Decrpytion

Preston White

Homework 1 Q1

Let γ represent any encrypted letter located in an encrypted text.

The shift of each encrypted letter is represented by Δ.

The general shifting equation: $\gamma - \Delta$.

An example how this equation works, let's say that the encrypted text is ABCD and the shift $\Delta = 1$. This means each letter of the text is shifted back 1. So, it now becomes ZABC.

There are 3 encrypted text that can be solved using Caesar cipher technique.

1. LWKLQNWKDWLVKDOOQHYHUVHHDELOOERDUGORYHOBDVDWUHH
    a. $\gamma - 1$
        i. KVJKPMVJCVKUJCNNPGXGTUGGCDKNNDQCTFNQXGNACUCVTGG
        ii. This is not readable
    b. $\gamma + 1$
        i. MXLMROXLEXMWLEPPRIZIVWIIEFMPPFSEVHPSZIPCEWEXVII
        ii. This is not readable
    c. $\gamma - 2$
        i. JUIJOLUIBUJTIBMMOFWFSTFFBCJMMCPBSEMPWFMZBTBUSFF
        ii. Not readable
    d. $\gamma + 2$
        i. NYMNSPYMFYNXMFQQSJAJWXJJFGNQQGTFWIQTAJQDFXFYWJJ
        ii. Not readable
    e. $\gamma - 3$
        i. ITHINKTHATISHALLNEVERSEEABILLBOARDLOVELYASATREE
        ii. I think that I shall never see a billboard lovely as a tree
2. UXENRBWXCUXENFQRLQJUCNABFQNWRCJUCNAJCRXWORWMB
    a. $\gamma - 1$
        i. TWDMQAVWBTWDMEPQKPITBMZAEPMVQBITBMZIBQWVNQVLA
        ii. Not readable
    b. $\gamma - 2$
        i. SVCLPZUVASVCLDOPJOHSALYZDOLUPAHSALYHAPVUMPUKZ
        ii. Note readable
    c. $\gamma - 4$
        i. QTAJNXSTYQTAJBMNHMFQYJWXBMJSNYFQYJWFYNTSKNSIX

ii. Not readable

d. $\gamma - 9$

i. LOVEISNOTLOVEWHICHALTERSWHENITALTERATIONFINDS

ii. Love is not love which alters when it alteration finds

3. BGUTBMBGZTFHNLXMKTIPBMAVAXXLXTEPTRLEXTOXKHHFYHKMAXFHNLX

a. $\gamma + 7$

i. INBAITINGAMOUSETRAPWITHCHEESEALWAYSLEAVEROOMFORTHE MOUSE

ii. In baiting a mouse trap with cheese always leave room for the mouse

Homework 1

2) a) The gold is hidden in the garden
I BX FEPA QL BQAAXW QW I BX FSVAXW

IBXFE PAQLB QAAXW QWIBX FSVAXW

b)

d	h	l	w	e	g	u	B	t	c	j	S	y	x	z	l	i	m	a	K	P	r	n	e	V	P
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

c) IBXLX [redacted] JVXIZ SLLDE VAQLL DEVAU[redacted] QLB
these cretp asswo rd iss wordF[redacted] i s h

the secret password is swordfish

QUESTION 3

Original:

GSZES GNUBE SZGUG SNKGX CSUUE QNZOQ EOVJN VXKNG XGAHS AWSZZ BOVUE
SIXCQ NQESX NGEUG AHZQA QHNSP CIPQA OIDLV JXGAK CGJCG SASUB FVQAV
CIAWN VWOVP SNSXV JGPCV NODIX GJQAE VOOXC SXXCG OGOVA XGNVU BAVKX
QZVQD LVJXQ EXCQO VKCQG AMVAX VWXCG OOBOX VZCSO SPPSN VAXUB DVVAX
QJQAJ VSUXC SXXCV OVJCS NSJXV NOJQA MVBSZ VOOSH VSAWX QHGMV GWVSX
CSXXC VBSNV ZVNVN SAWQZ ORVXJ CVOQE JCGUW NVA

Edited:

iamfa irlyf amili arwit hallf ormso fsecr etwri tinga ndamm yself
autho rofat rifli ngmon ograp hupon subje ctinw hichi analy zeone
hundr edsep arate ciphe rsbut iconf essth atthi sisen tirel ynewt
omeob jecto fthos ewhoi nvent edthi ssyst emhas appar ently beent
oconc ealth atthe secha racte rscon veyam essag eandt ogive ideat
hatth eyare merer andom sketc hesof child ren

Translated:

I am fairly familiar with all forms of secret writing and am myself
author of a trifling monograph upon subject in which I analyze one
hundred separate ciphers, but I confess that this is entirely new to
me. object of those who invented this system has apparently been to
conceal that these characters convey a message and to give idea that
they are mere random sketches of children.

