Northeastern Section Meeting Sample Article

1 Basic Text

The purpose of this file is to let you see what a document typeset in Mathbook XML looks like. This is by no means a complete sample of all of the possibilities of this system.

Definition 1.1 (RSA Encryption System)**.** Given two primes p and q we encipher a message M using the **RSA Encryption System** by calculating

$$C \equiv M^e \pmod{n}$$

where $n = p \cdot q$ and e is the public enciphering key which must be relatively prime to $\phi(n)$.

2 Images

Inserting an image with a pre-existing image file:

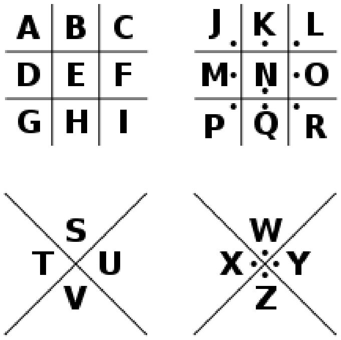


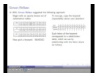
Figure 2.1: Pigpen Cipher Key

Inserting images with the picture environment or tikz:

$$\begin{tikzcd}
& M \arrow[d] & \\
& IP\text{=[2,6,3,1,4,8,5,7]} \arrow[dl] \arrow[dr] & \\
L_0 \arrow[drr] & & R_0 \arrow[dll] \\
L_1 = R_0 \arrow[d] & & R_1 = L_0 \oplus f(R_0, K_0) \arrow[d] \\
L_2 = L_1 \oplus f(R_1, K_1) \arrow[dr] & & R_2 = R_1 \arrow[dl] \\
& IP^{-1}\text{=[4,1,3,5,7,2,8,6]} \arrow[d] & \\
& C &
\end{tikzcd}$$

Figure 2.2: Really Simple DES

Inserting an instructional video from YouTube:



https://www.youtube.com/watch?v=5ISnCm4_V-Y

Figure 2.3: Modern look at the Vigenère Cipher

3 Falconer's Transposition

3.1 Enciphering the Transposition

A New Method How to Write Secretly by the Art of Combinations

1. To write by the method proposed, a certain number of letters are combined to lock and unlock the epistle. The differences of writing down the positions [of the letters] ... may be varied to a vast number; ...
2. The order of rows is agreed upon in parting.
3. The number of letters combined, which is the key, may be expressed in the epistle by some mathematical figure, as △ for three letters, □ for 4, etc. or by some private mark.
4. They [the individuals communicating] frame a rectangular table of as many columns as there are letters combined.
5. The letters so combined are placed in their natural order along the top of the table.
6. Having determined of how many lines the table shall consist, the order of combinations agreed upon is set down in a row in the first column towards the left hand; as you may see in the following table.
7. The table being thus prepared for writing, they observe the order of the combinations, and write according to its direction.
8. When they have placed one letter of every column of all the lines, they begin a new, and so go on until the writing be finished.
9. And lastly, they take the letters out of the table according to their partitions, as so many barbarous words, upon paper apart and send it to the confidant. - John Falconer

Let's see if you can follow Falconer's directions. Below I set up Table 3.1 according to his description in steps (5) and (6) and used it to encipher the pangram *"the quick brown fox jumps over the lazy sleeping dog."*

		A	B	C
1	CBA			
2	CAB			
3	ACB			
4	BCA			
5	BAC			

Table 3.1: Falconer's Transposition Table Initial Setup

		A	B	C
1	CBA	E	H	T
2	CAB	U	I	Q
3	ACB	C	B	K
4	BCA	W	R	O
5	BAC	F	N	O

Table 3.2: Falconer's Transposition Table First Pass

		A	B	C
1	CBA	EUS	HJY	TXZ
2	CAB	UPE	ISE	QML
3	ACB	COP	BEN	KVI
4	BCA	WHO	RRG	OTD
5	BAC	FL	NEG	OA

Table 3.3: Falconer's Transposition Table Filled Table

Final Message:

> "△ EUS HJY TXZ UPE ISE QML COP BEN KVI WHO RRG OTD FL NEG OA"

Refection Questions:

- Looking at Table 3.2 why is *the* from the beginning of the sentence written backwards? (Be sure to look carefully at the letters to the left of the row when answering.)

- In the second row of the same table why is *qui* from *quick* written in the order it is written? (Again, be sure to look carefully at the letters to the left of the row when answering.)

- In the last row we put down *n* from *brown* and the *fo* from *fox*, why are they in the order they are in and looking at the next table (Table 3.3) where do we put the *x* from *fox* and why?

- How do we finish writing the rest of the message into the boxes in the table?

- Refection Questions: Looking at the final message why is there a little triangle at the start of the message and why were the blocks of letters written in the order they were written?

- In what ways is this different from other ciphers we have looked at? (Hint: in this cipher what does cipher text *E* represent, or cipher text *F*?)

3.2 Decrypting the Transposition

After walking us through a careful exposition of how to find all the factors of a number and encouraging us to use this in order to find out the number of letters used for our key, Falconer lets us know that there is effectively an easier way to attack his own cipher.

