

Math 401 Fall 2019

Cryptology HW 2 Solutions

Due Thursday, September 12

1. Encrypt the plaintext message “NEVER ODD OR EVEN”, using a Vigenère cipher with key word “potato”.

Solution: POTATO becomes 15, 14, 19, 0, 19, 14 so we have

| | | | |
|------------|---------------|---------------|-------------|
| Plaintext | N E V E R | O D D O R | E V E N |
| Plaintext | 13 4 21 4 17 | 14 3 3 14 17 | 4 21 4 13 |
| Keystream | 15 14 19 0 19 | 14 15 14 19 0 | 19 14 15 14 |
| Ciphertext | 2 18 14 4 10 | 2 18 17 7 17 | 23 9 19 1 |
| Ciphertext | C S O E K | C S R H R | X J T B |

So the ciphertext is “CSOEK CSRHR XJTB”.

2. Decrypt the ciphertext “ODESL UKWGK SXMSK GEPP”, which was encrypted with Vigenère cipher using the key word “octopus”.

Solution: “OCTOPUS” becomes 14, 2, 19, 14, 15, 20, 18. So we have

| | | | | |
|------------|---------------|---------------|----------------|------------|
| Ciphertext | O D E S L | U K W G K | S X M S K | G E P P |
| Ciphertext | 14 3 4 18 11 | 20 10 22 6 10 | 18 23 12 18 10 | 6 4 15 15 |
| Keystream | 14 2 19 14 15 | 20 18 14 2 19 | 14 15 20 18 14 | 2 19 14 15 |
| Plaintext | 0 1 11 4 22 | 0 18 8 4 17 | 4 8 18 0 22 | 4 11 1 0 |
| Plaintext | A B L E W | A S I E R | E I S A W | E L B A |

This gives “ABLEW ASIER EISAW ELBA” or “Able was I, ere I saw Elba”.

3. Encrypt the plaintext message “RATS LIVE ON NO EVIL STAR”, using an Autokey cipher with the key word “vital”

Solution: VITAL is 21, 8, 19, 0, 11, so we have

| | | | | | |
|------------|------------|-------------|-------------|------------|------------|
| Plaintext | R A T S | L I V E | O N N O | E V I L | S T A R |
| Plaintext | 17 0 19 18 | 11 8 21 4 | 14 13 13 14 | 4 21 8 11 | 18 19 0 17 |
| Keystream | 21 8 19 0 | 11 17 0 19 | 18 11 8 21 | 4 14 13 13 | 14 4 21 8 |
| Ciphertext | 12 8 12 18 | 22 25 21 23 | 6 24 21 9 | 8 9 21 24 | 6 23 21 25 |
| Ciphertext | M I M S | W Z V X | G Y V J | I J V Y | G X V Z |

So the ciphertext is “MIMS WZVX GYVJ IJVY GXVZ”.

4. Decrypt the ciphertext “UBTW SEFH TTHF”, which was encrypted with an Autokey cipher using the key word “cipher”.

Solution:

“CIPHER” becomes 2, 8, 15, 7, 4, 17. So we have

| | | | |
|------------|------------|-------------|------------|
| Ciphertext | U B T W | S E F H | T T H F |
| Ciphertext | 20 1 19 22 | 18 4 5 7 | 19 19 7 5 |
| Keystream | 2 8 15 7 | 4 17 18 19 | 4 15 14 13 |
| Plaintext | 18 19 4 15 | 14 13 13 14 | 15 4 19 18 |
| Plaintext | S T E P | O N N O | P E T S |

Thus we get “STEP ONNO PETS” or “step on no pets.”

5. Compute **by hand** the indices of coincidence of each one of the following strings. Show your work.

- (a) It is a truth universally acknowledged (33)
- (b) that a single man in possession of a good (33)
- (c) fortune must be in want of a wife (26)

Solution: The frequency charts for each string are

(a)

| | | | | | | |
|-----------|-----------|-----------|-----------|-----------|-----------|---|
| Letter | A B C D E | F G H I J | K L M N O | P Q R S T | U V W X Y | Z |
| Frequency | 3 0 1 2 3 | 0 1 1 3 0 | 1 3 0 2 1 | 0 0 2 2 3 | 2 1 1 0 1 | 0 |

 length 33

(b)

(c)

| | | | | | | |
|-----------|-----------|-----------|-----------|-----------|-----------|---|
| Letter | A B C D E | F G H I J | K L M N O | P Q R S T | U V W X Y | Z |
| Frequency | 4 0 0 1 2 | 1 2 1 3 0 | 0 1 1 4 5 | 1 0 0 5 2 | 0 0 0 0 0 | 0 |

 length 33

(d)

