Network Security Lab1

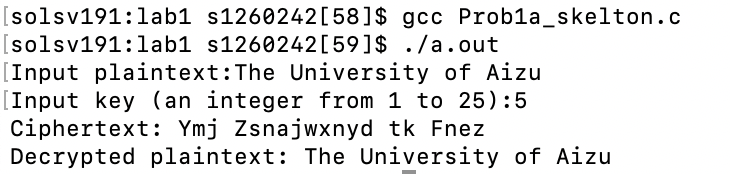
S1260242

Ryusei Takahashi

Problem1

a)

(1)



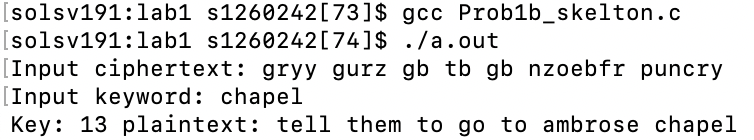
Input “The University of Aizu” as a plaintext and key=5.

the codes are included in C files

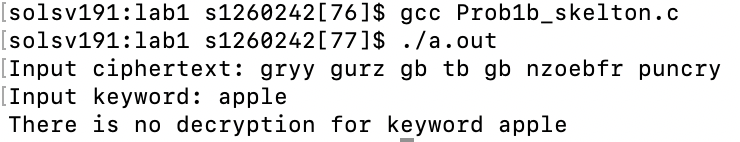
b)

(1)

With keyword:



Keyword is nothing:



Without keyword:

新聞の記事

自動的に生成された説明

the codes are included in C files

c)

(1)

k=6, plaintext=”Get me a vanilla ice cream, make it a double.”

Result:

記号 が含まれている画像

自動的に生成された説明

k=15, plaintext=”I don’t much care for Leonard Cohen.”

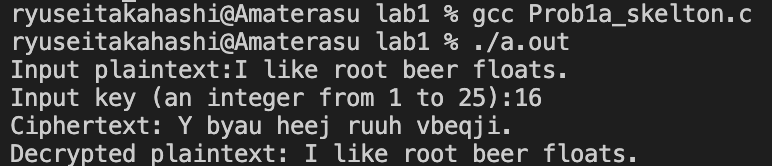
Result:

テキスト, 記号 が含まれている画像

自動的に生成された説明

k＝16, plaintext=”I like root beer floats.”

Result:



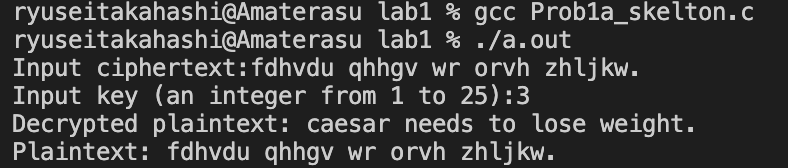
d)

k=12, ciphertext=” nduzs ftq buzq oazqe.”

記号 が含まれている画像

自動的に生成された説明

k=3, ciphertext= “fdhvdu qhhgv wr orvh zhljkw.”



k=20, ciphertext=” ufgihxm uly numnys.

In C file, I change the from encrypt to decrypt and from decrypt to encrypt for using comment out.

記号 が含まれている画像

自動的に生成された説明

e)

ciphertext=” gryy gurz gb tb gb nzoebfr puncry”, keyword=”chapel”

記号 が含まれている画像

自動的に生成された説明

ciphertext=” wziv kyv jyfk nyve kyv tpdsrcj tirjy.”, keyword=”symbal”

記号 が含まれている画像

自動的に生成された説明

cipheretxt=” baeeq klwosjl osk s esf ozg cfwo lgg emuz”, no keyword

テキスト, テーブル, 大きい, 立つ が含まれている画像

自動的に生成された説明

Problem2

1. I confirmed it.
2. bgepsonm\_lk\_ihy\_at\_uwfrdvc

Problem3

1. Implement a C function that performs frequency attacks on a mono-alphabetic substitution ciphers.

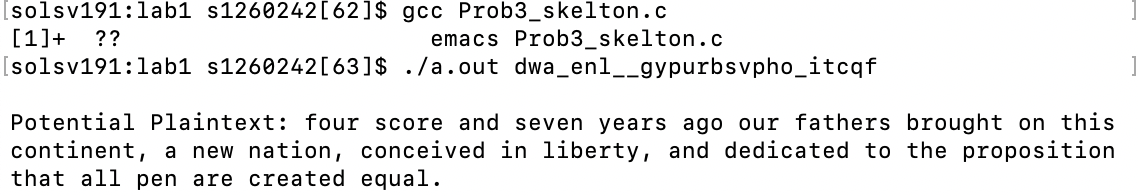
the codes are included in C files

1. Implement a C function that takes a partial mono-alphabetic substitution (i.e., subs in Problem 2) and a ciphertext and returns a potential plaintext.

the codes are included in C files

c) Use your functions from (a) and (b) to decrypt the following cipher text:

"ztmn pxtne cfa peqef kecnp cjt tmn zcwsenp ontmjsw ztnws tf wsvp xtfwvfefw, c feb fcwvtf, xtfxevqea vf gvoenwk, cfa aeavxcwea wt wse rntrtpvwvtf wscw cgg lef cne xnecwea eymcg."



The key is dwa\_enl\_\_gypurbsvpho\_itcqf .

黒い背景と白い文字

自動的に生成された説明

Based on the incidence of the letters above, we find out from the most used letters.