The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260 Data Security

GAME 5 Solutions

5th April 2019

Number of Questions: 5
Time allowed: 50min
Total marks: 5

In order to score marks you need to show all working/reasoning and not just the end result.

	Student Number	*Student Name*
Student 1		
Student 2		
Student 3		
Student 4		
Student 5		
Student 6		
Student 7		

Question 1	Question 2	Question 3	Question 4	Question 5	Total

1. In Vernam cipher the key is as long as the plaintext and it is a nonrepeating random sequence of characters, also represented as marks and spaces (0's and 1's); the key was punched on a paper tape, and each key-tape was meant to be used more than once.
Is such a system equivalent to a one-time pad (achieves perfect secrecy)?

- If so, outline why it is impossible to gain any knowledge about the contents of the plaintext regardless of how much is intercepted.
- If not, state at least one difference between Vernam cipher and a one-time pad, and outline a possible approach to attacking a Vernam cipher cipher.

Assume, if necessary, that the attacker is able to intercept the ciphertext and also to mount a chosen plaintext attack – that is, the attacker can put a new chosen plaintext through the system and obtain the corresponding ciphertext, encrypted with the same key as the original message .

Solution:
No, Vernam cipher is not equivalent to one time pad, because in Vernam the key is used more than once. If the key is reused, in a chosen plaintext attack the attacker is able compare the plaintext with the ciphertext to obtain the key.

2. Estimate the unicity distance of a transposition cipher with a period *d*, assuming that all keys are equally likely.

Solution:
$U = lg(d!)/3.2$, where lg is a logarithm for base 2.
To approximate U, we use Sterling's approximation for large *d*:
$d\,! \approx (d/e)^d(2\pi d)^{1/2}$.
Then lg $(d\,!) \approx d$ lg (d/e) and U = $(d$ lg$(d/e)) / 3.2 = 0.3\ d$ lg(d/e)

3. How many different encipherments can you get with a Rotor machine with 7 rotors? (Rotor machine has 26 input pins on front and 26 output pins on back)

Solution:
Formula: 26^k, where k is number of cylinders.
For k=7: number of enciperments = 8,031,810,176

4. A 15 character long ciphetext obtained by a monoalphabetic cipher was also engraved on a tombstone in St. Paul's Churchyard, New York, in 1796. The first published solution to this cipher appeared in the New York Herald in 1896 - over 100 years later.

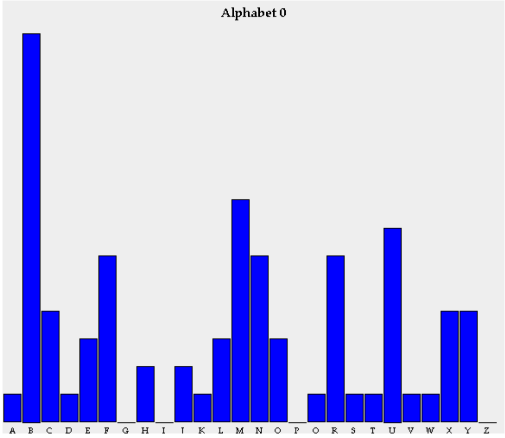
Why did it take so long to break this cipher?

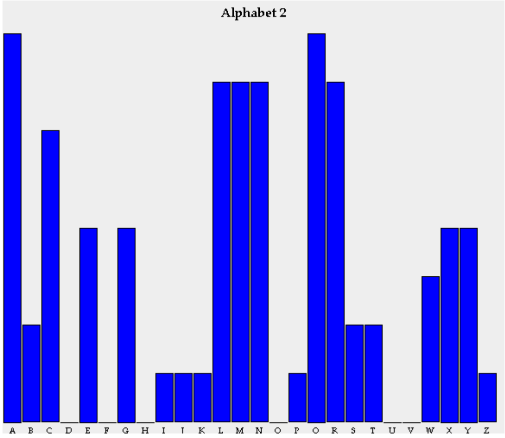
Solution: The reason why this was hard to break was that the intercepted ciphertext is only 15 characters long, while the unicity distance for the monolphabetic substitution cipher in approximately 27.6 characters.

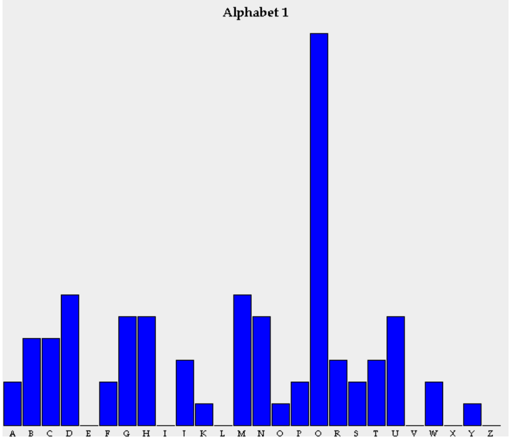
5. The following ciphertext was produced using a Beauford cipher with 4 alphabets:
FJLER AYECQ TDKQN NDGSW FHWHN UNHNB EUMMR FMGSL VQCEF HYHNC QZBSN DMMCT NUGSY QGYBQ BSRRQ ZRDAP BHAHC BQTBQ BHUMJ HOWCX TFEYX QMTJM LJYBX HXDAY MMNHA JAHMG ZQBNW JUQMS RGRHN FQPBD AIEWC ABURH SQNFH SXDBP MJXQR SXCLG RDYUB QRWBU CHLKM LHCLX EQLUL JGJUQ EYMNA TBYQR URRHB RLXEQ CEFDY HCTGU BHAPF TTHQG IHODE SYQNS YURGR CMDUP KHUML DNHQS WAMSF TQRMN QPMNA QBNWJ UQMLO QPXJQ NHCBX XLOX

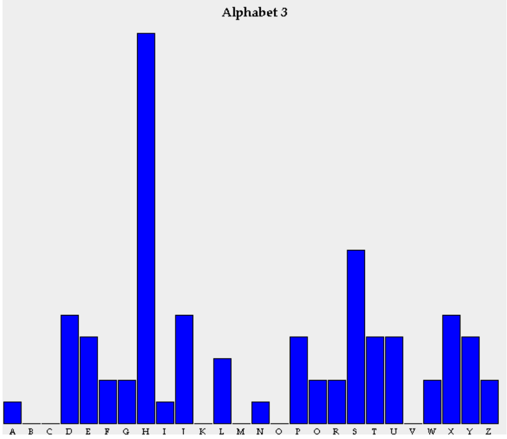
The frequency analysis is displayed below. Find the plaintext and the key.

Graphing Frequency Counts for 4 alphabets.









Solution:
Key: FUEL
Plaintext: Although delivery companies are starting to make changes, some critics say they need to do more. We need to see delivery companies switch their entire fleet of vehicles to ones powered by clean energy. Chief scientist for Green Peace UK says to be truly clean these would need to be charged by renewable power , rather than fossil fuel. It is not just about how the vehicles are powered though.