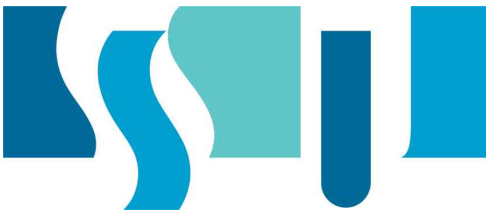

Assignment #1

Subject	Information Security
Professor	David Choi
Major	Computer Science & Engineering
Student No	20172655
Name	Kangsan Lee
Submission Date	29 September, 2021

Q1. 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 contains a known pattern. Second, the final n bits of the message contains a hash over the message. From a security point of view, are they equivalent? Discuss your answer. (1 point)

answer)
In my opinion, the second one is safer than the first. Because the hash is one-way function, cannot be used to decrypt. But providing known pattern like the first case could be analized and decrypted by the attacker.

Q2. Suppose that a message has been encrypted using DES in ciphertext block chaining mode. One bit of ciphertext in block Ci is accidentally transformed from a 0 to a 1 during transmission. How much plaintext in block Ci+1 received by the receiver will be garbled as a result? (1 point)

answer)
In CBC mode, we need previous ciphertext block(Ci) to decrypt the next ciphertext block(Ci+1). When we decrypt, we use XOR operation (Mi+1 = Ci xor Dk(Ci+1)). One bit of ciphertext in block Ci is changed, so the 1 bit of the plaintext in block Ci+1 will be affected.

Q3. The following are ciphertexts encrypted using two different techniques. For each ciphertext, (1) analyze and identify the ciphering technique used (1 point), give the corresponding plaintext and the used key (1 point), write programming code for decryption (2 points). Use either C, C++, Java, or Python.

Ciphertext A (6 points): (Hint: Quote)
GURTERNGRFGTYBELVAYVIVATYVRFABGVAARIRESNYYVATOHGVAEVFVATRIRELGVZRJ
RSNYY.ARYFBAZNAQRYN.GURJNLGBTRGFGNEGRQVFGBDHVGGNYXVATNAQORTVAQBV
AT.JNYGQVFARL.LBHEGVZRVFYVZVGRQFBQBABGJNFGRVGYVIVATFBZRBARRYFRFYVS
R.QBABGORGENCCRQOLQBTZN.JUVPUVFYVIVATJVGUGURERFHYGFBSBGURECRBCYRF
GUVAXVAT.FGRIRWBOF.VSYVSRJRERCERQVPGNOYRVGJBHYQPRNFRGBORYVSRNAQO
RJVGUBHGSYNIBE.RYRNABEEBBFRIRYG.VSLBHYBBXNGJUNGLBHUNIRVAYVSRLBHJVY
YNYJNLFUNIRZBER.VSLBHYBBXNGJUNGLBHQBABGUNIRVAYVSRLBHJVYYYARIREUNIR

RABHTU.BCENUJVASERL.VSLBHFRGLBHETBNYFEVQVPHYBHFYLUVTUNAQVGVFNSNVY
HERLBHJVYYSNVYNOBIRRIRELBARRYFRFFHPPRFF.WNZRFPNZREBA.YVSRVFJUNGUN
CCRAFJURALBHNEROHFLZNXVATBGURECYNAF.WBUAYRAABA.FCERNQYBIRRIRELJU
RERLBHTB.YRGABBARRIREPBZRGBLBHJVGUBHGYRNIVATUNCCVRE.ZBGUREGRERFN.
JURALBHERNPUGURRAQBSLBHEEBCRGVRNXABGVAVGNAQUNATBA.SENAXYVAQ.EBB
FRIRYG.NYJNLFERZRZOREGUNGLBHNERNOFBYHGRYLHAVDHR.WHFGYVXRRIRELBAR
RYFR.ZNETNERGZRNQ.QBABGWHQTRRNPUQNLOLGURUNEIRFGLBHERNCOHGOLGURF
RRQFGUNGLBHCYNAG.EBOREGYBHVFFGRIRAFBA.GURSHGHERORYBATFGBGUBFRJUB
ORYVRIRVAGURORNHGLBSGURVEQERNZF.RYRNABEEBBFRIRYG.GRYYZRNAQVSBETRG
.GRNPUZRNAQVERZRZORE.VAIBYIRZRNAQVYRNEA.ORAWNZVASENAXYVA.GURORFGN
AQZBFGORNHGVSHYGUVATFVAGURJBEYQPNAABGORFRRABERIRAGBHPURQGURLZHF
GORSRYGJVGUGURURNEG.URYRAXRYYRE.VGVFQHEVATBHEQNEXRFGZBZRAGFGUNGJ
RZHFGSBPHFGBFRRGURYVTUG.NEVFGBGYR.JUBRIREVFUNCCLJVYYZNXRBGUREFUNC
CLGBB.NAARSENAX.QBABGTBJURERGURCNGUZNLYRNQTBVAFGRNQJURERGURERVF
ABCNGUNAQYRNIRNGENVY.ENYCUJNYQBRZREFBA.

