34  

CHAPTER 3. TRANSPOSITION CIPHERS

12. Find some information about how route ciphers work, and the Union route cipher that was used during the American Civil War, and write a summary of your findings.

13. Find some information about how double transposition ciphers work, and the double transposition ciphers that were used during World Wars I and II, and write a summary of your findings.

3.2 Cryptanalysis of Transposition Ciphers

3.2.1 Cryptanalysis of Simple Columnar Ciphers

For a simple columnar transposition cipher, the only key is the number of columns in the array. Thus, for a ciphertext formed using a simple columnar transposition cipher, the cipher can usually be broken by a brute force attack, meaning we would try arrays with various numbers of columns (in some systematic fashion) until obtaining the correct plaintext.

Example 3.6 Consider the ciphertext TANHY IHWGA MEEAR TYNSS YDFDE ATARS, which was formed using a simple columnar transposition cipher. To decrypt this message without knowledge of the number of columns in the array, we will first try an array with two columns. Since there are 30 letters in this message, for an array with two columns there will be $30/2 = 15$ letters per column. This yields the following array.

```
T  T
A  Y
N  N
H  S
Y  S
I  Y
H  D
W  F
G  D
A  E
M  A
E  T
E  A
A  R
R  S
```

Transcribing this array by rows gives TTYNNHSIYHDWFDAEMAETEARRS, which is clearly not the correct plaintext. So next we will try an array with three columns. For an array with three columns there will be $30/3 = 10$ letters per column. This yields the following array.
3.2. *CRYPTANALYSIS OF TRANSPOSITION CIPHERS*

Transcribing this array by rows gives $\text{TMYAEDHADYREITAHYTWNAGSRASS}$, which is also clearly not the correct plaintext. So we will try an array with four columns. For an array with four columns, dividing the number of letters by the number of columns yields the following.

\[
\begin{array}{c}
4 \div 30 \\
-28 \\
2
\end{array}
\]

Thus, the first two columns of the array will contain eight letters, and the remaining two columns will contain seven. This yields the following array.

\[
\begin{array}{cccc}
T & G & Y & D \\
A & A & N & E \\
N & M & S & A \\
H & E & S & T \\
Y & E & Y & A \\
I & A & D & R \\
H & R & F & S \\
W & T
\end{array}
\]

Transcribing this array by rows gives $\text{TGYDANMSAHESTYEYAIADRHRFSWT}$, which is still clearly not the correct plaintext. So we will try an array with five columns, and $30/5 = 6$ letters per column.

\[
\begin{array}{cccc}
T & H & E & S & E \\
A & W & A & S & A \\
N & G & R & Y & T \\
H & A & T & D & A \\
Y & M & Y & F & R \\
I & E & N & D & S
\end{array}
\]

Transcribing this array by rows finally gives the correct plaintext **THE SEA WAS ANGRY THAT DAY MY FRIENDS.**

---

9George Costanza, quote.
3.2.2 Cryptanalysis of Keyword Columnar Ciphers

Because keyword columnar transposition ciphers do not necessarily take the columns of the cipher array in order, cryptanalysis can be more difficult than it is for simple columnar transposition ciphers. To break a keyword columnar transposition cipher by a brute force attack, not only must arrays with various numbers of columns be considered, but various ways to order the columns of these arrays must be considered as well. The cryptanalysis process can be simplified, however, if a part of the plaintext longer than the keyword(s) is known. When trying to break any type of cipher, we call a known part of a plaintext a crib.

Example 3.7 Consider the ciphertext AHLCC MSOAD NWSSS MTSSI AASDI NRVLF WANTO ETITIA IDERI HLEYL AECVL W, which was formed using a keyword columnar transposition cipher, and suppose we have the crib THEFAMILY. (That is, suppose we know THE FAMILY is part of the corresponding plaintext.) To try to decrypt this message, in the hope that our crib is longer than the keyword(s) for the cipher, we will start by assuming there are exactly eight letters in the keyword(s). If there are eight letters in the keyword(s), then the array will have eight columns, and the crib would appear in these columns in the following form.

THEFAMILY

Thus, the digraph TY would have to appear in the ciphertext. However, TY does not appear in the ciphertext, and so there are not exactly eight letters in the keyword(s). So next we will assume there are exactly seven letters in the keyword(s). If there are seven letters in the keyword(s), then the array will have seven columns, and the crib would appear in these columns in the following form.

THEFAMI

However, the digraphs TL and HY do not both appear in the ciphertext, and so there are not exactly seven letters in the keyword(s). (Although neither digraph appears in the ciphertext, either one failing to appear would be enough to indicate this.) So we will assume there are exactly six letters in the keyword(s), in which case the array will have six columns, and the crib would appear in these columns in the following form.

