Assignment #1:

Department: Department of Mathematics / College of Natural Science

ID: 20212211

Name: 권대호

Q1. (5 points) For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.

a. A student maintaining a blog to post public information.

   A. Confidentiality: Low. A blog post, being publicly accessible for anyone to view, is unrelated to confidentiality.

   B. Integrity: Moderate. If the integrity of public information is compromised, it is a concern in and of itself. However, given the nature of public information, the ability for others to access and make comparisons from various sources mitigates the severity of the issue.

   C. Availability: Low. Not being able to post on the blog immediately or access public information on the blog right away is not a significant issue. Public information can be accessed through other channels, so the situation is not critical.

b. An examination section of a university that manages sensitive information about exam papers.

   A. Confidentiality: High. If information about the exam itself is leaked to unauthorized individuals, it can disrupt the proper conduct of the exam and undermine its credibility. This is critically important from the university's perspective.

   B. Integrity: High. It concerns the integrity of exam questions or answers. This is even more critical because exams are designed to evaluate students' academic abilities, and any compromise in the integrity of exam materials can result in unacceptable circumstances.

   C. Availability: Moderate. These days, there are cases where exams are conducted online, which can indeed introduce potential issues. However, for most exams where materials are printed days in advance, even if availability is temporarily compromised, there may not be an immediate problem. Exam grading, while it may experience some delays, is generally not rendered impossible.

c. An information system in a pathological laboratory maintains the patient's data.

   A. Confidentiality: High. Patient's data is considered personal information, and unauthorized disclosure to anyone can lead to legal issues.

   B. Integrity: High. If the data is corrupted or altered, there is a risk that the research results may be distorted.

   C. Availability: High. Given the nature of a laboratory, there is a potential need to add or modify data promptly, making availability crucial.

d. A student information system used for maintaining student data in a university that contains both personal and academic information and routine administrative information (not privacy-related). Assess the impact for the two data sets separately and the information system as a whole.

   A. personal and academic information.

      i. Confidentiality: High. Personal information is associated with legal issues, and its disclosure could potentially lead to identity theft and fraud. Furthermore, the leak of such information can damage the university's reputation.

      ii. Integrity: High. Students encounter situations where they must authenticate themselves, such as class attendance, taking exams, seeking academic support, etc. Academic information contains grades, attendance, etc., and these pieces of information are significant to the university. If the integrity of personal information is breached, students may struggle to establish their identity, and the university cannot tolerate such a scenario.

iii. Availability: Moderate. Personal information and academic records, such as attendance and grades, are not necessarily required for immediate access, as adjustments can be made later. Therefore, their availability is not considered extremely high.

B. Routine administrative information (not privacy-related).

i. Confidentiality: Moderate. While the routine administrative information itself does not contain private personal information, the long-term concern lies in the possibility of third-parties utilizing the system's information for other purposes.

ii. Integrity: High. If the integrity of the routine administrative information is compromised, it can potentially disrupt common academic processes.

iii. Availability: Moderate. It is crucial during peak periods of access such as "Grade submission period", but not as concerning for routine administrative information, as there is potential for recovery at a later time.

C. Information system as a whole.

i. Confidentiality: High. Overall, the academic system contains personal information of individual students, and any unauthorized disclosure could lead to serious legal implications.

ii. Integrity: High. As mentioned above, if the information of individual students is corrupted, there is a significant potential for disruptions in the progress of academic schedules.

iii. Availability: Moderate. Immediate data access may result in minor issues, but as long as there is no long-term data inaccessibility, recovery should be possible later on.

e. A university library contains a library management system that controls the distribution of books amongst the students of various departments. The library management system contains both the student data and the book data. Assess the impact for the two data separately and the information system as a whole.

A. Student data

i. Confidentiality: High. While the student information in the university library may be less extensive than the information in the academic system, it still constitutes personal data and carries legal responsibilities if exposed.

ii. Integrity: Moderate. The core of the library system is centered on the status of book borrowing and returns, if there are issues with this information, as it may be irreparable later.

iii. Availability: Moderate. Take such as borrowing, returns, and access control can be manually managed for the short-term, so immediate data access may not be critical even if it's unavailable for the time being.

B. Book data

i. Confidentiality: Low. Book data is not considered personal information, so it is not closely related to confidentiality.

ii. Integrity: Moderate. Book data can be corrected promptly in the event of errors, and its unlikely to lead to significant issues.

iii. Availability: Moderate. Book data can also be manually managed in the short term without the need for immediate additions, deletions, or queries.

C. Information system as a whole

i. Confidentiality: High. The book data itself is fine, but we must be careful with personal information storage.

ii. Integrity: Moderate. Both book data and personal information can be corrected in case of errors.

iii. Availability: Moderate. Both book data and personal information can be managed manually for the time being, and it won't be a problem to add information once the system is restored.

