Spring 2015
Chris Christensen
MAT/CSC 483

Permutation Ciphers

There are two common techniques used to construct ciphers: substitution and permutation. Substitution replaces plaintext letters or strings of letters by letters or numbers or symbols. Permutation uses the plaintext message letters but rearranges their order.

Affine ciphers, keyword ciphers, the Hill cipher, the Playfair cipher, and the Vigenère cipher are all examples of substitution ciphers. Frequency analysis is a tool to identify the substitutions. Frequency analysis of a ciphertext message that has been enciphered using a permutation cipher reveals only plaintext frequencies.

Consider the following plaintext message.

```
monoalphabeticunilateralsubstitutionsystem
```

We will encipher it using a permutation that divides the message into 5-letter blocks,

```
monoa lphab eticu nilat erals ubsti tutio nsyst em
```

Because the numbers of the letters in the plaintext message is not a multiple of 5, the last block must be padded. Padding must be chosen so that the person who receives the ciphertext message and deciphers it can distinguish the message from the padding. In this example, the last block is padded with x's.

```
monoa lphab eticu nilat erals ubsti tutio nsyst emxxx
```

Then we rearrange the letters of the blocks according to the following permutation:

1	2	3	4	5

4	5	1	3	2

The letter in the first position of the block (on the left) moves to position 3, the letter in position 2 moves to position 5, the letter in position 3 moves to position 4, the letter in position 4 moves to position 1, and the letter in position 5 moves to position 2.

After the permutation is applied to the first block, we have:

m o n o a

1	2	3	4	5

4	5	1	3	2

o a m n o

When the permutation is applied to all the blocks, we obtain:

```
monoa lphab eticu nilat erals ubsti tutio nsyst emxxx
oamno ablhp cueit atnli lsear tiusb onttu stnys xxexm
```

So, the ciphertext message is

```
oamnoablhpcueitatnlilseartiusbonttustnysxxexm
```

If desired, the ciphertext can be divided into blocks for transmission.

Here is a ciphertext message enciphered using the 5-letter permutation give above.

```
THNROKEENRCKNUTIVYNUITESRXXYXX
```

The message is deciphered by applying the inverse of the permutation:

> The letter in the first position of the block (on the left) moves to position 4, the letter in position 2 moves to position 5, the letter in position 3 moves to position 1, the letter in position 4 moves to position 3, and the letter in position 5 moves to position 2.

4	5	1	3	2

```
   THNROKEENRCKNUTIVYNUITESRXXYXX
THNRO KEENR CKNUT IVYNU ITESR XXYXX
north ernke ntuck yuniv ersit yxxxx
```

Now we encipher the plaintext message

```
monoalphabeticunilateralsubstitutionsystem
```

with a permutation of 10-letter blocks.

1	2	3	4	5	6	7	8	9	10

3	8	2	5	9	7	4	6	10	1

The plaintext message is divided into 10-letter blocks and padded as needed.

```
monoalphab eticunilat eralsubsti tutionsyst emxxxxxxxx
```

After the permutation is applied to the first block, we have:

