浙江大學

《Big Data Security and Privacy Protection》

Set 1

题　　目： set 1

上课时间： August 24th

授课教师： Rongxing Lu

姓　　名： 杜宗泽

学　　号： 3220105581

组　　别： 个人

日　　期： 8月24日

1 Question 1

1. Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash. Give examples of confidentiality, integrity, and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirement.)

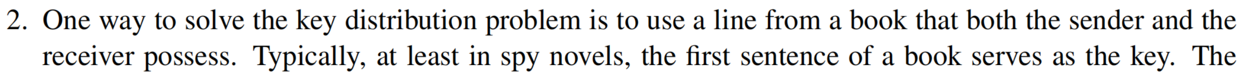
My answer:

Confidentiality, integrity, and availability are three key aspects of information security. In the context of an automated cash deposit machine, here are examples of requirements for each aspect:

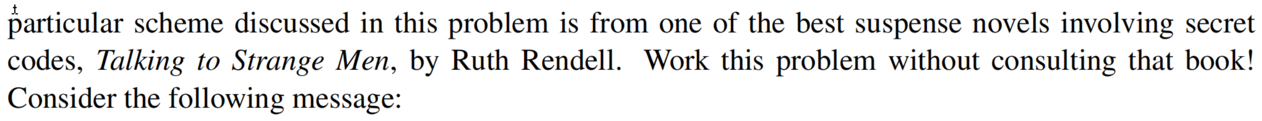
1. Confidentiality:
   - Requirement: User account information should be kept confidential and protected from unauthorized access.
   - Importance: High. Maintaining the confidentiality of user account information is crucial to prevent identity theft, fraud, and unauthorized transactions.
2. Integrity:
   - Requirement: Cash deposits should be accurately recorded and credited to the correct user account without any tampering or alteration.
   - Importance: High. Ensuring the integrity of cash deposits is crucial to maintain trust in the system and prevent financial discrepancies or disputes.
3. Availability:
   - Requirement: The cash deposit machine should be available and operational for users to deposit cash at any time.
   - Importance: High. Availability is critical for users who rely on the machine to deposit cash conveniently. Downtime or unavailability may inconvenience users and impact their trust in the system.

It's important to note that the importance of these requirements may vary depending on the specific context and the organization's risk assessment. These examples provide a general understanding of the confidentiality, integrity, and availability requirements associated with an automated cash deposit machine.

2 Question 2

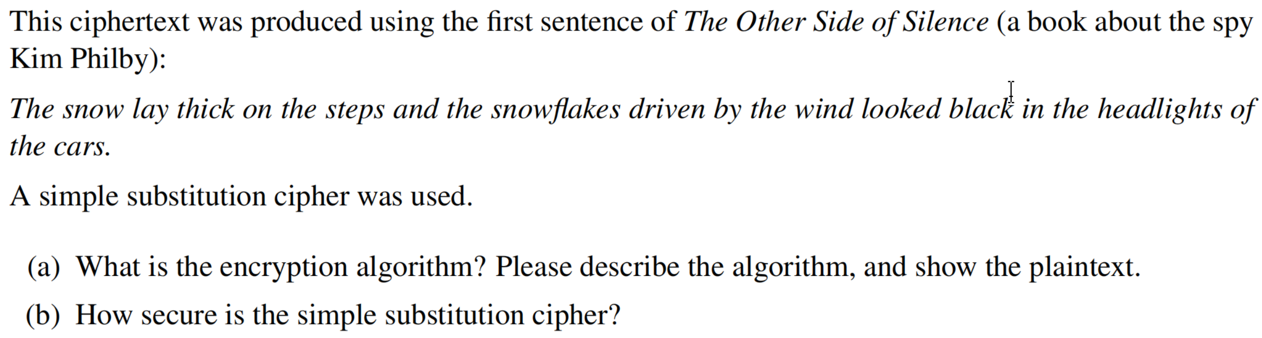


2. One way to solve the key distribution problem is to use a line from a book that both the sender and the receiver possess. Typically, at least in spy novels, the first sentence of a book serves as the key. The



particular scheme discussed in this problem is from one of the best suspense novels involving secret codes, *Talking to Strange Men*, by Ruth Rendell. Work this problem without consulting that book! Consider the following message:

```
SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA
```



This ciphertext was produced using the first sentence of *The Other Side of Silence* (a book about the spy Kim Philby):

The snow lay thick on the steps and the snowflakes driven by the wind looked black in the headlights of the cars.

A simple substitution cipher was used.

(a) What is the encryption algorithm? Please describe the algorithm, and show the plaintext.

(b) How secure is the simple substitution cipher?

My answer:

(a) The encryption algorithm used in this case is a simple substitution cipher. In a simple substitution cipher, each letter in the plaintext is replaced with a corresponding letter from the ciphertext according to a fixed substitution rule.

To decrypt the given ciphertext, we need to find the corresponding plaintext letters based on the substitution rule. In this case, the substitution rule is based on the first sentence of the book "The Other Side of Silence" by using the snowflakes as a key.