Q2. (2 points) A fundamental cryptographic principle states that all messages must have redundancy. But we also know that redundancy helps an intruder tell if a guessed key is correct. Consider two forms of redundancy. First, the initial n bits of the plaintext contain a *known pattern*. Second, the final n bits of the message contain a hash over the message. From a security point of view, are they equivalent? Discuss your answer.

No. they are not equivalent. The known pattern in the initial n bits of plaintext introduces a direct vulnerability by providing predictable information. Conversely, adding a hash at the end of the message primarily focuses on data integrity and does not address the predictability of the plaintext.

Q3. (2 points) Suppose that a message has been encrypted using DES in ciphertext block chaining mode. One bit of ciphertext in block C_i is accidentally transformed from a 0 to a 1 during transmission. How much plaintext in block C_{i+1} received by the receiver will be garbled as a result?

In CBC mode, each ciphertext block depends on the previous ciphertext block and the current plaintext block. If we are in the situation where the block number is i+1, and the ith block is manipulated as mentioned, then both the ith block and the i+1th block will be garbled as a result.

Q4. (2 points) The following ciphertext was generated using a simple substitution algorithm. Find the key and the plaintext.

ciphertext

hzsrnqc klyy wqc flo mflwf ol zqdn nsoznj wskn lj xzsrbjnf,
wzsxz gqv zqhhnf ol ozn glco zlfnco hnlhrn; nsoznj jnrqosdnc
lj fnqj kjsnfbc, wzsxz sc xnjoqsfrv gljn efeceqr. zn rsdnb
qrlfn sf zsc zlecn sf cqdsrrn jlw, wzsoznj flfn hnfnojqonb.
q csfyrn blgncosx cekksxnb ol cnjdn zsg. zn pjnqmkqconb qfb
bsfnb qo ozn xrep, qo zlejc gqozngqosxqrrv ksanb, sf ozn cqgn
jllg, qo ozn cqgn oqprn, fndnj oqmsfy zsc gnqrc wsoz loznj
gngpnjc, gexz rncc pjsfysfy q yenco wsoz zsg; qfb wnfo zlgn
qo naqxorv gsbfsyzo, lfrv ol jnosjn qo lfxn ol pnb. zn fndnj
ecnb ozn xlcv xzqgpnjc wzsxz ozn jnkljg hjldsbnc klj soc
kqdlejnb gngpnjc. zn hqccnb onf zlejc leo lk ozn ownfov-klej
sf cqdsrrn jlw, nsoznj sf crnnhsfy lj gqmsfy zsc olsrno.

Key

Plain	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	R	S	T	U	V	W	X	Y
Cipher	Q	P	X	B	N	K	Y	Z	S	M	R	G	F	L	H	J	C	O	E	D	W	A	V

plaintext

phileas fogg was not known to have either wife or children,
which may happen to the most honest people; either relatives
or near friends, which is certainly more unusual. he lived
also in his house in saville row, whither none penetrated.
A single domestic sufficed to serve him. he breakfasted and
dined at the club, at hours mathematically fixed, in the same
room, at the same table, never taking his meals with other
members, much less bringing a guest with him; and went home
at exactly midnight, only to retire at once to bed. he never
used the cosy chambers which the reform provides for its
favored members. he passed ten hours out of the twenty-four
in saville row, either in sleeping or making his toilet.

Q5. (2 points) Using the Vigenère cipher, encrypt the word "explanation" using the key "leg".

Key	L	E	G	L	E	G	L	E	G	L	E
Plain	e	x	p	l	a	n	a	t	i	o	n
Cipher	P	B	V	W	E	T	L	X	O	Z	R

Result: explanation -> pbvwetlxozr

Q6. (2 points) This problem explores the use of a one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5…, then the first letter of the plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

(a) Encrypt the plaintext "send more money" with the keystream 9 0 1 7 23 15 21 14 11 11 2 8 9

Plain	S	E	N	D	M	O	R	E	M	O	N	E	Y
Key	9	0	1	7	23	15	21	14	11	11	2	8	9
Cipher	B	E	O	K	J	D	M	S	X	Z	P	M	H

Result: SENDMOREMONEY -> BEOKJDMSXZPMH

(b) Using the ciphertext produced in part (a), find a key so that the ciphertext decrypts to the plaintext "cashnotneeded."

