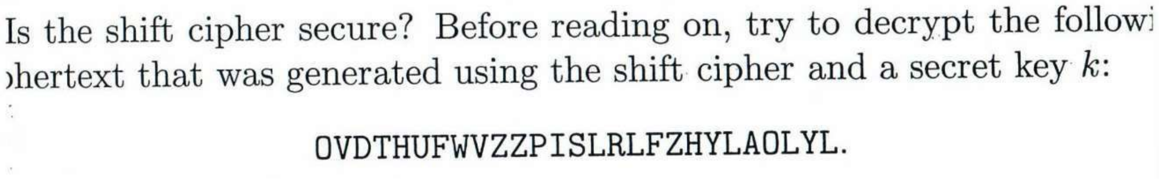
Hardware-Oriented Security and Trust
ECE 4156 HST / ECE 6156 HST
Spring 2024
Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology
Homework 1, 20 pts. (ECE 4156) 30 pts. (ECE 6156)
Due Friday January 12 prior to 11:55pm

1) (10 pts.) In the Media Gallery on Canvas, listen to the lecture “02CryptoI.” There is no need to notify Professor Mooney that you have done so **unless** you have problems. Canvas provides information regarding which GT usernames have accessed / listened to lectures, so there is no need to turn anything in if you have been successful.

Watch the video uploaded on Canvas.

2) (10 pts.) Decrypt the text shown on page 10 of Katz and Lindell (also shown below). Please assume that a shift cipher was used with a single key (shift amount).



Is the shift cipher secure? Before reading on, try to decrypt the followi
hertext that was generated using the shift cipher and a secret key k:

OVDTHUFWVZZPISLRLFZHYLAOLYL.

Solution

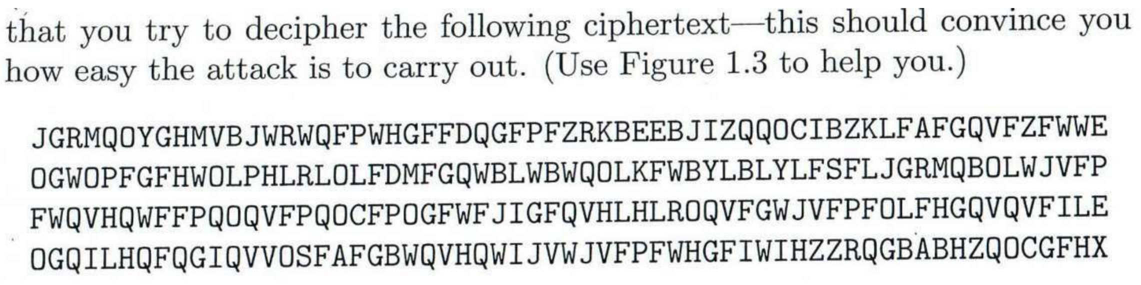
It is known that for a shift cipher brute forcing can be done to get the plain text. For the given cipher text, we can obtain the right plaintext by shifting the register with –7/+19.

The decrypted text is as follows: HOWMANYPOSSIBLEKEYSARETHERE.

With spaces, lower case and punctuation added (based on human knowledge!), the answer is, “How many possible keys are there?”

[TURN TO THE NEXT PAGE FOR AN ADDITIONAL PROBLEM FOR GRADUATE STUDENTS ONLY!]

3) [ECE 6156 only!] (10 pts.) Decrypt the text shown on page 12 of Katz and Lindell (also shown below). Please assume that a mono-alphabetic substitution cipher was used with a single key.



that you try to decipher the following ciphertext—this should convince you how easy the attack is to carry out. (Use Figure 1.3 to help you.)

```
JGRMQOYGHMVBJWRWQFPWHGFFDQGFPFZRKBEEBJIZQQOCIBZKLFAFGQVFZFWWE
OGWOPFGFHWOLPHLRLOLFDMFGQWBLWBWQOLKFWBYLBLYLFSFLJGRMQBOLWJVFP
FWQVHQWFFPQOQVFPQOCFPOGFWFJIGFQVHLHLROQVFGWJVFPFOLFHGQVQVFILE
OGQILHQFQGIQVVOSFAFGBWQVHQWIJVWJVFPFWHGFIWIHZZRQGBABHZQOCGFHX
```

