

Теория Информации

В.Н. Ярмолик

Лекция 2

2015

Encryption Algorithms

Transposition Cipher

A lot of codes are simple in design. Just by changing the order of words, letters, or the way read them can turn the message into secret code. The simplest examples of the Transposition Ciphers are:

Lumping Words (Format)

Get rid of spaces and returns to lump words together. Use upper case to make the code harder to read and decode.

Ciphertext: THISISHARDCODEFORMANYPEOPLE

Message: THIS IS HARD CODE FOR MANY PEOPLE

Character Bloks

Block letter of a message by 2,3 or more characters.

Ciphertext: TH IS IS HA RD CO DE FO RM AN YP EO PL E

Message: THIS IS HARD CODE FOR MANY PEOPLE

Backwards English

Writing words, sentences, or entire message backwards can be very confusing!

Ciphertext: SIHT SI DRAH EDOC ROF YNAM ELPOEP

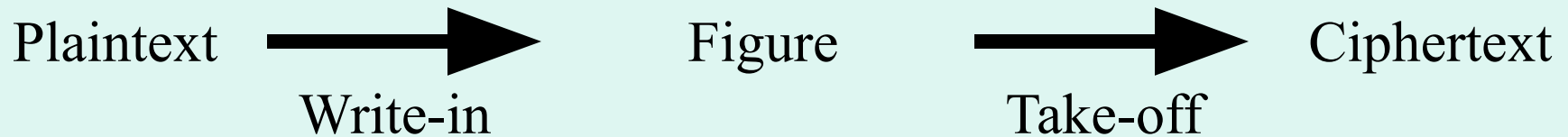
Message: THIS IS HARD CODE FOR MANY PEOPLE

Reading SIHT backwards yields the answer THIS.

Encryption Algorithms

Transposition Cipher

Transposition cipher rearrange characters according to some scheme. This rearrangement was classically done with the aid of some type of geometric figure. Enciphering procedure consists of two steps as shown next:



First, the plaintext was written into the figure according to some “Write-in” path, then the ciphertext was taken off the figure according to some “Take-off” path.

Example 2.1. Suppose that the plaintext CRYPTOGRAPHY is written into 3 rows by 4 columns matrix by rows as follows:

<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>
C	R	Y	P
T	O	G	R
A	P	H	Y

If the columns are taken off in the order 3-1-4-2, the resulting ciphertext is YGHCTAPRYROP.

Encryption Algorithms

Transposition Cipher

Many transposition ciphers permute the characters of the plaintext with a **fixed period** d . The key for the cipher is given by the pair $K=(d,f)$, where d is the number of characters within the block and f is function of permutation. Thus, a plaintext message

$$M=m_1, \dots, m_d m_{d+1}, \dots, m_{2d}, \dots$$

is enciphered as

$$E_K(M)=m_{f(1)}, \dots, m_{f(d)} m_{f(d+1)}, \dots, m_{f(2d)}, \dots$$

Decipherment uses the inverse permutation.

Example. Suppose that $d=4$ and the function of permutation f is

i	1	2	3	4
$f(i)$	3	1	4	2

thus, the plaintext is divide into the blocks with 4 bits each, then for every block first plaintext character is moved to the second position, the second character to the fourth position and so forth.

M=CRYP TOGR APHY

Ek(M)=YCPR GTRO HAYP

Encryption Algorithms

Transposition Cipher

Like columnar transposition, periodic permutation cipher can be viewed as transpositions of the columns of a matrix in which the plaintext is written in by rows.

Example. Suppose that $d=12$ and the geometric figure is matrix 4 column by 3 rows and function of columns permutation f has a form

$$\begin{array}{c} i \\ f(i) \end{array} \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{array}$$

M = HERE IS A SECRET MESSAGE ENCIPHERED BY
TRANSPOSITION \Rightarrow

H	E	R	E
I	S	A	S
E	C	R	E

T	M	E	S
S	A	G	E
E	N	C	I

P	H	E	R
E	D	B	Y
T	R	A	N

S	P	O	S
I	T	I	O
N			

$E_k(M)$ =RAR HIE ESE ESC EGC TSE SEI MAN EBA PET RYN
HDR OI SIN SO PT

Encryption Algorithms

Transposition Cipher

Using a key word or phrase, such as, for example CONVENIENCE, assign a number to each letter in the word using this rule: the numbers are assigned starting with 1, and they are assigned first by *alphabetical order*, and second, where the same letter appears twice, by *position* in the word.