Cipher	B	E	O	K	J	D	M	S	X	Z	P	M	H
Key	Z	E	W	D	W	P	T	F	T	V	M	I	E
Plain	C	A	S	H	N	O	T	N	E	E	D	E	D

Result: ZEWDWPTFTVMIE

Q7. (5 points) For the following ciphertext:

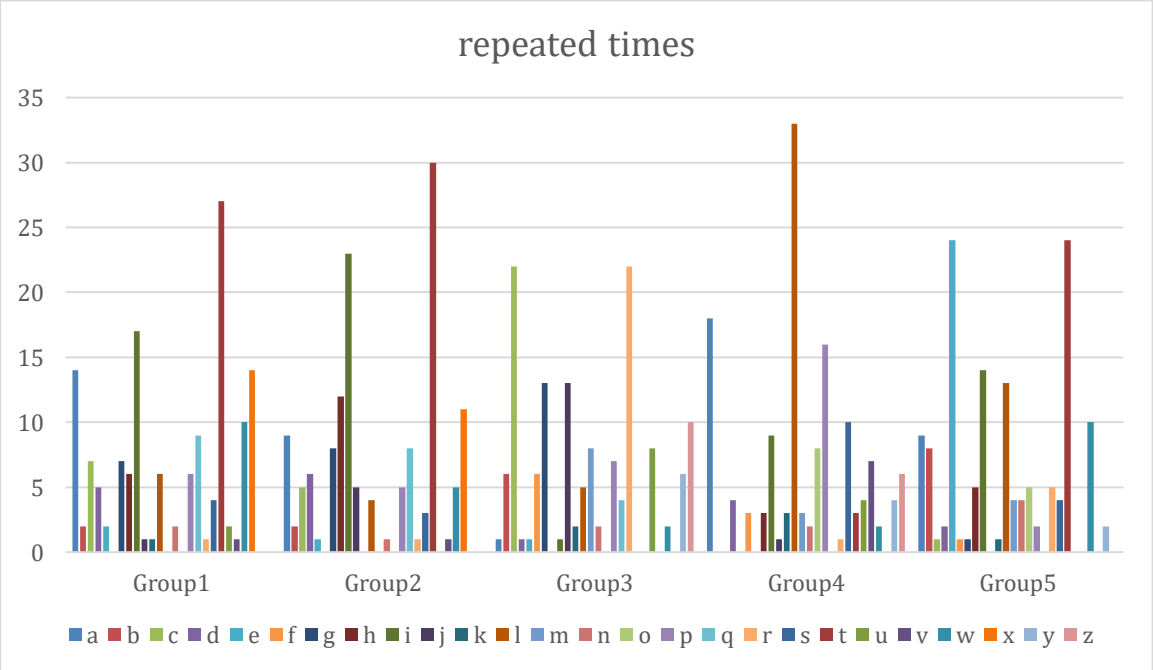
dhtcgmicskfstadpnixklsduryojqjlmdiflrbppfcdbcztdbczptpipnvlmydhdddihsmtltigabtplkicbwoojgmmdpgiuehhqoexhqaacs
guggxeotxcdyocimmmthnlazxlnwdgbzoulgzddbjltxizlltigabtacaiiqcseixrieatrptqtuoihecywdgbzoulgzddbjltxizlacsuoeciflb
gdilnwtyyttsnloeacsikxlniciflwdgjkavgcltwtplwxajiepcyusltpseixrieudpahdjeotwtwtanqcwagicktwtplihhrplapaoacrcahpiro
enlgslhtcahtgcdiaazlacplzwtgjltxizlltigabtacaiiqcseixrieatrptqtwlawiflrtlgslqtyuachulratrptqtjltxizlltigabtacaiiqcseixrielwg
zptguvrshmmwxhbvmatrptqtjltxizlltigabtacaiiqcfepwjltxizlwwxqweglmydhdddihsmtltigabtplkwwtlahtcgnhixqjldjbftwtpli
hhrplapjpgwiroaihfpnthmumthfpntjlaiaimtoggmdltigabtxuhktjnaoiwczojcbvfbjqpcbdroegbyyyrdklsidklsetyricvuvrshmm
wxhbvmatrptqtjltxizlltigabtacaiiqcfepwjltxizltwtplwxajiepcyusltpseixrieatrptqtjltxizlltigabtnchhatrptqtroegtuplaqchnpcqd
egacaiiqcseixrieatrptqtjltxizlytpfseixrielwgzptguvrshmmwxhbvmatrptqt

(1) Analyze and identify the ciphering technique used (1 points)

I have found two repeating strings.

Repeated Fragment	Index of Each Occurance	Distance Values
atrpt	178, 393, 423, 478, 688, 753, 778, 818, 863	215, 30, 55, 210, 65, 25, 40, 45
caiiq	165, 380, 445, 500, 710, 805	215, 65, 55, 120, 95

The greatest common divisor of all distance values is 5, and since 5 is a prime number, we can confidently estimate that the key length is 5. When we divide the sentence into blocks of 5 characters each and analyze the frequency of the first five characters in each block, we get the following information.