(e)

| | | | | | | |
|-----------|-----------|-----------|-----------|-----------|-----------|---|
| Letter | A B C D E | F G H I J | K L M N O | P Q R S T | U V W X Y | Z |
| Frequency | 2 1 0 0 3 | 3 0 0 2 0 | 0 0 1 3 2 | 0 0 1 1 3 | 2 0 2 0 0 | 0 |

 length 26

So the indices of coincidence are

(a)

$$\frac{1}{33 \cdot 32} (3 \cdot 2 + 2 \cdot 1 + 3 \cdot 2 + 3 \cdot 2 + 3 \cdot 2 + 2 \cdot 1 + 2 \cdot 1 + 2 \cdot 1 + 3 \cdot 2 + 2 \cdot 1) = \frac{40}{1056} = .0378.$$

(b)

$$\frac{1}{33 \cdot 32} (4 \cdot 3 + 2 \cdot 1 + 2 \cdot 1 + 3 \cdot 2 + 4 \cdot 3 + 5 \cdot 4 + 5 \cdot 4 + 2 \cdot 1) = \frac{76}{1056} = .07196.$$

(c)

$$\frac{1}{26 \cdot 25} (2 \cdot 1 + 3 \cdot 2 + 3 \cdot 2 + 2 \cdot 1 + 3 \cdot 2 + 2 \cdot 1 + 3 \cdot 2 + 2 \cdot 1 + 2 \cdot 1) = \frac{34}{650} \approx .05231.$$

6. Compute the mutual index of coincidence for each pair of strings in the previous problem. Show me your work.

Solution: To calculate the mutual indices of coincidence, we get

(a) and (b):

$$\begin{aligned} \frac{1}{33 \cdot 33} (3 \cdot 4 + 2 \cdot 1 + 3 \cdot 2 + 1 \cdot 2 + 1 \cdot 1 + 3 \cdot 3 + 3 \cdot 1 + 2 \cdot 4 + 1 \cdot 5 + 2 \cdot 5 + 3 \cdot 2) \\ = \frac{64}{1089} \approx .05877. \end{aligned}$$

(a) and (c):

$$\frac{1}{33 \cdot 26} (3 \cdot 2 + 3 \cdot 3 + 3 \cdot 2 + 2 \cdot 3 + 1 \cdot 2 + 2 \cdot 1 + 2 \cdot 1 + 3 \cdot 3 + 2 \cdot 2 + 1 \cdot 2) = \frac{48}{858} \approx .055944.$$

(b) and (c):

$$\frac{1}{33 \cdot 26} (4 \cdot 2 + 2 \cdot 3 + 1 \cdot 3 + 3 \cdot 2 + 1 \cdot 1 + 4 \cdot 3 + 5 \cdot 2 + 5 \cdot 1 + 2 \cdot 3) = \frac{57}{858} \approx .06653.$$

7. Compute **by hand** the index of coincidence of the following string. What is unusual about this string?

A quick brown fox jumps over the lazy dog

Solution: This text has 33 letters, with four “o”s, 2 “a”, “e”, “r”, and “u”, and 1 of each other letter. Thus the index of coincidence is

$$\text{IndCo} = \frac{1}{33 \cdot 32} (4 \cdot 3 + 2 \cdot 1 + 2 \cdot 1 + 2 \cdot 1 + 2 \cdot 1) = \frac{20}{33 \cdot 32} = \frac{5}{33 \cdot 8} \approx .019.$$

This is really unusually low—much lower than you’d expect even for completely random text. In a very long text you can’t go much below .036, but this text is so short that we can have a very low index of coincidence.

(The text is famously a *panagram*: a sentence that contains each letter at least once. It is not a perfect pangram, containing each letter exactly once; such a sentence would have an index of coincidence equal to zero. Perfect pangrams exist, but tend to be strange and extremely awkward in phrasing (“Mr Jock, TV quiz PhD, bags few lynx”).)

For the remaining problems, you may use an index of coincidence calculator like the one at <http://www.practicalcryptography.com/cryptanalysis/text-characterisation/index-coincidence/>

You should be able to copy and paste the ciphertexts from the PDF.