Example. Thus: the plaintext message M=HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION

<i>C</i>	<i>O</i>	<i>N</i>	<i>V</i>	<i>E</i>	<i>N</i>	<i>I</i>	<i>E</i>	<i>N</i>	<i>C</i>	<i>E</i>
1	10	7	11	3	8	6	4	9	2	5
H	E	R	E	I	S	A	S	E	C	R
E	T	M	E	S	S	A	G	E	E	N
C	I	P	H	E	R	E	D	B	Y	T
R	A	N	S	P	O	S	I	T	I	O
N										

Produces next ciphertext C=HECRN CEYI ISEP SGDI RNT0
AAES RMPN SSRO EEBT ETIA EEHS

Encryption Algorithms

Transposition Cipher

Example. Another method of transposition is a Variant of column transposition that produces a different cipher:

<i>C</i>	<i>O</i>	<i>N</i>	<i>V</i>	<i>E</i>	<i>N</i>	<i>I</i>	<i>E</i>	<i>N</i>	<i>C</i>	<i>E</i>
1	10	7	11	3	8	6	4	9	2	5
H										
E	R	E	I	S	A	S	E	C	R	
E	T	M	E	S						
S	A	G	E	E	N	C	I			
P	H	E	R	E	D	B	Y	T	R	A
N	S	P	O	S	I	T				
I	O	N								

C=HEESPNI RR SSEES EIY A SCBT EMGEPN ANDI CT
RTAHSO IEERO

This method has the advantage of dividing the text being transposed in a more irregular fashion than ordinary columnar transposition.

Encryption Algorithms

Transposition Cipher

Another interesting form of transposition is the "turning grille", used by Germany during the First World War.

A square grille, divided into a grid of squares, one-quarter of which are punched with holes, is placed over a sheet of paper. The message is written on the paper through the holes, and then the grille is rotated by 90 degrees, and then the message continues to be written, as the grille is turned through all four possible positions.

The trick to designing such a grille is to divide the grille into quarters, numbering the squares in each quarter so that as the grille is rotated, corresponding squares have the same number. Then, choose one square with each number for punching.

Example. Example of a turning grille and its use:

Grid
numbering:

1	2	3	4	1
4	5	6	5	2
3	6	7	6	3
2	5	6	5	4
1	4	3	2	1

Layout:

<u>1</u>	2	<u>3</u>	4	1
4	5	6	5	<u>2</u>
3	6	<u>7</u>	<u>6</u>	3
2	<u>5</u>	6	5	4
1	<u>4</u>	3	2	1

Encryption Algorithms

Transposition Cipher

Example. Example of a turning grille and its use for message:
M=HERE IS A SECRET MESSAGE WRITE

First Round

<u>1</u>	2	<u>3</u>	4	1
4	5	6	5	<u>2</u>
3	6	<u>7</u>	<u>6</u>	3
2	<u>5</u>	6	5	4
1	<u>4</u>	3	2	1

H		E		
				R
		E	I	
	S			
	A			

Second Round

1	2	3	4	<u>1</u>
<u>4</u>	<u>5</u>	6	5	2
3	6	*	6	<u>3</u>
2	5	<u>6</u>	5	4
1	4	3	<u>2</u>	1

H		E		S
E	C			R
		E	I	R
	S	E		
	A		T	

Encryption Algorithms

Transposition Cipher

Example. M=HERE IS A SECRET MESSAGE WRITE

Third Round

1	2	3	<u>4</u>	1
4	5	6	<u>5</u>	2
3	<u>6</u>	*	6	3
<u>2</u>	5	6	5	4
1	4	<u>3</u>	2	<u>1</u>

H		E	M	S
E	C		E	R
	S	E	I	R
S	S	E		
	A	A	T	G

Fourth Round

1	<u>2</u>	3	4	1
4	5	<u>6</u>	5	2
<u>3</u>	6	*	6	3
2	5	6	<u>5</u>	<u>4</u>
<u>1</u>	4	3	2	1

H	E	E	M	S
E	C	W	E	R
R	S	E	I	R
S	S	E	I	T
E	A	A	T	G

C=HEEMS ECWER RSEIR SSEIR SSEIT EAATG

Encryption Algorithms

Simple Substitution Ciphers

Simple substitution cipher replace each character of plaintext with a corresponding character of ciphertext; a single one-to-one mapping from plaintext to ciphertext characters is used.