The plaintext can be obtained by replacing each ciphertext letter with the corresponding letter from the substitution rule. Here is the plaintext:

`SIDKHKDM AF HCRKIABIE SHIMC KD LFEAILA`
becomes
`BASILISK TO LEVIATHAN BLAKE IS CONTACT`

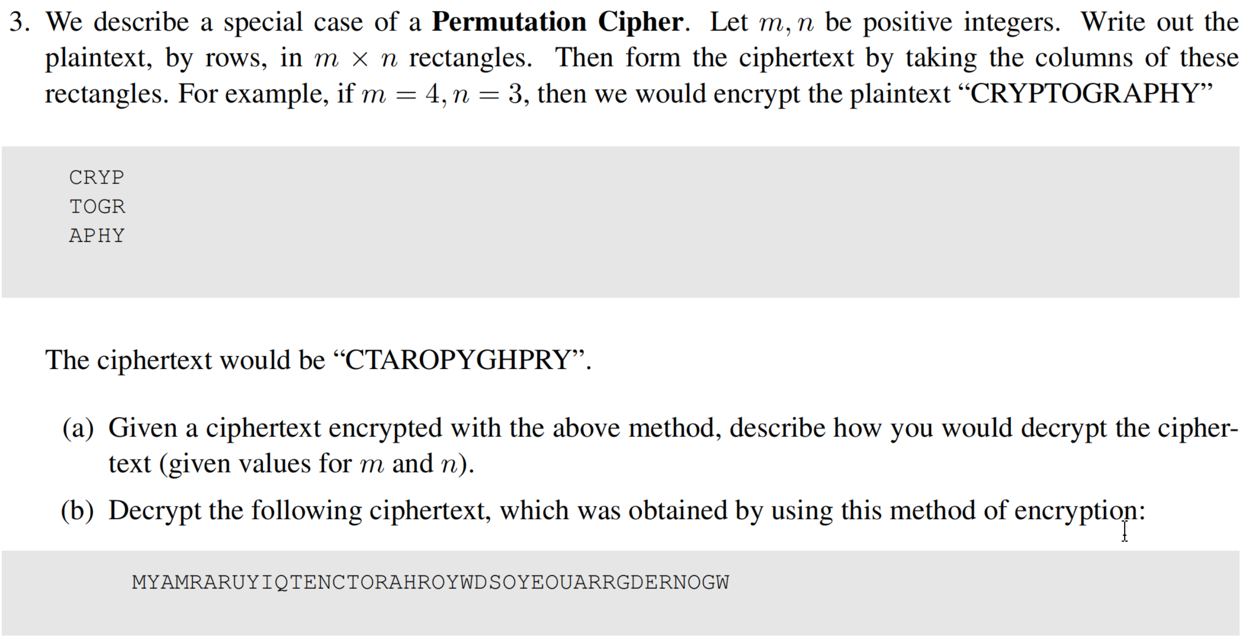
The reason is that the substitution rule is that the letter in turn in the given sentence is corresponding to the alphabetical.(eg: $s \rightarrow a\backslash\ i \rightarrow b\backslash\ d \rightarrow s$)

(b) The simple substitution cipher is not considered secure. It is vulnerable to frequency analysis attacks, where an attacker can analyze the frequency of letters in the ciphertext and compare it to the expected frequency of letters in the language being used (in this case, English). By identifying the most frequently occurring letters in the ciphertext, an attacker can make educated guesses about the corresponding plaintext letters.

Additionally, the simple substitution cipher does not provide any form of key management or key distribution, making it susceptible to brute-force attacks. An attacker can try all possible substitution rules until the correct one is found.

Overall, the simple substitution cipher is a relatively weak encryption algorithm and is not recommended for secure communication.

3 Question 3



3. We describe a special case of a **Permutation Cipher**. Let m, n be positive integers. Write out the plaintext, by rows, in $m \times n$ rectangles. Then form the ciphertext by taking the columns of these rectangles. For example, if $m = 4, n = 3$, then we would encrypt the plaintext “CRYPTOGRAPHY”

```
CRYP
TOGR
APHY
```

The ciphertext would be “CTAROPYGHPRY”.

(a) Given a ciphertext encrypted with the above method, describe how you would decrypt the ciphertext (given values for m and n).

(b) Decrypt the following ciphertext, which was obtained by using this method of encryption:

```
MYAMRARUYIQTENCTORAHROYWDSOYEOUARRGDERNOGW
```

My answer:

In this question, we can use the python to help us solve it easily.

(a) how you would decrypt the cipher text (given values for m and n).

1. Partition the ciphertext into blocks of m, n letters.

2. use python to rearrange the block.(just transpose the matrix and print in a line)

```python
string = "CTAROPYGHPRY"

matrix = [string[i:i+3] for i in range(0, len(string), 3)]

transposed_matrix = ["".join(row) for row in zip(*matrix)]

output = "".join(matrix)

print(output)
```

(b) in this question, I have to acknowledge that I use the google because I don't be conscious of the ciphertext matrix could be partitioned in blocks before transposed. Google shows me that this encryption is called "Rail Fence Cipher".