Group1

C	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

Group2

C	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

Group3

C	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B

Group4

C	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Group5

C	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

So, this cipher is created using the Vigenère cipher

(2) Identifying the correct key and the corresponding plaintext (1 point)

Key: HAPPY

Corresponding plaintext:

When I find myself in times of trouble mother mary comes to me speaking words of wisdom let it be and in my hour of darkness he is standing right in front of me speaking words of wisdom let it be let it be let it be let it be Let it be whisper words of wisdom let it be and when the broken hearted people living in the world agree there will be an answer let it be for though they may be parted there is still a chance that they will see there will be an answer let it be let it be let it be let it be let it be yeah there will be an answer let it be let it be let it be let it be let it be whisper words of wisdom let it be let it be let it be let it be let it be whisper words of wisdom let it be and when the night is cloudy there is still a light that shines on me shine until tomorrow let it be I wake up to the sound of music mother mary comes to me speaking words of wisdom let it be let it be let it be let it be yeah let it be there will be an answer let it be let it be let it be let it be let it be there will be an answer let it be let it be let it be let it be let it be yeah let it be whisper words of wisdom let it be

(3) Programming code for decryption (3 point): The fully automated code (which gives output with analysis) is not necessary. However, the students need to implement codes that do the analysis for them. You cannot just simply guess or do it by trial and error. It is important that the code includes the analysis code.

```
#include <stdio.h>
#include <string.h>

// to calculate greatest common divisor
int gcd(int a, int b) {
    while (b != 0) {
        a %= b;
        a ^= b;
        b ^= a;
        a ^= b;
    }
    return a;
}

int main() {
    char ciphertext[1000000];
    scanf("%s", ciphertext);

    int cipherlength = strlen(ciphertext);
    int distanceValue[100];
```

```
            int distanceCount = 0;

            //to find repeated strings
            for (int i = 0; i < cipherlength - 4; i++) {
                int searchLocation = i;
                char block[5];
                for (int j = 0; j < 5; j++) {
                    block[j] = ciphertext[searchLocation + j];
                }
                char candidate[6];
                strcpy(candidate, block);
                int priority = 1;
                for (int k = i + 5; k < cipherlength - 4; k += 5) {
                    int compareLocation = k;
                    for (int j = 0; j < 5; j++) {
                        if (ciphertext[compareLocation + j] != block[j]) {
                            break;
                        }
                        if (j == 4) {
                            priority++;
                            if (priority == 9) {
                                for (int l = 0; l < 8; l++) {
                                    distanceValue[distanceCount++] = k - i;
                                }
                            }
                        }
                    }
                }
                if (priority >= 4) {
            printf("repeated string '%s' repeated %d times.\n", candidate, priority);
                }
            }
            int prevGCD = distanceValue[0];

              //calculate gcd of the entire distanceValue array
            for (int i = 1; i < distanceCount; i++) {
                prevGCD = gcd(prevGCD, distanceValue[i]);
            }
            printf("Greatest Common Divisor: %d\n", prevGCD);


        //split blocks in to groups
            char group[30][10000];
            int groupCount = 0;
            for (int i = 0; i < cipherlength; i += 5) {
                char block[5];
                for (int l = 0; l < 5; l++) {
                    block[l] = ciphertext[l + i];
                }
                for (int l = 0; l < 5; l++) {
                    group[l][groupCount + l] = block[l];
                }
                groupCount++;
            }
            for (int i = 0; i < prevGCD; i++) {
                printf("Group%d: \n", i);
                for (int j = 0; j < groupCount; j++) {
                    printf("%c", group[i][j]);
                }
                printf("\n");
            }

        //Identify the most frequently used letter and assume it has been shifted from
        the letter 'e' in the alphabet.
```

```
            printf("Encrypt Key: ");
            char keys[30];
            for (int i = 0; i < prevGCD; i++) {
                int repeatedTime[26] = {0};
                for (int j = 0; j < groupCount; j++) {
                    char temp = group[i][j];
                    if (temp >= 'a' && temp <= 'z') {
                        repeatedTime[temp - 'a']++;
                    }
                }
                int maxIndex = 0;
                int maxCount = 0;
                for (int j = 0; j < 26; j++) {
                    if (repeatedTime[j] > maxCount) {
                        maxCount = repeatedTime[j];
                        maxIndex = j;
                    }
                }
                int key = (maxIndex - ('e' - 'a') + 26) % 26;
                keys[i] = key;
                printf("%c", 'a' + key);
            }
            printf("\n");

        //shift backward to decrypt ciphertext
            for (int i = 0; i < cipherlength; i += 5) {
                char block[5];
                for (int l = 0; l < 5; l++) {
                    block[l] = ciphertext[l + i];
                    if (block[l] - keys[l] < 'a') {
                        ciphertext[l] = block[l] - keys[l] + 26;
                    } else {
                        ciphertext[l] = block[l] - keys[l];
                    }
                    printf("%c", ciphertext[l]);
                }
            }
            return 0;
        }
```