A *simple substitution* cipher replace each character of an ordered plaintext alphabet, denoted as A , with the corresponding character of an ordered cipher alphabet, denoted of C . Suppose A is an n -character alphabet $\{a_0, a_1, \dots, a_n\}$, then C is an n -character alphabet $\{f(a_0), f(a_1), \dots, f(a_n)\}$, where $f: A \rightarrow C$ is a one-to-one mapping of each character of A to the corresponding character of C . The key K to the cipher is given by C or, equivalently, by the function f .

To encipher, a plaintext message $M = m_1 m_2 \dots$ is written as the ciphertext message $E_K(M) = f(m_1) f(m_2) \dots$

Example 2.7. Suppose that f maps English alphabet $A = \{a_0, a_1, \dots, a_n\}$ into the cipher alphabet C as:

$A: ABCDEFGHIJKLMNOPQRSTUVWXYZ$

$C: YARMOLIKBCDEFGHJNPQRSTUUVWXZ$

then the plaintext CRYPTOGRAPHY is enciphered as:

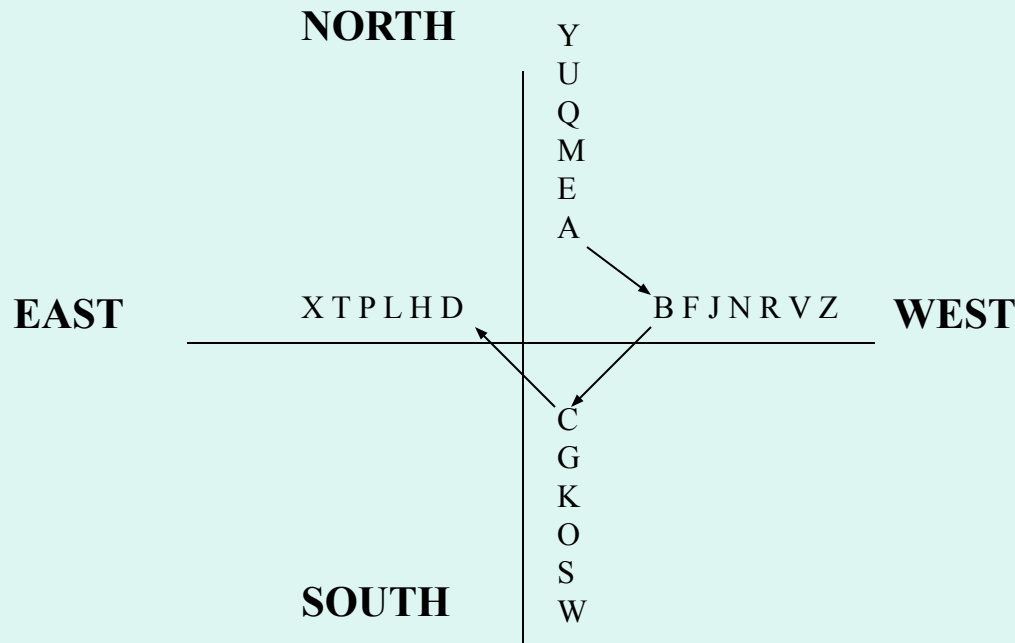
$E_K(M) = RPXJSHIPYJKX$

Encryption Algorithms

Simple Substitution Ciphers

Compass Cipher-A Method for Alphabet Substitution

There are lots of ways to create a compass cipher key.



The arrows show the direction used to fill in the compass lines.