A-(1) analyze and identify the ciphering technique used. (1 point)

answer) It used the Caesar Cipher. In the ciphertext A, some strings are shown repeatedly such as "GUR", "LBH". I used the while loop to see every shifted state of those repeated strings, found the meaningful words "THE", "YOU" at 13th shift.

A-(2) give the corresponding plaintext and the used key. (1 point)

answer)
The key is shifting 13 times. (A->N, B->O...)
It is the quotes of famous people such as Nelson Mandela, Walt Disney... etc.

THEGREATESTGLORYINLIVINGLIESNOTINNEVERFALLINGBUTINRISINGEVERYTIMEWEFALL
.NELSONMANDELA.THEWAYTOGETSTARTEDISTOQUITTALKINGANDBEGINDOING.WALTDIS
NEY.YOURTIMEISLIMITEDSODONOTWASTEITLIVINGSOMEONEELSESLIFE.DONOTBETRAPP
EDBYDOGMA.WHICHISLIVINGWITHTHERESULTSOFOTHERPEOPLESTHINKING.STEVEJOBS.I
FLIFEWEREPREDICTABLEITWOULDCEASETOBELIFEANDBEWITHOUTFLAVOR.ELEANORRO
OSEVELT.IFYOULOOKATWHATYOUHAVEINLIFEYOUWILLALWAYSHAVEMORE.IFYOULOOKAT
WHATYOUDONOTHAVEINLIFEYOUWILLLNEVERHAVEENOUGH.OPRAHWINFREY.IFYOUSETY
OURGOALSRIDICULOUSLYHIGHANDITISAFAILUREYOUWILLFAILABOVEEVERYONEELSESS
UCCESS.JAMESCAMERON.LIFEISWHATHAPPENSWHENYOUAREBUSYMAKINGOTHERPLAN
S.JOHNLENNON.SPREADLOVEEVERYWHEREYOUGO.LETNOONEEVERCOMETOYOUWITHOU
TLEAVINGHAPPIER.MOTHERTERESA.WHENYOUREACHTHEENDOFYOURROPETIEAKNOTINI
TANDHANGON.FRANKLIND.ROOSEVELT.ALWAYSREMEMBERTHATYOUAREABSOLUTELYU

NIQUE.JUSTLIKEEVERYONEELSE.MARGARETMEAD.DONOTJUDGEEACHDAYBYTHEHARVESTYOUREAPBUTBYTHESEEDSTHATYOUPLANT.ROBERTLOUISSTEVENSON.THEFUTUREBELONGSTOTHOSEWHOBELIEVEINTHEBEAUTYOFTHEIRDREAMS.ELEANORROOSEVELT.TELLMEANDIFORGET.TEACHMEANDIREMEMBER.INVOLVEMEANDILEARN.BENJAMINFRANKLIN.THEBESTANDMOSTBEAUTIFULTHINGSINTHEWORLDCANNOTBESEENOREVENTOUCHEDTHEYMUSTBEFELTWITHTHEHEART.HELENKELLER.ITISDURINGOURDARKESTMOMENTSTHATWEMUSTFOCUSTOSEETHELIGHT.ARISTOTLE.WHOEVERISHAPPYWILLMAKEOTHERSHAPPYTOO.ANNEFRANK.DONOTGOWHERETHEPATHMAYLEADGOINSTEADWHERETHEREISNOPATHANDLEAVEATRAIL.RALPHWALDOEMERSON.

A-(3) write programming code for decryption. (2 points)

answer)
Enter ./(executable file) (data file) (key number) to run the program.
The result file will be created with the name (decrypted data file)
./caesar A.dat 13

caesar.c

```
//20172655 LEE KANG SAN
//caesar.c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
int main(int argc, char** argv) {
	if(argc!=3) {
		printf("Usage : %s (datafile) (key)\n", argv[0]);
		exit(1);
	}

	FILE *fp1, *fp2;
	int key=atoi(argv[2]);
	int c;
	char outfile[100]="decrypted";
	strcat(outfile, argv[1]);
	fp1=fopen(argv[1], "r"); //A.dat
	fp2=fopen(outfile, "w"); //decryptedA.dat

	while((c=fgetc(fp1))!=EOF) {
		if('A'<=c&&c<='Z')
			c=(c-key<'A')?26+(c-key):(c-key);
		fputc(c, fp2);
```

```
        }

        fclose(fp1);
        fclose(fp2);
        return 0;
}
```

Ciphertext B (6 points): (Hint: Song Lyric)