8. Which of the following is likely to be a message encrypted with a simple substitution cipher?

- (a) GSZES GNUBE SZGUG SNKGX CSUUE QNZOQ EOVJN VXKNG XGAHS AWSZZ BOVUE SIXCQ
NQESX NGEUG AHZQA QHNSP CIPQA OIDLV JXGAK CGJCG SASUB FVQAV CIAWN VWOVP
SNSXV JGPCV NODIX GJQAE VOOXC SXXCG OGOVA XGNVU BAVKX QZVQD LVJXQ EXCQO
VKCQG AMVAX VWXCG OOBOX VZCSO SPPSN VAXUB DVVAX QJQAJ VSUXC SXXCV OVJCS
NSJXV NOJQA MVBSZ VOOSH VSAWX QHGMV GWVSX CSXXC VBSNV ZNVVN SAWQZ ORVXJ
CVOQE JCGUW NVA
- (b) DWVQP IIKOP UUYGC ZJDRU ZDSHI CXEAO AKRZC QAMSM DNQLF LUJYI IMJPJ VJZQL
GCJSN XTXFL MWOLW IFUQK DBBEY HVMVF ZOJXV FYMJA RDTGT TZQKL YNHPD UPUYU
XKNOI DXZXG IHIWK VXZET XFMO S KGIWU EIFDW RLLXH PZXPI VFWKL THEAS IROWC
GJAYJ KKODL WXFPI ZVUIK LEXEL IOWVC YMFMR UIZUD CETFE TBPIX SWSPZ MRPKP
LIYKL FGSTJ ZTPUH AEBQC QAEPQ GIAKH TDUVM KFGEU MWHAY ZGVSJ LNLJJ MLPEO
YEMZU PYMEW XLG

Solution: We compute the indices of coincidence. The index of coincidence of the first sample is $\approx .063$, and the index of coincidence of the second sample is $\approx .039$. Thus the second looks more like random text, and the first looks like it was encrypted with a simple substitution cipher.

9. Consider the following ciphertext:

TOGMG GBYMK KCQIV DMLXK KBYIF VCUEK CUUIS VVXQS PWWEJ KOQGG PHUMT WHLSF
YOVVW KNHMM RCQFQ VVHKW PSUED UGRSF CTWIJ KHVFA THKEF FWPTJ GGVIV CGDRA PGWVM
OSQXG HKDVT WHUEV KCWYJ PSGSN GFWSL JSFSE OOQHW TOFSH ACIIN GFBIF GABGJ ADWSY
TOPML ECQZW ASGVS FWRQS FSFVQ RHDRS NMVMK CBHRV KBLXK GZI

- (a) Use the Kasiski test (either by shifting the text over one-by-one, or by comparing repeated trigrams) to guess the keyword length. (Hint: the repeated trigrams are LXX at 17 and 232; TWH at 54 and 134; NGF at 149 and 174; and SFS at 156 and 209).

Solution: We see that the offsets that the trigrams have are $232 - 17 = 215$; $124 - 54 = 80$; $174 - 149 = 35$; $209 - 156 = 53$. Since the first three have 5 as a common factor, we might guess the keyword has length five.

Alternately, we can offset the text and look for coincidences. With an offset of 2 or 3 there are eight coincidences; with an offset of 4 there are 4; with an offset of 5 there are 16; with an offset of 6 there are 10; with an offset of 7 or 8 there are 9. This gives more weak evidence that the keyword has length 5.

- (b) Use the tool at <http://jaydaigle.net//substring.html> to split the text up into substrings. Test the index of coincidence of each substring, and use this to determine the key length. Does this match your answer in part (a)?

Solution: If we use three substrings, the indices are .044, .041, .044. If we use four, the indices are .039, .042, .040, .045. If we use five, the indices are .062, .069, .059, .072, .056, which is high enough that this is almost certainly the

correct keylength. But for completeness we see that with six substrings we get .037, .045, .046, .044, .031, .035, and with seven we get .046, .029, .032, .041, .036, .032, .046. So at this point we're pretty sure the keyword has length 5.

- (c) Find the keyword and decrypt the message. You can use frequency analysis on substrings, or you can use mutual indices of coincidence, but be sure to show intermediate steps so I can see what you did.

Solution: The keyword is `codes` and the message is

radio, envisioned by its inventor as a great humanitarian contribution, was seized upon by the generals soon after its birth...and impressed as an instrument of war....But radio turned over to the commander a copy of every enemy cryptogram it conveyed....Radio made cryptanalysis an end in itself.

10. Would the method we used on the Vigenère cipher work to decrypt an autokey cipher? Why or why not?

Solution: No, because the keystream does not repeat. As we saw in class this week, the autokey cipher is quite vulnerable, but since the keystream doesn't repeat you can't use substring analysis to find the keyword. However, the keystream comes from *somewhere*, and we can attack that connection.

11. The ciphertext `bxo tam det xzx pjl baj lqf asa mde ohy wpc wlb ajl` was encrypted with an autokey cipher. Decrypt it, using the knowledge that the word "the" appears.

Solution: `itw ast heb est oft ime sit was the wor sto fti mes` or "It was the best of times, it was the worst of times".