THEFAM

3.2. CRYPTANALYSIS OF TRANSPOSITION CIPHERS

Since the digraphs TI, HL, and EY all appear in the ciphertext, it is likely that there are exactly six letters in the keyword(s) and six columns in the array. Dividing the number of letters in the ciphertext by this number of columns yields the following.

\[
\begin{align*}
9 & \div 6 \rightarrow 56 \\
\quad & \div 54 \\
\quad & \rightarrow 2
\end{align*}
\]

Thus, the first two columns of the array will contain 10 letters, and the remaining four columns will contain nine letters. So we will split the ciphertext into blocks of nine letters each, which we label as follows.

\[
\begin{align*}
AHLCCMSOA & \quad ONMSMSTS & SIAASDINR & VLFWANOE & TTIAOERI & HLEYLAECV & LW \\
1 & 2 & 3 & 4 & 5 & 6
\end{align*}
\]

Next, we will arrange these blocks as columns in an array in the only way in which the known crib and digraphs TI, HL, and EY all line up correctly. This yields the following.

\[
\begin{array}{cccccccc}
5 & 1 & 6 & 4 & 3 & 2 \\
H & V & S & O \\
T & A & L & L & I & N \\
T & H & E & F & A & M \\
I & L & Y & W & A & S \\
A & C & L & A & S & S \\
I & C & A & N & D & S \\
O & M & E & T & I & M \\
E & S & C & O & N & T \\
R & O & V & E & R & S \\
I & A
\end{array}
\]

When reading across the rows of this array from the top, the letters begin to form sensible English starting with the columns labeled 1 and 6. Thus, it is likely that these columns are the first two in the original cipher array, and would therefore be the two columns that contain 10 letters instead of nine. So we will split the ciphertext into blocks again, using 10 letters in the blocks labeled 1 and 6, and nine letters in the rest.

\[
\begin{align*}
AHLCCMSOA & \quad ONMSSMTSS & SIAASDINR & VLFWANOE & TTIAOERI & HLEYLAECV & LW \\
1 & 2 & 3 & 4 & 5 & 6
\end{align*}
\]

Arranging these blocks as columns in the same order as in the previous array, with the block labeled 5 moved from the front of the array to the end, yields the following.
Thus, the plaintext is ALL IN THE FAMILY WAS A CLASSIC AND SOMETIMES CONTROVERSIAL TV SHOW.

3.2 Exercises

1. Cryptanalyze the following ciphertexts, which were formed using simple columnar transposition ciphers.
   
   (a) AOANS BUYTE NBIEB ELNDA REVBL DDEAL
   (b) DMAIN TATLR EITVE SBXJS SHEDK AXANM INBEL X
   (c) PTIEO OGTBI NEYRA SICEY AYTRR DOISA FKFR ELGWE GITOC
       APIHO EILCT RLIOO EDIEH DNNIR TNPNE NMEIS HTONR UFITR
       EIOGN RLDLG WGES
   (d) FMGEO DFKOY AAOYL HIOIE ITUOY EFTBN UOALN RNTNH LIOAM
       HODDU WTGKD HLANO UOALN IOSOE TXSII TVGMO NTUFN TNGOX
       QNFYE IATES SYTIT OWX

2. Recall from Exercise 3 in Section 2.2 the concept of superencryption.
   
   (a) Use simple columnar transposition ciphers with four and six columns (in that order) to superencrypt LIKE AN OLD MAN TRYING TO SEND BACK SOUP IN A DELI.
   (b) Decrypt LBLPY IEAAD OURLS EKNNO TEOKC MNNDD TIADI IASG, which was superencrypted using simple columnar transposition ciphers with six and four columns (in that order).

---

10 Groucho Marx (1890–1977), quote.
11 Jeff Foxworthy, quote.
12 George Costanza, quote.
3.3 ADFGX and ADFGVX Ciphers

(c) Does superencryption by two simple columnar transposition ciphers yield more security than encryption by one simple columnar transposition cipher? In other words, if a plaintext $P$ is encrypted using a simple columnar transposition cipher, yielding $M$, and then $M$ is encrypted using another simple columnar transposition cipher, yielding $C$, would $C$ be harder in general to cryptanalyze than $M$? Explain your answer completely, and be as specific as possible.

3. The following ciphertexts were formed using keyword columnar transposition ciphers. Cryptanalyze each with the given crib.

(a) UAODI HRNNI AODSE FSQUI CWLAI HSTHO HIBYF TROTI TVRDE LRETF ENEL, with the crib CIVIL WAR
(b) IDHTE NCLEX MECEH ACLHX AHPAO OARGA NTABF HDEFB SSAKT POATL IUESR OSBRL, with the crib PEACH BASKET
(c) RSELS UEIOT EEINC HYBAG UFETF EEATL RHETE IXWRI VNSRE TFOHI SEIED EPSUE EULIN SRCEG IUUI FIODE BONHA LRSEL RTINCE TEDEB GIEEI TPHRSES ECTIN OITLAE TRLRO XITTE,\textsuperscript{13} with the crib INTELLIGENCE
(d) RSRDI HILGS LDRGL GBHTS WLOTA SIDIA SGOTA NDNHD ORSET RIOEI ATUJT GIREB EENAA OTRUY LHatC MEJDD NHORD HHIYD JMAAE ADSRT TKYNI IWEEN CTGEI DOTCH EOEAI MUYME NEIAX AITLO FEBEE GKH, with the crib AT CHRISTMAS

4. Find a copy of Herbert Yardley’s book *The American Black Chamber*, and write a summary of the description of the cryptanalysis of a German transposition cipher that can be found in Chapter 7 of it.

3.3 ADFGX and ADFGVX Ciphers

Toward the end of World War I, while most of the rest of the world was using either substitution ciphers or transposition ciphers, Germany began using a new type of cipher that combined features of both. These new ciphers, called *ADFGX* ciphers, are named for the only five letters that can appear in ciphertexts. These five letters were chosen because they sound very different from one another in Morse code, thus minimizing transmission errors. ADFGX ciphers were created by German Signals Officer Colonel Fritz Nebel, and first used by the German military in March, 1918.

ADFGX ciphers involve two steps. The first step is a substitution cipher applied to the plaintext (after spaces and punctuation have been removed)

\textsuperscript{13}Ernest Hemingway (1899–1961), quote.