Assignment #2

CPEN 442

September 28, 2015

<zero>

Department of Electrical and Computer Engineering

University of British Columbia

Vancouver, Canada

# Problem #1

*Recover the plain text, name the cipher, provide the key, and describe your method.*

As of writing, I have neither recovered the plaintext nor the key to this cipher text. I began with an analysis of the cipher text. I wrote my tools in python, beginning with simple letter frequency counts, then bigraphs and trigraphs. My first approach was to naively decrypt the message by mapping each character by occurrence rank in cipher text to expected rank in plain English as provided by Peter Norvig on his website [1]. I knew out of the gate that this was not likely to produce much of substance as the provided cipher text is comparatively short for a proper frequency analysis to be much use. The distribution looks enough like a proper English distribution that I was fairly certain it was a mono-alphabetic substitution cipher but not close enough to normal to be a simple Caesar cipher. Figure 1 below shows the relative matching of frequencies between cipher and plain text.

After comparing my frequent 3-,4-, and 5- grams, I noticed a suspicious number of repeating sequences of 5 characters, specifically the sequence ‘GOZZT’. I wasn’t sure what this was at first, so kept it in mind as I looked towards the 3-grams instead. The most common 3-grams were ‘QEJ’ and ‘GOZ’. Because ‘QEJ’ was not a substring of my most frequent 5-gram, I chose to try it out as translated to ‘THE’. The remainder of the mappings were found in a similar manner, albeit with a hefty dose of trial and error. A breakthrough occurred when it became clear that my 5-gram ‘GOZZT’ was actually ‘COMMA’ in plaintext. Following this, discovering that ‘AOQ’ mapped to ‘DOT’, helped to give the message toms more structure, leading the way for a context-based approach to finishing the translation table. As I decrypted more of the message, it became apparent that it was a passage from The Lord of the Rings. I performed a Google search to identify the passage[2] and used the now known plaintext to finish the decryption. The final key is given in Table 1 below. Cipher characters are on top, plaintext counterparts on bottom.



Table 1- Problem 1 Cipher Key

The plaintext is:

“thebanquetwasverysplendidcommahowevercommathoughihadabadcoldatthetimecommairemembercommaandcouldonlysaythagyouverybuchdotinowrepeatitmorecorrectlythankyouverymuchforcomingtomylittlepartydotobstinatesilencedottheyallfearedthatasongorsomepoetrywasnowimminentandtheyweregettingboreddotwhycouldnthestoptalkingandletthemdrinkhishealthbutbilbodidnotsingorrecitedothepausedforamomentdotthirdlyandfinallycommahesaidcommaiwishtomakeanannouncement”.

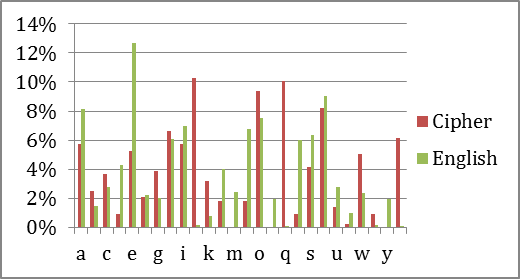


Figure 1- Relative Letter Frequencies

Formatted for readability and substitutions made for punctuation:

“the banquet was very splendid, however, though i had a bad cold at the time, i remember, and could only say thag you very buch. i now repeat it more correctly thank you very much for coming to my little party. obstinate silence. they all feared that a song or some poetry was now imminent and they were getting bored. why couldnt he stop talking and let them drink his health but bilbo did not sing or recite. he paused for a moment. thirdly and finally, he said, i wish to make an announcement”

# Problem #2

The first thing I did with the cipher text, as with problem 1, was to feed it into my text analysis tools. The frequency distribution looked similar but more flat than question I would have expected, given the length of the cipher text. Additionally, it had a complete lack of ‘J’ occurrences. The graphing can be seen below in Figure 2.

I remembered from class that this could be an indication of the Playfair cipher and decided to look at the bigraphs to see what they could tell me. There turned out to be no duplicate letters in bigraphs, leading me to strengthen my lean towards this being a Playfair cipher.

# Problem #3

*Demonstrate that the CRC is not a good candidate for a cryptographic hash function by showing it has almost no strong collision property.*

To illustrate the function’s lack of strong collision property, I had to find two values x and y such that the hash of x is equal to the hash of y. In order to find two values that result in a hash collision using CRC32, I first had to decide on a language with which to automate my task. I initially chose C# as it is the language I am most familiar with but I quickly became disillusioned with its performance and the usability of the CRC32 implementation I could find. I decided to switch language and learn Python as the PyCRC library was already provided as canonical. My python implementation generates ordered permutations of strings composed of the characters [a-z, 0-9], beginning at ‘a’ and growing to the length of 8, at which point I found a collision. The hash value that the collision occurred at is 2051433057. The first value to hash to that was acccddf4 and the second was aack8899. The total time to compute the hashes required to find the collision was 1 minute and 16 seconds. The total time I spent on this problem, inclusive of failed implementations, was roughly 12 hours.

# Problem #4

*Demonstrate that the CRC is not a good candidate for a cryptographic hash function by showing it has almost no weak collision property.*

Similar to question 3, my Python implementation permutes strings of [a-z, 0-9] and checks for a collision with the specific hash of my student number using PyCRC. The difference between this one and question three is that it is much less likely to find a collision with that specific hash than an arbitrary hash. As of writing, my solver program has been running for 4.5 hours. It will be allowed to run until morning, at which time I will re-evaluate my life choices if it hasn’t found anything.

