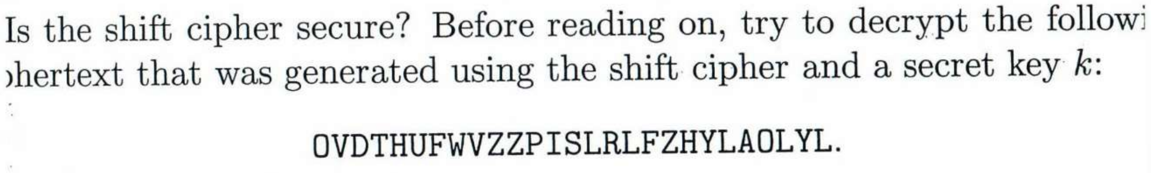
Hardware-Oriented Security and Trust
ECE 4156 A / ECE 6156 A
Spring 2024
Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology
Homework 1, 20 pts. (ECE 4156) 30 pts. (ECE 6156)
Due Friday January 12 prior to 11:55pm

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.

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).

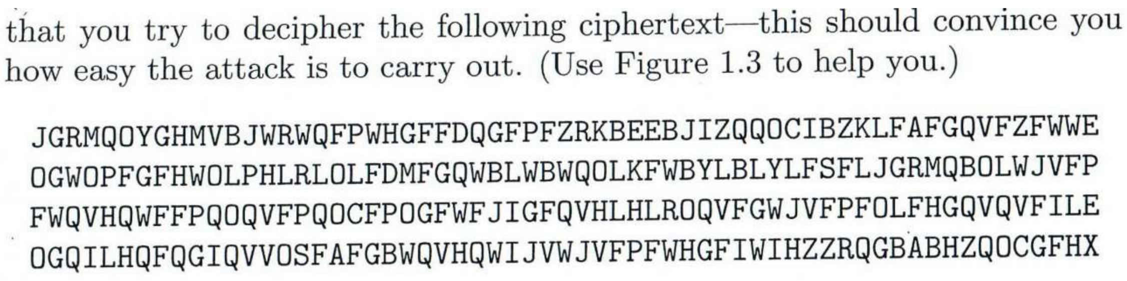


Is the shift cipher secure? Before reading on, try to decrypt the followi
hertext that was generated using the shift cipher and a secret key k:

OVDTHUFWVZZPISLRLFZHYLAOLYL.

[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
```

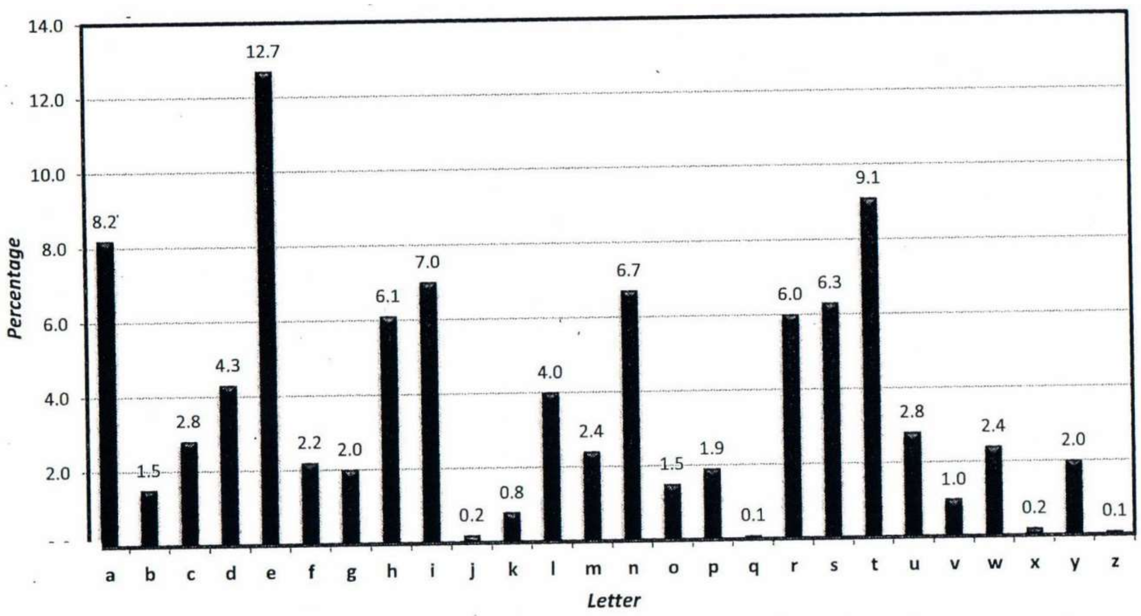


FIGURE 1.3: Average letter frequencies for English-language text.

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 actually 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.

YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES, INCLUDING OTHER/PREVIOUS SECTIONS OF ECE COURSES TAUGHT BY PROFESSOR MOONEY SUCH AS THOSE WITH NAMES INCLUDING HARDWARE ORIENTED SECURITY AND TRUST AS WELL AS CRYPTOGRAPHIC HARDWARE FOR EMBEDDED SYSTEMS. ALL HOMEWORK SUBMISSIONS MUST INCLUDE YOUR NAME, COURSE NUMBER, SECTION, AND THE HOMEWORK SET NUMBER. ALL SUBMISSIONS MUST BE DONE ONLINE. ALL WRITING MUST BE EASY TO READ (FOR EXAMPLE, YOU MAY HAVE TO WRITE WITH THICK INK AND MAY NOT BE ABLE TO USE LOW RESOLUTION PHOTOS OF HANDWRITTEN DIAGRAMS). FAILURE TO PROVIDE CLEAR AND LEGIBLE ANSWERS MAY RESULT IN ZERO POINTS. ALL WORK MUST BE YOUR OWN. NO PLAGIARISM IS ALLOWED, AND YOU MUST PROPERLY REFERENCE ALL SOURCES OF YOUR INFORMATION – ALTHOUGH YOU SHOULD NOT LOOK FOR AND MAY NOT CONSULT "SOLUTIONS" AVAILABLE FROM OTHER SOURCES (TO REPEAT, YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES OR ANY OTHER SOURCE!).