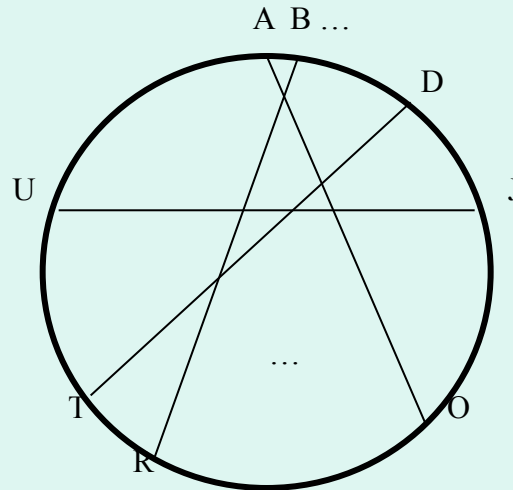
Once you have all the letters written into your compass write out the letters, from outside in and then combine all of the letters into a long line. **Compass Key:** YUQMEAZVRNJFBWSOKGCXTPLHD

Encryption Algorithms

Simple Substitution Ciphers

Letter Spokes Cipher Clock

It's another way of making up a random alphabet substitution wheel. The letter spokes cipher clock, developed by Angie Wimer, resemble the spokes of a wheel. According to his idea you have to simply take each letter in the wheel and line it up with another letter somewhere else in the wheel.



See if you can decipher the encrypted message “ROT” by making the use of the Letter Spokes clock below the answer is “BAD”.

Encryption Algorithms

Simple Substitution Ciphers

Alphabet & Word Correlated Ciphers.

Sometimes keywords are used to help encipher a message. By writing out a sentence(s) that contains all the letters of the alphabet you can correlate plain alphabet letters within a word found in the keyword phrase to make the cipherring a bit more difficult to decipher.

The keyword phrase “*The quick brown fox jumps over the lazy dog*” contains all the letters of the alphabet. Even though some letters appear more than once it shall serve as a keyword phrase because it still contains all the letters of the alphabet. To get started, write out your keyword phrase and number each word:

THE	QUICK	BROWN	FOX	JUMPS	OVER	THE	LAZY	DOG
1	2	3	4	5	6	7	8	9

Plaintext: *Johnson is a spy*

Ciphertext:

J	O	H	N	S	O	N	I	S	...
51	33	12	35	55	33	35	23	55	

Encryption Algorithms

Simple Substitution Ciphers

Cipher based on *shifted alphabet* (“direct standard alphabets”) shift the letters of the alphabet to the right by k positions, modulo the size of the alphabet according to the equation

$$f(a)=(a+k) \bmod n,$$

where n is the size of the alphabet and a denotes letter and its position in A .

For the English alphabet

0-A, 1-B, 2-C, 3-D, 4-E, 5-F, 6-G, 7-H, 8-I, 9-J, 10-K, 11-L, 12-M, 13-N, 14-O, 15-P, 16-Q, 17-R, 18-S, 19-T, 20-U, 21-V, 22-W, 23-X, 24-Y, 25-Z.

Under the Caesar cipher, our plaintext CRYPTOGRAPHY is enciphered by

$$f(a)=(a+3) \bmod 26,$$

then $E_K(M)=FUBSWRJUDSKB$.

There are more complex transformation of the plaintext alphabet. Ciphers based on multiplications (“decimations”) are shown below

$$f(a)=ka \bmod n,$$

where k and n are relatively prime so that the letter of the alphabet produce a complete set of residues. For the plaintext CRYPTOGRAPHY and $k=3$ we will get $f(a)=3a \bmod 26$, and $E_K(M)=GZUTFQSZATVU$.

Encryption Algorithms

Simple Substitution Ciphers

Addition (shifting) and multiplication can be combined to give an *affine transformation*

$$f(a) = (ak_1 + k_0) \pmod n,$$

where k_1 and n are relatively prime.

Higher-order transformations are obtained with *polynomial transformations* of degree t :

$$f(a) = (a^t k_t + a^{t-1} k_{t-1} + \dots + ak_1 + k_0) \pmod n,$$

Some substitution cipher use nonstandard ciphertext alphabet. The *Churchyard cipher* shown below was engraved on a tombstone in Trinity Churchyard, New York, in 1794.

A*	B*	C*	K**	L**	M**	T	U	V		
D*	E*	F*	N**	O**	P**	W	X	Y		
G*	H*	I-J*	Q**	R**	S**	Z				

What is the plaintext corresponding to the next ciphertext?

	**	*	**	*	**	*	*	**	
	*	*	*	*					

Encryption Algorithms

Single-Letter Frequency Analysis

Simple substitution cipher are generally easy to break in a ciphertext-only attack using single-letter frequency distributions. The letters of English alphabet can be divided into subsets of *high*, *medium*, *low*, and *rare* frequency as shown below:

high: E T A O N I R S H

medium: D L U C M

low: P F Y W G B V

rare: J K Q X Z

By comparing the letter frequencies in a given ciphertext with the expected frequencies, a cryptanalyst can match the ciphertext letter with the plaintext letters. Diagram and trigram distributions are also helpful.