OVSAOXQYVAMFKDNTFHWZKKWQLFCHHDMXGHVRXEICQQCZKKBZESGCKSSTFUKBXVA
ZXKWFJGUWWHWGHWIYVWBZEZWFJCTQGJSYWGGFNWQDKHOAJAVRJWUUZAVQJCBG
UXUPKDSNQAVROCFQYGNHAGRBSDMEAHPRRWBTLPSYKLQETSZRZABMWZSGOLJPOV
WFVWZHGFRFUXETKRCZRWBTLPSNTVESWBHUKTZZCSBUKSZEWRDRUHTPDWJVTYQY
LVSJUJTOSUFRKLPPJSKVRDJPSBOAYOMCDSHVZTMQGFHUUMOSLVSLSSGMWDOEZW
LEZSFROKAEAZZNIZIYUSHUGLBSWMKVRDAPWHVRXWETDZPRGFIYKKSERWBTLPSYK
LQETSZRZABMWZSGOLJPDSHVZTMJWOVGNWZPOWZYHWIYSBGJKJTPLWHOKDMEAHP
RRWBTLPSYKLQETSZRZABMWKVVYHMCOCFQYGNHAGRBSDMEAHPRRWBTLPSYKLQET
SZRZABMWMSNNDMEAHPRCZQDHSFJUJLDGTKVYVWXDSHVZTMLFRKUKFBSWBWTNL
QDUZCHJQBSWFSVYKBTDZOYOYPELVOGYZQYWGCASWASABSHTLQWLCABXJWHDSHV
ZTMTOOYRAHBZLVSFUMVOGTAHYAKXGHVRXEICQQCZKKBZESGCKSSTFUKBXVAZXKWF
JGUWWHWGHWTPLWHOKDMEAHPRRWBTLPSLKSPWWHWGHWBSWFSJODTMWOBNTK
EPJZSGOLJPDSHVZTMWWHWGHWTPLWHOKQMLZZSGOLJPLVSEKOQWDPSNTSVDOSF
YKLQETSZRZABMWZSGOLJPDSHVZTMJWOVYKLQETSKUOKXPJKCEJKWQOWGQUETPL
WHOK

B-(1) analyze and identify the ciphering technique used. (1 point)

answer) It used the Vigenere Cipher. I found the repeated strings such as "TPLWHOK", "WWHWGHW" etc, but couldn't find meaningful words when I shift them. Also, both ciphertext A and B is used the different way to encrypt, so it doesn't use the Caesar cipher. Becuase of the repeated strings, I gusessed it would be used the Vigenere cipher, checked it out with the online vigenere decoder and found that it's encrypted by using vigenere cipher.

B-(2) give the corresponding plaintext and the used key. (1 point)

answer)

The key is 'SOONGSIL'

It is the lyrics of 'Let it be', sung by the Beatles.

WHENIFINDMYSELFINTIMESOFTROUBLEMOTHERMARYCOMESTOMESPEAKINGWORDSOF
WISDOMLETITBEANDINMYHOUROFDARKNESSSHEISSTANDINGRIGHTINFRONTOFMESPEA
KINGWORDSOFWISDOMLETITBELETITBELETITBELETITBELETITBEWHISPERWORDSOFWIS
DOMLETITBEANDWHENTHEBROKENHEARTEDPEOPLELIVINGINTHEWORLDAGREETHEREW
ILLBEANANSWERLETITBEFORTHOUGHTHEYMAYBEPARTEDTHEREISSTILLACHANCETHATT
HEYWILLSEETHEREWILLBEANANSWERLETITBELETITBELETITBELETITBELETITBEYEAHTH
EREWILLBEANANSWERLETITBELETITBELETITBELETITBELETITBEWHISPERWORDSOFWIS
DOMLETITBELETITBELETITBELETITBEYEAHLETITBEWHISPERWORDSOFWISDOMLETITBE
ANDWHENTHENIGHTISCLOUDYTHEREISSTILLALIGHTTHATSHINESONMESHINEUNTILTOM
ORROWLETITBEIWAKEUPTOTHESOUNDOFMUSICMOTHERMARYCOMESTOMESPEAKINGWO
RDSOFWISDOMLETITBELETITBELETITBELETITBEYEAHLETITBETHEREWILLBEANANSWER
LETITBELETITBELETITBELETITBEYEAHLETITBETHEREWILLBEANANSWERLETITBELETITB
ELETITBELETITBEYEAHLETITBEWHISPERWORDSOFWISDOMLETITBE

B-(3) write programming code for decryption. (2 points)

answer)
Enter ./(executable file) (data file) (key string) to run the program.
The result file will be created with the name (decrypted data file)
./vigenere B.dat SOONGSIL

vigenere.c

```
//20172655 LEE KANG SAN
//vigenere.c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
int main(int argc, char** argv) {
        if(argc!=3) {
                printf("Usage : %s (datafile) (key)\n", argv[0]);
                exit(1);
        }

        FILE *fp1, *fp2;
        int c, i=0;
        int keylength=strlen(argv[2]);
        char outfile[100]="decrypted";

        strcat(outfile, argv[1]);
        fp1=fopen(argv[1], "r"); //B.dat
        fp2=fopen(outfile, "w"); //decryptedB.dat
```

```
        while((c=fgetc(fp1))!=EOF) {
                if('A'<=c&&c<='Z') {
                        c=c-argv[2][i];
                        c=c<0?'A'+26+c:'A'+c;
                }
                fputc(c, fp2);
                i=(i+1)%keylength; //repeat the key value
        }

        fclose(fp1);
        fclose(fp2);
        return 0;
}
```