Cracking Cryptic Messages

Have you ever gotten caught passing a note to a classmate? Whether or not you have, a teacher intercepting your message and reading it out loud sounds like a recipe for embarrassment. To protect ourselves against snooping intermediaries, let's learn some ways to encrypt our most private of notes.

Problem 1. *Before we examine any ciphers in-depth, put yourself in the shoes of a nosy teacher. Decrypt the following message.*

DTZ RFD MFAJ HFZLMY RJ TSHJ,

GZY N XMFQQ WJYZWS XYWTSLJW

FSI XRFWYJW!

Assuming you cracked the message without skipping ahead, congratulations! The cipher you just decrypted is called a **Caesar cipher**. To use a Caesar cipher like Emperor Julius Caesar did, you first pick a number from 1 to 25. Then, you shift every letter of your message by your chosen number, wrapping around from Z to A. Caesar ciphers are an example of a **mono-alphabetic** cipher, meaning that the message is encoded by using some rearrangement of the alphabet.

Problem 2. *Encode the message "Hello Neighbor, I would like to establish contact" with shifts of length 1, 2, 3, and 4.*

Problem 3. *Exchange coded messages with a partner using a Caesar cipher.*

(i) *What information do you need to share with each other to be able to easily decode each others' messages?*

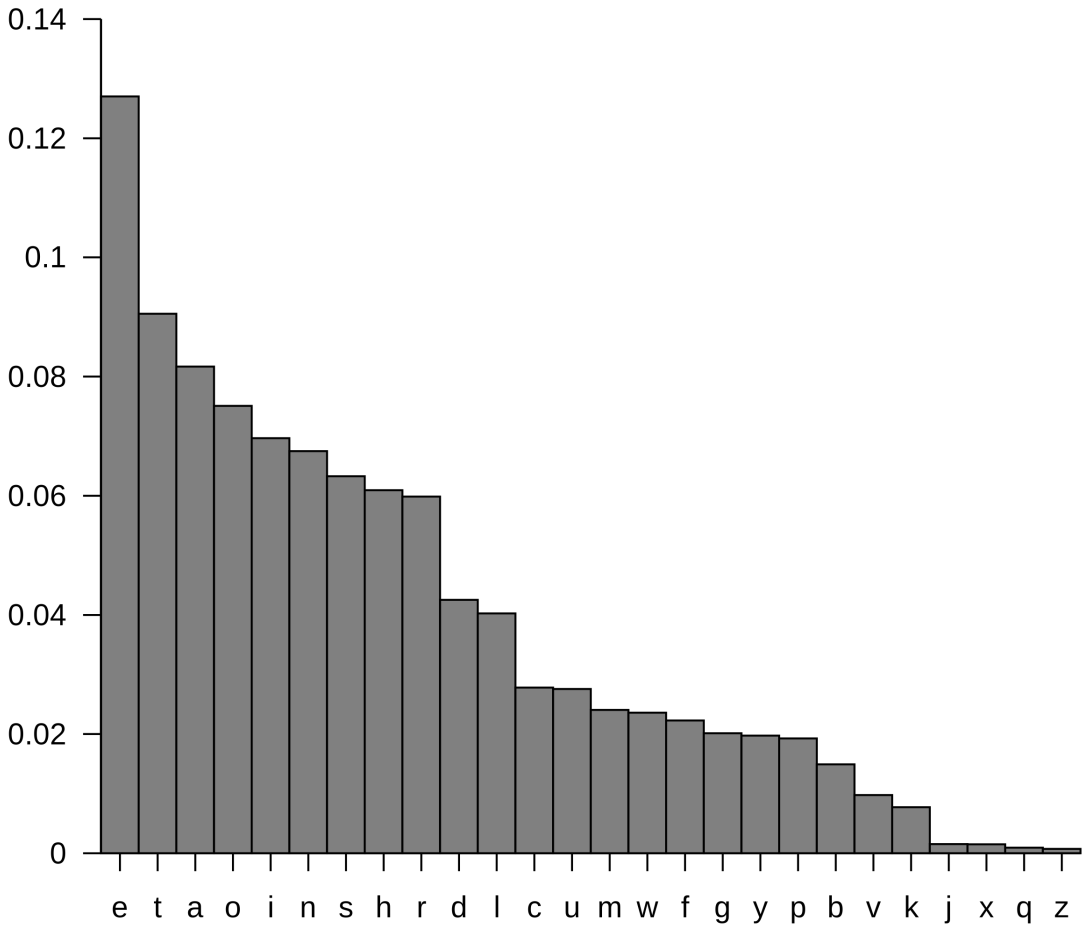
(ii) *Do you think that Caesar ciphers are a secure method of encryption? Why or why not?*