m	o	n	o	a	l	p	h	a	b
1	2	3	4	5	6	7	8	9	10

3	8	2	5	9	7	4	6	10	1
n	h	o	a	a	p	o	l	b	m

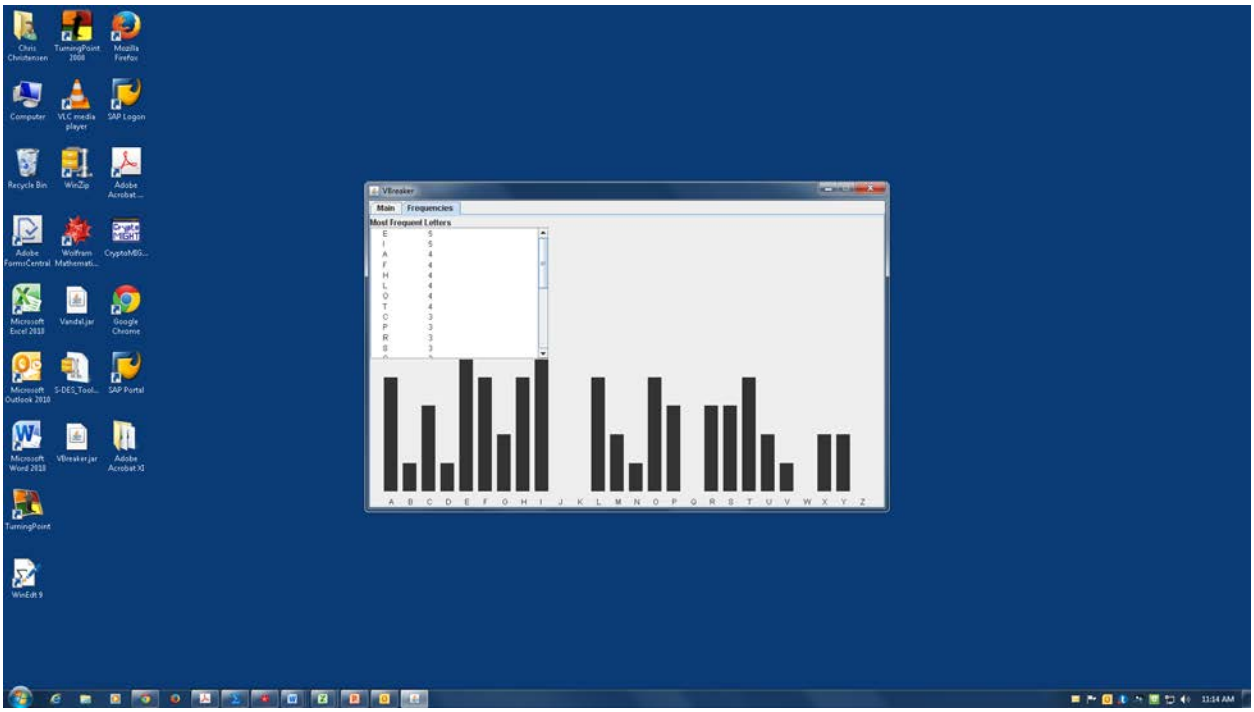
When the permutation is applied to all the blocks, we obtain:

```
monoalphab eticunilat eralsubsti tutionsyst emxxxxxxxx
nhoaapolbm iltuaicnte asrstbluie tyuossintt xxmxxxxxxe
```

Here is a ciphertext message to cryptanalyze:

```
OEMHTMFATSISFUOIDCLEIERHPCLLANOPTYRIGYOLAHETSXGVFXEPHIC
BUFAR
```

Frequencies suggest that a permutation cipher was used:



The number of letters in the ciphertext message is 60. The length of the block must divide 60; so, the number of letters in a block could be: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, or 60. There is no obvious padding.

Let's pick a block length to try. Say, 5 (which happens to be an excellent choice).

```
OEMHT MFATS ISFUO IDCLE IERHP CLLAN OPTYR IGYOL AHETS
XGVFX EPHIC BUFAR
```

Cryptanalysis is accomplished by anagramming the blocks simultaneously.

Arrange the 5-letter blocks in a column.

```
OEMHT
MFATS
ISFUO
IDCLE
IERHP
CLLAN
OPTYR
IGYOL
AHETS
XGVFD
EPHIC
BUFAR
```

`E`, `H`, and `T` stand out in the first block. Let's arrange them to be `the` and arrange the other blocks similarly.

```
the
stf
ous
eld
phe
nal
ryp
log
sth
xfg
cip
rau
```

It seems that the best arrangement for the first block is `themo`. Arrange the other blocks similarly.

```
themo
stfam
ousfi
eldci
pheri
nallc
rypto
logyi
sthea
dfgvx
ciphe
raufb
```

The plaintext message is

```
themostfamousfieldcipherinallcryptologyistheadfgvxciphe
raufb
```

or

```
the most famous field cipher in all cryptology is the
adfgvx cipher aufb
```

`aufb` appears to be padding.