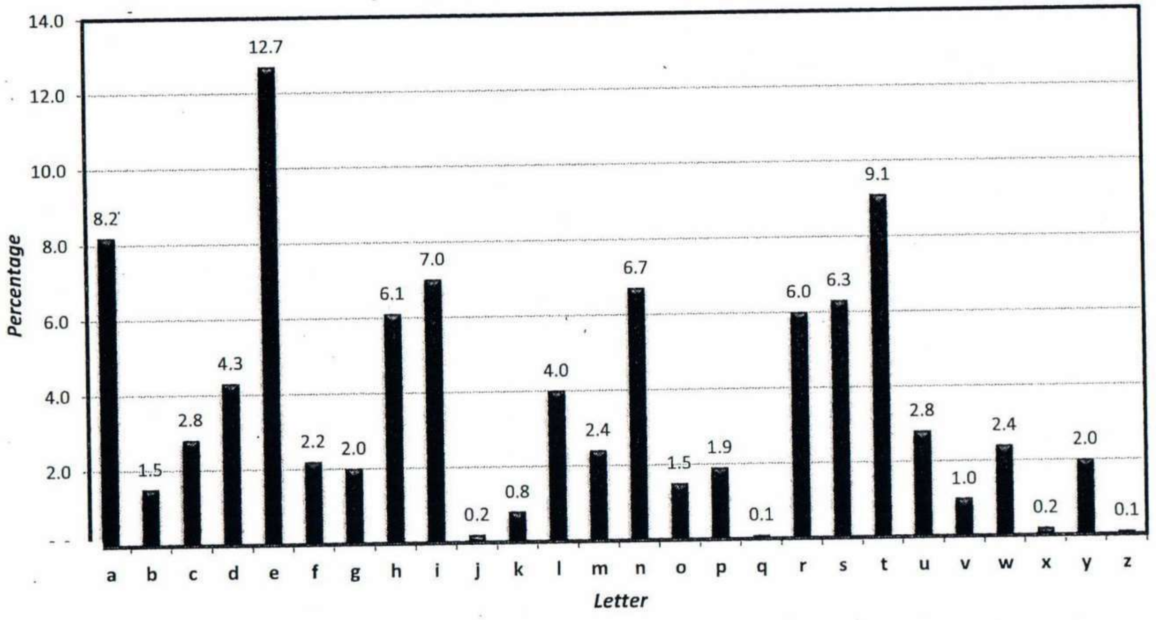


FIGURE 1.3: Average letter frequencies for English-language text.

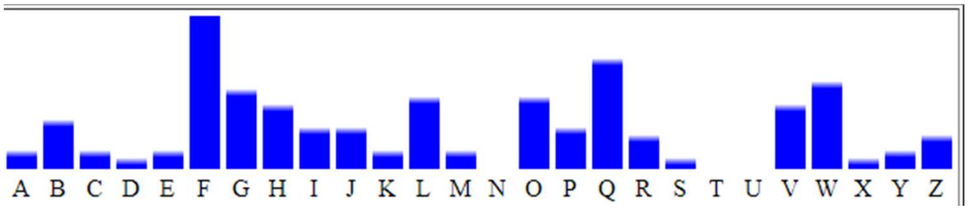
Also, to reduce unnecessary search time, it is hereby officially confirmed that the following substitutions are correct: F becomes E, W becomes S and Q becomes T. Please note that capitalization is completely ignored, so, for example, E in the plaintext would be "e" in most locations – in fact, it is also hereby officially revealed that the correct answer does not have the letter "e" at the beginning of any sentence and so it is always lower case.

Solution

It is given that F becomes E
W becomes S
Q becomes T.

To decipher, use an online frequency counter. Given below is the data obtained.