Translated (with added "the"s):

I am fairly familiar with all forms of secret writing and am myself
the author of a trifling monograph upon **the** subject in which I
analyze one hundred separate ciphers, but I confess that this is
entirely new to me. **The** object of those who invented this system has
apparently been to conceal that these characters convey a message and
to give **the** idea that they are mere random sketches of children.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
nyhbfzigucwjvrspoka_ledt_m

V	S	X	G	A	O	Q	C	N	J	U	Z	E	W	B	P	I	H	K	D	M	L	R	F
39	29	29	22	21	21	20	20	19	13	11	11	10	8	8	6	5	5	5	4	3	2	1	1

The most frequent bigrams are: XC (10 times), NV (7 times), and CS,
OV, QA, and SX (6 times each)

Assume V is **e** since it is the most common letter.

Note EAX appears 4 times in the above text.

Note the bigrams XC, CS, and SX. These all share X, C, S. Let's focus on these letters first. Also note XCSXXC appears thrice in the above text. Based on the bigrams, bigram frequency, and individual letter frequency, let's assign XC to be **th**, CS to be **ha**, and SX to be **sa**.

Then XCSXXC is **thatth**. One of the occurrences of XCSXXC is followed by VOV. This occurrence translates to **that the**O**e** with our current assumptions. O is likely **r** or **s**.

Another occurrence of XCSXXC is followed by GOGO. This most likely implies O is **s** since it is hard to imagine a letter for G in the case of **that th**G**r**G (in the case where O is **r** and G cannot be **e**).

Following from this, G might be **i** so that XCSXXCGOGO is **that this is**.

The last occurrence of XCSXXC is followed by VBSNV. With our current translation, this is **thatth e**B**a**N**e**. Again, **the** cannot be in the message. This implies **the**B is one word. B could be **y**, making this **that they a**N**e**. This assumption makes sense because B is low in the letter frequency list.

Looking at **that they a**N**e**, we can guess N is **r**. Again this makes sense based on N's frequency. The bigram NV would be **re**.

iW**ea** appears in the text before **that they**. W is possibly **d**.
systeZ appears in the text. Z is likely **m**.
aPP**are**A**t**U**y** is in the text. P is likely **p**. A is likely **n**. U is likely **l**
myselE is in the text. E is likely **f**.
familiar K**ith all f**Q**rms** is in the text. K is likely **w**. Q is likely **o**.
J**hildren** is in the text. J is likely **c**.
writinH is in the text. H is likely **g**.
D**een** is in the text. D is likely **b** based on the context.
sR**etches of children** is in the text. R is likely **k**.
inM**ented this system** is in the text. M is likely **v**.
aI**thor** is in the text. With the remaining letters, I is likely **u**.
analyF**e** is in the text. With the remaining letters, F is likely **z**.
obL**ect** is in the text. With the remaining letters, L is likely **j**.

4)

a. There are 26! simple substitution ciphers

b.

(i) This is the derangement of 26, notated by !26

Counting !26:

Let A be an alphabet with 26 characters

Let $a_i \in A$ be the i^{th} character in A for $1 \leq i \leq 26$

Let A' be a duplicate of A where $a_i = a_i'$ for $a_i \in A$, $a_i' \in A'$

To create a simple substitution cypher w/ no fixed letters:

For all $a_i' \in A$, assign $a_j \in A$ to a_i' s.t. $i \neq j$, a_j has not been assigned

So, start with an arbitrary $a_n' \in A'$

Assign to it some $a_m \in A$ where $m \neq n$

Then there are two cases:

Case 1: a_n' gets matched with a_n

Then we have pairs (a_n', a_m), (a_m', a_n)

So the problem is reduced to size 26-2=24 b/c the n^{th} + m^{th} elements are no longer in use

Case 2: a_n' gets matched with some other $a_k \in A$ where $k \neq n$

Then there are 25 characters in A, A' since (a_n', a_m) have been paired up

And for each $a_i' \in A'$, there is exactly one letter in A they cannot be assigned (for $i \neq m$, it is simply a_i, for $i = n$, it is a_n since this is assumed for the case)

Thus this case is simply the problem with size 26-1=25

Therefore, for each 25 original characters that can be assigned to a_n', there are a resulting !24+!25 possible assignments (sum of cases)

So $!26 = 25(!25 + !24)$

Or more generally $!n = (n-1)(!(n-1) + !(n-2))$ where $!0 = 1$, $!1 = 0$

$\therefore !n = (n-1)(!(n-1) + !(n-2))$, $!0 = 1$, $!1 = 0$. More specifically, there are !26 ciphers w/ no fixed letters

(NOTE: Proof inspired by similar proof from MATH 574)

b. continued

(ii) This is equivalent to all ciphers minus ciphers with no fixed letters

Thus, this is the difference between (a) and (b.i)

So there are $26! - !26$ ciphers w/ at least one fixed letter

(iii) Choose some $a_n \in A$ to be fixed

Then we have 25 letters to assign s.t. none can be fixed

As seen in (b.i), this is simply $!25$

And there are 26 ways of choosing an a_n (since $|A| = 26$)

$\therefore$ There are $26(!25)$ ciphers w/ only one fixed letter

(iv) This is equivalent to all ciphers with at least one letter fixed minus all ciphers w/ exactly one letter fixed

Thus, this is the difference of (b.ii) and (b.iii)

$\therefore$ There are $(26! - !26) - 26(!25)$ ciphers w/ at least two fixed letters