> “or rather for dispatch, take out the seeming words, and write them down in [columns] beginning at the first, and then proceed to the second, third, fourth, fifth, etc., until you have gone through them” - John Falconer

Let’s follow Falconer’s advice using the message we used when we introduced his cipher in Section 3:

> “△ EUS HJY TXZ UPE ISE QML COP BEN KVI WHO RRG OTD FL NEG OA”

Which transforms to the following when we rewrite it following Falconer’s directions:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	E	H	T	U	I	Q	C	B	K	W	R	O	F	N	O
2	U	J	X	P	S	M	O	E	V	H	R	T	L	E	A
3	S	Y	Z	E	E	L	P	N	I	O	G	D	·	G	·

Table 3.4: Transpose Table for a Falconer Cipher

> “1. Search in the several lines for some of the particles [(words or n-grams)] of that language you shall suppose the epistle to have been writ in. If in English, make suppositions, e.g. for such little words as *the, that, for, of, to, and, etc.* and the like, without some of which no man can well express business of any moment.”
>
> “2. Having supposed in any of the lines; for some one of those mentioned, or the like particles, you may prove the truth of your supposition, by taking out the opposite letters of all the lines: And if they do not make words, or syllables, or produce such letters as can probably follow one another in that order, your first supposition is false, and you must suppose anew.”
>
> “3. Having by fresh suppositions found some useful word: And the letters of the other lines (in the same order) agreeing, the words or syllables arising from them, will direct you to some new [column] that goes before or after in the true order: And thus you may proceed till you have found out the whole writing, which by this time will be no great difficulty.” - John Falconer

Taking Falconer’s advice from step one look at each line of Table 3.4 we created above as you consider the following.

- Are there three letters in line one which we would expect to go together assuming this is written in English?
- There is a Q in row one column six, what needs to come after that? What column is it in?

- Looking now at line two what three letters do we again see that should go together?
- In line three are there three letters you could put together to get a common English ending? Are there other letters you could arrange with them in order to get an entire word?
- Finally, columns thirteen and fourteen only have two characters in them each, where do you think they belong if we were to rearrange the lines?

Use the observations you just made in order to rearrange the columns in the table, you should make a copy of this table to help you.

Col's															
1	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__
2	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__
3	__	__	__	__	__	__	__	__	__	__	__	__	__	__	__

Table 3.5: Blank Transpose Table for a Falconer Cipher

Test your understanding by working on the following exercises of increasing size, be patient they are finicky and time consuming. As a hint, all of the quotes contain the word *WINTER*.

Exercise 3.6. Try to use this new method to decipher this quote.

```
IRPL WPDL FSNE INIH NIEE
RBY  OFY  TNRY CEB  EGC
MAS  SBH  ERS  CEE  AHS
```

Hint.

- Transpose each block, you will end up with a table of four lines and fifteen columns.
- Can you find common or even not so common words or combinations in any lines?
- When you rearrange the columns do you see more words?
- Stay organized, if you don't keep things lined up this will never work

A few closing observations:

- Look carefully at how the blocks of characters (columns in the tables) are grouped after they are deciphered, i.e. did you ever get column one next to column thirteen or fourteen?
- Why do you think this happened? How might it be related to the number of key letters?
- Given your answers to the previous questions, how can we make use of Falconer's strategies for finding divisors and the number of key letters?

4 Sage Incorporation

Falconer Cipher Cell

```
import textwrap
import re
@interact
def falconer(message=input_box("The␣quick␣brown␣fox␣jumps␣
    over␣the␣lazy␣sleeping␣dog.",
                                  label="Message:",
                                      type=str, width=50,
                                      height=3),
             keys=input_grid(1,6,default=["CBA", "CAB",
                 "ACB", "BCA","BAC",""],
                    label="Keys:", to_value=list, type=str),
            chars=[3..5]):
    text = re.sub('[^A-Z]',''
        ,str(message.encode('ascii','replace')).upper())
    columns = "ABCDE"
    key = keys[0]
    while "" in key: key.remove("")
    message_table = [["" for x in range(chars)] for y in
        range(len(key))]
    for i in xrange(0,len(text),chars):
        row = (i/chars)%len(key)
        for j in range(chars):
            try:
                col = columns.index(key[row][j])
            except:
                col = chars-1 #pass
            try:
                message_table[row][col] += str(text[i+j])
            except:
                pass
    out_message = ""
    print "Chracters␣in␣text:␣",len(text)
    print "Cipher␣Table:"
    for k in range(len(key)):
        print
            "\t",str(key[k][0:chars]),":\t","\t".join(message_table[k])
        for i in range(chars):
            out_message += str(message_table[k][i])+"␣"
    print "Completed␣Message:"
    #for i in xrange(0,len(out_message),50):
    #    print
        "\t",out_message[i:min(i+50,len(out_message))].strip()
    print textwrap.fill(out_message, 50)
```