOJZCNSPOXBXSBTVWJC

JZDXGXXMOZQMSCSCJXBOVQXCJZMOJZCNSPJZHGXXMOSPLH

JZDXZAAXZBXHCSCJXTCSGXSCJXBOVQX

 plaintext from Lewis Carroll, *Alice in Wonderland*

Plaintext: NEVER IMAGINE YOURSELF NOT TO BE OTHERWISE THAN WHAT ITMIGHT APPEAR TO OTHERS THAT WHAT YOU WERE OR MIGHTHAVE BEEN WAS NOT OTHERWISE THAN WHAT YOU HAD BEEN WOULDHAVE APPEARED TO THEM TO BE OTHERWISEKey



12. Write a program to help an analyst decrypt a simple substitution cipher. Your program should take the cipher text as input, compute letter frequency counts, and display these for the analyst. The program should then allow the analyst to guess a key and display the results of the corresponding "decryption" with the putative key.

import java.io.BufferedReader;

import java.io.IOException;

import java.io.InputStreamReader;

import java.util.HashMap;

import java.util.LinkedHashMap;

import java.util.Map;

public class SubstitutionCipher

Map letterFreqMap;

Map key;

String ciphertext;

String plaintext;

BufferedReader reader;

private void createInputBuffer()

reader = new BufferedReader(new InputStreamReader(System.in));

private void closeInputBufer() throws Exception

if(reader!=null)

try

reader.close();

catch (IOException e)

e.printStackTrace();

throw new Exception(Error while trying to close the input stream);

private void getCipherText() throws Exception

System.out.println(\*\*\*\*\* Substitution Cipher Cracker \*\*\*\*\*);

System.out.print(Enter ciphertext: );

reader =...

13. Extend the program described in Problem 12 so that it initially tries to decrypt the message. One sensible way to proceed is to use the computed letter frequencies and the known frequencies of English for an initial guess at the key. Then from the resulting putative decryption,count the number of dictionary words that appear and use this as a

score. Next, for each letter in the key, try swapping it with the letterthat is adjacent (with respect to frequency counts) and recompute the score. If the score improves, update the key; if not, don't change theputative key. Iterate this process until the score does not improve for a entire pass through the alphabet. At this point you will give your putativedecryption to the analyst. To aid the analyst in the manual phase,your program must maintain all of the functionality of the program in

Problem 12.

<http://ddsgibberish.blogspot.com/2015/09/autosolve-substitution-cipher.html>

14. Encrypt the message **we are all together** using a double transposition cipher (of the type described in the text) with 4 rows and 4 columns, using the row permutation

(1,2,3,4)—> (2,4,1,3)

and the column permutation

(1,2,3,4)—\* (3,1,2,4)



15. Decrypt the ciphertext

IAUTMDCSMNIMREBOTNELSTRHEREOAEVMWIH

TSEEATMAEOHWHSYCEELTTEOHMUOUFEHTRFT

This message was encrypted with a double transposition (of the typediscussed in the text) using a matrix of 7 rows and 10 columns. Hint:The first word is "there."

Ans

There are some who say that communism is the wave of the future, let them come to Berlin

16. Outline an automated attack on a double transposition cipher (of the type discussed in the text), assuming that the size of the matrix is known.

17. A double transposition cipher can be made much stronger by using the

following approach. First, the plaintext is put into *an n x m* array,

as described in the text. Next, permute the columns, and then write

out the intermediate ciphertext column by column. That is, column 1

gives the first *n* ciphertext letters, column 2 gives the next n, and so

on. Then repeat the process, that is, put the intermediate ciphertext

into a n n x m array, permute the columns, and write out the ciphertext

column by column. Use this approach, with a 3 x 4 array, and permutations

(2,3,1,4) and (4, 2,1,3) to encrypt the plaintext attackatdawn.

18. Using the letter encodings in Table 2.1, the following two ciphertext

messages were encrypted with the same one-time pad:

KHHLTK and KTHLLE.

Find all possible plaintexts for each message and the corresponding

one-time pad.