## Question #a

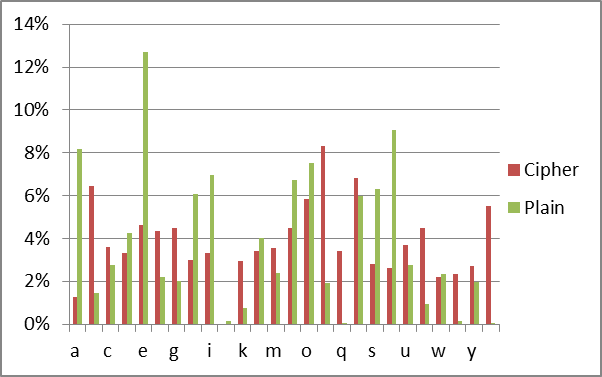


Figure 2 – Relative Letter Frequencies

Answer question #a here.

## Equations

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in Eq. 1, using a right tab stop. To make your equations more compact, you may use the solidus ( / ), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in

 

Note that the equation is centered using a center tab stop. Be sure that the symbols in your equation have been defined before or immediately following the equation. Use “Eq. 1” or “Equation 1”, not “(1)”, especially at the beginning of a sentence: “Equation 1 is . . .”

# Using the Template

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

## Authors and Affiliations

The template is designed so that author affiliations are not repeated each time for multiple authors of the same affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization). This template was designed for two affiliations.

### For Author/s of Only One Affiliation (Heading 3): To change the default, adjust the template as follows.

#### Selection (Heading 4): Highlight all author and affiliation lines.

#### Change Number of Columns: Select Format > Columns >Presets > One Column.

#### Deletion: Delete the author and affiliation lines for the second affiliation.

### For Authors of More than Two Affiliations: To change the default, adjust the template as follows.

#### Selection: Highlight all author and affiliation lines.

#### Change Number of Columns: Select Format > Columns > Presets > One Column.

#### Highlight Author and Affiliation Lines of Affiliation 1 and Copy this Selection.

#### Formatting: Insert one hard return immediately after the last character of the last affiliation line. Then paste down the copy of affiliation 1. Repeat as necessary for each additional affiliation.

#### Reassign Number of Columns: Place your cursor to the right of the last character of the last affiliation line of an even numbered affiliation (e.g., if there are five affiliations, place your cursor at end of fourth affiliation). Drag the cursor up to highlight all of the above author and affiliation lines. Go to Format > Columns and select “2 Columns”. If you have an odd number of affiliations, the final affiliation will be centered on the page; all previous will be in two columns.

## Identify the Headings

Headings, or heads, are organizational devices that guide the reader through your paper. There are two types: component heads and text heads.

Component heads identify the different components of your paper and are not topically subordinate to each other. Examples include Acknowledgments and References and, for these, the correct style to use is *“Heading 5”*. Use *“figure caption”* for your Figure captions, and *“table head”* for your table title. Run-in heads, such as “Abstract”, will require you to apply a style (in this case, italic) in addition to the style provided by the drop down menu to differentiate the head from the text.

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced. Styles named *“Heading 1”*, “*Heading 2”*, *“Heading 3”*, and *“Heading 4”* are prescribed.

## Figures and Tables

Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table captions should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation “Fig. 1” in the text, and “Figure 1” at the beginning of a sentence.

Use 8 point Times New Roman for figure labels. Use words rather than symbols or abbreviations when writing figure-axis labels to avoid confusing the reader. As an example, write the quantity “Magnetization”, or “Magnetization, M”, not just “M”.

If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write “Magnetization (A/m)” or “Magnetization {A[m(1)]}”, not just “A/m”. Do not label axes with a ratio of quantities and units. For example, write “Temperature (K)”, not “Temperature/K”.

## Footnotes

Use footnotes sparingly (or not at all) and place them at the bottom of the column on the page on which they are referenced. Use Times 8-point type, single-spaced.

1. Table Type Styles

| Table Head | Table Column Head | | |
| --- | --- | --- | --- |
|  | Table column subhead | Subhead | Subhead |
| copy | More table copya |  |  |

a. Sample of a table footnote. *(table footnote)*

1. Example of a figure caption. *(figure caption)*

We suggest that you use a text box to insert a graphic (ideally 300 dpi, with all fonts embedded) because, in an MSW document, this method is somewhat more stable than directly inserting a picture.

To have non-visible rules on Example of a figure caption. *(figure caption)* your frame, use the MSWord pull-down menu, select Format > Borders and Shading > Select ”None”.

To help your readers, avoid using footnotes altogether and include necessary peripheral observations in the text (within parentheses, if you prefer, as in this sentence).

Number footnotes separately from reference numbers, and in superscripts. Do not put footnotes in the reference list. Use letters for table footnotes.

##### References

List and number all bibliographical references in 9-point Times, single-spaced, at the end of your paper. When referenced in the text, enclose the citation number in square brackets, for example: [1]. Where appropriate, include the name(s) of editors of referenced books. The template will number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in “[3]”—do not use “Ref. [3]” or “reference [3]”. Do not use reference citations as nouns of a sentence (e.g., not: “as the writer explains in [1]”).

Unless there are six authors or more give all authors’ names and do not use “et al.”. Papers that have not been published, even if they have been submitted for publication, should be cited as “unpublished” [4]. Papers that have been accepted for publication should be cited as “in press” [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

1. Norvig, P. English Letter Frequency Counts: Mayzner Revisited or ETAOIN SRHLDCU. Retrieved September 28, 2015, from http://norvig.com/mayzner.html
2. Tiriel, E. (Ed.). (2007, July 29). Henneth Annûn Research Center. Retrieved September 28, 2015, from http://www.henneth-annun.net/events\_view.cfm?evid=1279
3. I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
4. K. Elissa, “Title of paper if known,” unpublished.
5. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
6. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
7. M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.