A	3
B	12
C	3
D	2
E	4
F	37
G	19
H	14
I	9
J	9
K	3
L	17
M	4
N	0
O	16
P	10
Q	26
R	7
S	2
T	0
U	0
V	15
W	21
X	1
Y	3
Z	7



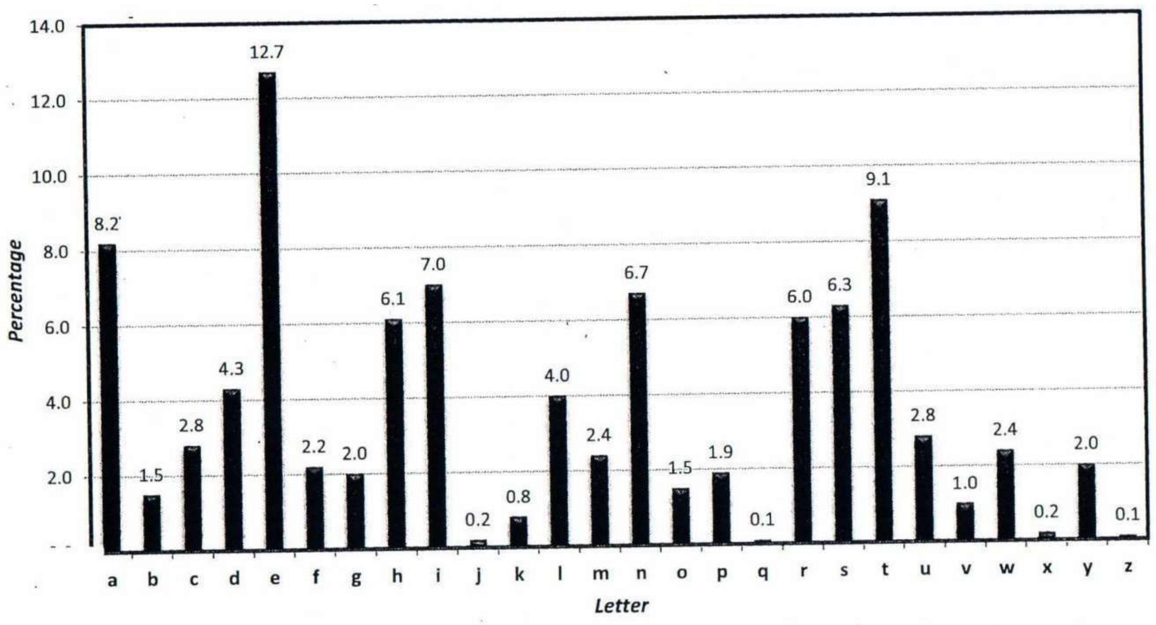


FIGURE 1.3: Average letter frequencies for English-language text.

It is assumed that based on the given graph and the character count we obtained, we can guess the other letters and try to get a meaningful decrypted text back. From the data we obtain the given decrypted character list.

A	3	H
B	12	C
C	3	J
D	2	K
E	4	F
F	37	E
G	19	Y
H	14	V
I	9	B
J	9	N
K	3	X
L	17	Z
M	4	P
N	0	L
O	16	O
P	10	M
Q	26	T
R	7	G
S	2	W
T	0	Q
U	0	I
V	15	A
W	21	S
X	1	D
Y	3	R
Z	7	U

Substituting the characters, you get the given text:

CRYPTOGRAPHICSYSTEMSAREEXTREMELYDIFFICULTTOBUILDNEVERTHELESS
FORSOMEREASONMANYNONEXPERTSINSISTONDESIGNINGNEWENCRYPTIONSC
HEMESTHATSEEMTOTHEMTOBEMORESECURETHANANYOTHERSCHEMEONEAR
THTHEUNFORTUNATETRUTHHOWEVERISTHATSUCHSCHEMESAREUSUALLYTRI
VIALTOBREAK

The answer is the following (with spaces and lower case added):

Cryptographic systems are extremely difficult to build nevertheless for some reason many non experts insist on designing new encryption schemes that seem to them to be more secure than any other scheme on earth the unfortunate truth however is that such schemes are usually trivial to break