The decrypt Python code:

```python
import re
```

```python

print("*****Rail Fence Cipher*****")

string = "MYAMRARUYIQTENCTORAHROYWDSOYEOUARRGDERNOGW"
m_ = []

for f in range(len(string)):
    if len(string) % (f + 1) == 0 and f > 0:
        m_.append(f + 1)

# print(m_)

for p in m_:
    print("\nGrouping into ", p, " characters per group, total ", int(len(string) / p), " groups", sep='')
    part = re.findall(r'.{%s}' % p, string)  # Grouping every p characters
    for q in range(p):
        if p % (q + 1) == 0:
            print("Each group ", q + 1, "x", int(p / (q + 1)), sep='')
            for each_part in part:
                for i in range(q + 1):
                    str_part = each_part[i::q + 1]  # [start:end:step] step defaults to 1
                    print(str_part, end='')
                # The next line controls the space, whether to include it or not
                print(" ", end='')
            print()

```

The operation results are as follows:

```
yaoyaoling@localhost ~/c/test> python3 test.py
*****Rail Fence Cipher*****

Grouping into 2 characters per group, total 21 groups
Each group 1x2
MY AM RA RU YI QT EN CT OR AH RO YW DS OY EO UA RR GD ER NO GW
Each group 2x1
MY AM RA RU YI QT EN CT OR AH RO YW DS OY EO UA RR GD ER NO GW

Grouping into 3 characters per group, total 14 groups
Each group 1x3
MYA MRA RUY IQT ENC TOR AHR OYW DSO YEO UAR RGD ERN OGW
Each group 3x1
MYA MRA RUY IQT ENC TOR AHR OYW DSO YEO UAR RGD ERN OGW

Grouping into 6 characters per group, total 7 groups
Each group 1x6
MYAMRA RUYIQT ENCTOR AHROYW DSOYEO UARRGD ERNOGW
Each group 2x3
MARYMA RYQUIT ECONTR ARYHOW DOESYO URGARD ENGROW
Each group 3x2
MMYRAA RIUQYT ETNOCR AOHYRW DYSEOO URAGRD EORGNW
Each group 6x1
MYAMRA RUYIQT ENCTOR AHROYW DSOYEO UARRGD ERNOGW

Grouping into 7 characters per group, total 6 groups
```

```
Each group 1x7
MYAMRAR UYIQTEN CTORAHR OYWDSOY EOUARRG DERNOGW
Each group 7x1
MYAMRAR UYIQTEN CTORAHR OYWDSOY EOUARRG DERNOGW

Grouping into 14 characters per group, total 3 groups
Each group 1x14
MYAMRARUYIQTEN CTORAHROYWDSOY EOUARRGDERNOGW
Each group 2x7
MARRYQEYMAUITN COARYDOTRHOWSY EURGENGOARDROW
Each group 7x2
MUYYAIMQRTAERN COTYOWRDASHORY EDOEURANRORGGW
Each group 14x1
MYAMRARUYIQTEN CTORAHROYWDSOY EOUARRGDERNOGW

Grouping into 21 characters per group, total 2 groups
Each group 1x21
MYAMRARUYIQTENCTORAHR OYWDSOYEOUARRGDERNOGW
Each group 3x7
MMRIETAYRUQNOHAAYTCRR ODYUREOYSEAGRGWOORDNW
Each group 7x3
MUCYYTAIOMQRRTAAEHRNR OEDYOEWURDANSROORGYGW
Each group 21x1
MYAMRARUYIQTENCTORAHR OYWDSOYEOUARRGDERNOGW

Grouping into 42 characters per group, total 1 groups
Each group 1x42
MYAMRARUYIQTENCTORAHROYWDSOYEOUARRGDERNOGW
Each group 2x21
MARRYQECOARYDOEURGENGYMAUITNTRHOWSYOARDROW
Each group 3x14
MMRIETAODYUREOYRUQNOHYSEAGRGAAYTCRRWOORDNW
Each group 6x7
MREADUEYUNHSARAYCRORNMITOYRORQOYEGGATRWODW
Each group 7x6
MUCOEDYYTYOEAIOWURMQRDANRTASROAEHORGRNRYGW
Each group 14x3
MCEYTOAOUMRARARAHRRRGUODYYEIWRQDNTSOEOGNYW
Each group 21x2
MOYYAWMDRSAORYUEYOIUQATRERNGCDTEORRNAOHGRW
Each group 42x1
MYAMRARUYIQTENCTORAHROYWDSOYEOUARRGDERNOGW
```

Conclusion: The meaningful result is the situation where each group is divided into 2x3 fences for every 6 groups of 1, a total of 7 groups. The result is `MARY MARY QUITE CONTRARY HOW DOES YOUR GARDEN GROW`