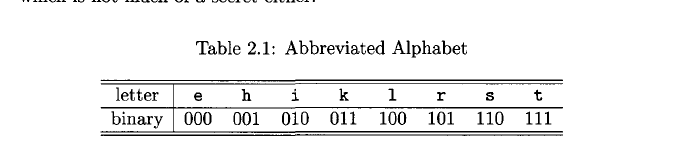
19. Using the letter encodings in Table 2.1, the following ciphertext message

was encrypted with a one-time pad:

KITLKE.

a. If the plaintext is "thrill," what is the key?

b. If the plaintext is "tiller," what is the key?



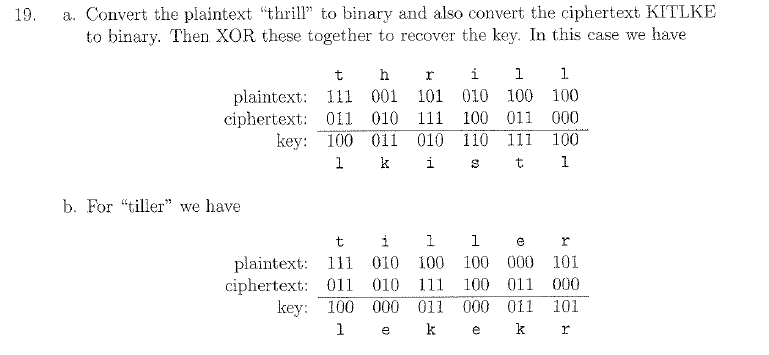
19. Using the letter encodings in Table 2.1, the following ciphertext message

was encrypted with a one-time pad:

KITLKE.

a. If the plaintext is "thrill," what is the key?

b. If the plaintext is "tiller," what is the key?



20. Suppose that you have a message consisting of 1024 bits. Design a

method that will extend a key that is 64 bits long into a string of 1024

bits, so that the resulting 1024 bits can be XORed with the message,

just like a one-time pad.

Easy way to extend a 64 bit length is to just repeat by multiplying it by (24)16 to achievea length of 1024 bits. And since they are the same length, they can be XORed

Is the resulting cipher as secure as a one-timepad?

No, because while they are of the same length, the one-time pad uses wholly random keyof distinct 1024 bits. While, the 64 bit extension uses repeating keys

Is it possible for any such cipher to be as secure as a one-time

pad?

The one-time pad seems to be the only provable secure one since you have to assumealgorithms are known but specific keys are not.The one-time pad makes sure the key iswholly random and due to that, all plaintexts are equally likely

21. Design a codebook cipher that can encrypt any block of bits, not just

specific words. Your cipher should include many possible codebooks,

with a key used to determine which codebook will be employed to encrypt

(or decrypt) a particular message. Discuss some possible attacks

on your cipher.

22. Suppose that the following is an excerpt from the decryption codebook

for a classic codebook cipher.

123

199

202

221

233

332

451

once

or

maybe

twice

time

upon

a

Decrypt the following ciphertext:

242, 554, 650, 464, 532, 749, 567

assuming that the following additive sequence was used to encrypt the

message:

119, 222, 199, 231, 333, 547, 346

Decrypt the following cipher-text242, 554, 650, 464, 532, 749, 567Assuming that the following additive sequence was used to encrypt the message:119, 222, 199, 231, 333, 547, 346Additive was used to encrypt so you minus the additive from the cipher-text to create:123, 332, 451, 233, 199, 202, 221Which, after you use the codebook comes to:Once upon a time or maybe twice.

26. In the this chapter, we discussed a forward search attack.

a. Explain how to conduct a forward search attack.

To conduct a forward search attack you attack a public key. You suspect that the text issome text(book says “yes” or “no”) and encrypt the possibility text with the public key.And by comparing your cipher-text with the intercepted cipher-text, comparisons with thei ntercepted cipher-text and the cipher-text you create with the public key can lead to aleak

b. How can you prevent a forward search attack against a public key cryptosystem?

To prevent a forward search attack against a public key you need to have a biggermessage space so that the message is not predictable enough to be attacked in this way.Source: me, thinking with the book as a resource

c. Why can't a forward search attack be used to break a symmetric cipher?

A forward search attack cannot break a symmetric cipher because the hacker does nothave a public key to play with.