We previously defined mono-alphabetic ciphers to be rearrangements of the alphabet. In other words, a mono-alphabetic cipher sends each letter in the alphabet to a unique encrypted letter, such that every letter of the alphabet is used. For example, we could define a cipher that send A to Z, B to B, C to A, etc. Note that we are allowed to send a letter to itself. As long as every letter of the alphabet gets sent to another letter, and all the sent letters can reconstruct the alphabet, our cipher is a valid mono-alphabetic cipher.

Problem 4. *Exchange coded messages with a partner using your own mono-alphabetic cipher. What information do you need to share with each other to be able to easily decode each others' messages?*

Problem 5. *How many unique mono-alphabetic ciphers are there?*

While the answer to the previous question may make it seem like monoalphabetic ciphers are somewhat secure, one way to help break them is using letter frequencies. The idea is that (especially in longer messages) the most frequent letters in the coded message will correspond to the most frequent letters in usual English text. Consider the following letter frequency chart:



Problem 6. *Exchange coded messages with a different partner using the same cipher from Problem 4. Do not give them any information besides the encrypted message itself. Write down your best guess of your partner's message.*

Problem 7. *Decrypt the following message. Collaboration is encouraged!*

FURHJ UFEPQJI KQJOJN WX ENJ

KOCRWP NQJ NFRI XWJ HFWK

GJURJYJ RVZXNNRGUJ KQRWPN R

IFOJNFC CXE QFYJWK QFI VEHQ

ZOFHKRHJ NFRI KQJ MEJJW AQJW R

AFN CXEWPJO R FUAFCN IRI RK LXO

QFUL FW QXEO F IFC AQC

NXVJKRVJN RYJ GJURJYJI FN VFWC

FN NRB RVZXNNRGUJ KQRWPN

GJLXOJ GOJFTLFNK - UJARN

HFOOXUU LOXV FURHJ RW

AXWIJOUFWI.

As you've experienced firsthand, frequency analysis can enable us to crack mono-alphabetic ciphers relatively quickly by helping us make smart guesses. If we want to exchange messages that elude even statistically savvy teachers, we're going to have to come up with a stronger encryption scheme.

Enter the **Vigenère cipher**! This is an example of a poly-alphabetic substitution cipher, which means the same letters in a plaintext message may correspond to different letters in the encrypted message. Many people believed it was a completely secure way to send secret messages; the French called it *le chiffre indechiffrable*, "the undecipherable cipher."

To see how it works, imagine using a Caesar cipher, but with a different shift for each letter of the message. The pattern of the shifts is determined by a keyword. For example, let's make JUICE our keyword. To encode a message, write JUICE above the letters of the message, over and over, like this:

J	U	I	C		E	J	U	I	C	E	J	
t	h	i	s		m	e	s	s	a	g	e	

U	I	C	E		J	U	I		C	E	J	U
u	s	e	s		t	h	e		v	i	g	e

I	C	E	J		U	I	C	E	J	U		
n	e	r	e		c	i	p	h	e	r	.	

Now for each letter with a J above it, encrypt that letter using a shift that takes A to J. Similarly, for each letter below a U, use an A to U shift; for letters below I, use an A to I shift; for letters below C, use an A to C shift; and for letters below E, use an A to E shift. Once you are done encrypting each letter, you're ready to send your secret message!

Decrypting a message, if you know the key, just means doing things in reverse. Write down the keyword above each letter of the ciphertext, then use each letter of the keyword to tell you the shift to go back to the plaintext. The difference is that if the keyword letter is J (for example), you will decode using the reverse shift that takes J to A.

Problem 8. *We encrypted the first few words of "this message uses the Vigenère cipher" under the keyword JUICE, except we made a mistake. In the first row, find the letter that was incorrectly encrypted. Fix the mistake, and then finish encrypting the last two rows.*

J	U	I	C		E	J	U	I	C	E	J	
t	h	i	s		m	e	s	s	a	g	e	
C	B	Q	U		T	N	M	A	C	K	N	

U	I	C	E		J	U	I		C	E	J	U
u	s	e	s		t	h	e		v	i	g	e

I	C	E	J		U	I	C	E	J	U		
n	e	r	e		c	i	p	h	e	r	.	

Problem 9. *Using a Vigenère cipher with key word "ABCD", encrypt the following joke.*

WHY DID THE CHICKEN CROSS THE

MOBIUS STRIP?

Problem 10. *Decrypt the follow ciphertext that uses a Vigenère cipher and key word "ABCD".*

TP IHT UQ WHF UDMF ULDF.

Problem 11. *Find a partner and exchange coded messages using a Vigenère cipher. What information do you need to share between each other to decode each others' messages?*

Despite many thinking the Vigenère cipher was unbreakable, eventually people figured out how to crack it. Let's try it ourselves!

Problem 12. *Suppose you knew that the keyword for a Vigenère cipher was of length 3. Can you use letter frequency analysis to crack the following cipher? (Hint: group letters assigned to the same key-letter together)*

KVX DOGRUXI OM R PHRH-KVBMRZ

VFBVVGLZCG NSGK HH KVX VRZV

CY KVX CODV OGU MXCZXU, PHRH

GLAUVF 99, VFAX SOVB. MHLF MZAX

ZG NG. PNK HAV PHRH WZRG'K

FXKIKE. PHRH GLAUVF 99, AV

VHCZXISW RUTZB. KVHNIB MF HAV

RHTY BDAXUWTKSEP CK Z'ZE

TVTIUX PCN FJXIHBDS. LFAXKVBEU

BJ KKFBZ, SCLJ, VBJ OLJWLKOGK

GTZR. PV CGCM ARJX 75 SCTKG.

MYSKV WL EC GLAUVF 99. MYS

FRBTXSK KVHLUAK THI O FFAXEH.

UFOM EIFSSK 66, YS RVZEVR. TIS RFI

ARJBEU MICNSZX FIMKVXIS?

To decode the previous message, we assumed prior knowledge of the keyword length. In practice, the only information available to us would be the ciphertext alone. How can we decrypt Vigenère ciphers in the real world?

One idea, named **Kasiski Examination**, is to look for repeated strings of letters in the ciphertext. You want strings of length at least 3 to be repeated, but the more the better. For instance, in the previous ciphertext the string "GLAUVF 99" appears three times.

Problem 13. *How do you suppose it happened that the same string repeated itself in three different places?*

Problem 14. *Circle the three places where GLAUVF appears in the ciphertext. Count the distance (in letters ONLY–don't count the numbers!) between the G in the first GLAUVF, and the G in the second GLAUVF. What are the factors of this number?*

Problem 15. *Now count the distance between the G in the second GLAUVF and the G in the third GLAUVF. What are the factors of this number? Does it have any factors in common with the number you got in Problem 14? How can this help you find the key length for that cipher?*

Problem 16. *Use Kasiski Examination to determine possible key lengths and decrypt the following cipher. Collaboration is highly encouraged!*

A VNNS SGIAV GVDJRJ! WG OOF AB

GZS UAZYK PRZWAV HUW HESRVFU

CGGG GB GZS AADVYCA JWIWF NL

HUW BBJHUWFA LWC GT YSYR

KICWFVGF. JZWYW VVCWAY, W

SGIAV GBES FZWAQ GGGBRK. ZNLSE

A PEGITZH GZSZ LC N ESGSZ RPDRJH

GG VNNS GZSZ SDCJOVKSQ. KIEW

SAGITZ, HUWM NJS FAZIWF - VF O

IWFL HIEW TBJA. GZSEW AHKH OW

ABJS - V OWYD FRLIEF OAV GGSYR S

QYSWZ.