Ciphers based on shifted alphabets are usually easy to solve, because each ciphertext letter is a constant distance from its corresponding plaintext letter. Cipher based on affine transformations

$$f(a) = (ak_1 + k_0) \pmod{n},$$

are somewhat trickier. To determine the values of k_1 and k_0 the system of two linear equations have to be solved. So, for the two pairs of $(f(a), a)$: $(10, 4)$, $(19, 9)$ we have two equations

$$10 = (4k_1 + k_0) \pmod{26},$$

$$19 = (9k_1 + k_0) \pmod{26},$$

then subtracting (1) from (2) we get $9 = 5k_1 \pmod{26}$. The last equation can be solved to determine $k_1 = 7$. Substituting in (1) value of k_1 gives $(28 + k_0) \pmod{26} = 10$.

Encryption Algorithms

Homophonic Substitution cipher

A homophonic substitution cipher maps each character a of the plaintext alphabet into a set of ciphertext elements $f(a)$ called homophones. A plaintext message $M=m_1m_2\dots$ is enciphered as $C=c_1c_2\dots$, where each c_i is picked at random from the set of homophones $f(m_i)$.

Example. Let the English letters are enciphered as integers between 00 and 99, where the number of integers assigned to a letter is proportional to the relative frequency of the letter, and no integer is assigned to more than one letter. A possible assignment of integers to the letters in the message CRYPTOGRAPHY are show below (integer assignment for the remaining letters of the alphabet are not given)

letter	Homophones
A	23, 25, 97, 95, 81, 33, 12, 11
C	44, 77, 34, 51
G	87, 41
H	59, 90, 00, 26
O	66, 87, 02, 15, 22, 09, 83, 54
P	04, 58
R	38, 07, 94, 30, 56, 67
T	55, 71, 72, 80, 01, 12, 29, 50, 68
Y	88

One possible encipherment of the message is:

$C = 77\ 07\ 88\ 58\ 72\ 54\ 41\ 30\ 97\ 04\ 00\ 88$

Encryption Algorithms

Homophonic Substitution cipher

1. Single letter frequency distributions.

A	0.0804	H	0.0549	O	0.0760	V	0.0099
B	0.0154	I	0.0726	P	0.0200	W	0.0192
C	0.0306	J	0.0016	Q	0.0011	X	0.0019
D	0.0399	K	0.0067	R	0.0612	Y	0.0173
E	0.1251	L	0.0414	S	0.0654	Z	0.0009
F	0.0230	M	0.0253	T	0.0925		
G	0.0196	N	0.0709	U	0.0271		

Encryption Algorithms

Beale Ciphers

The *Beale cipher* is an example of a homophonic substitution cipher. The key is the Declaration of Independence. The words of the Declaration are numbered consecutively as shown below

Declaration of Independence (first 100 words)

01 When, in the course of human events, it becomes necessary
11 for one people to dissolve the political bands which have
21 connected them with another, and to assume among the Powers
31 of the earth the separate and equal station to which
41 the Laws of Nature and of Nature's God entitle them,
51 a decent respect to the opinions of mankind requires that
61 they should declare the causes which impel them to the
71 separation. We hold these truths to be self-evident; that
81 all men are created equal, that they are endowed by
91 their Creator with certain unalienable rights; that among

Beale enciphered each letter in the plaintext message by substituting the number of some word which started with that letter. The letter W, for example, was enciphered with the number 1, 19, 40, 66, 72, As an example let consider the word PLAIN. The result of enciphering are shown below:

$$\begin{array}{rcccccc} M = & P & L & A & I & N \\ C = & 13 & 42 & 81 & 08 & 44 \end{array}$$

Encryption Algorithms

Polygram Substitution Cipher

All of the preceding substitution cipher encipher a single letter of plaintext at a time. By enciphering larger blocks of letters, *polygram substitution ciphers* make cryptanalysis harder by destroying the significance of single-letter frequencies.

The Playfair cipher is a diagram substitution cipher named after the English scientist Lyon Playfair; the cipher was actually invented in 1854 by Playfair's friend, Charles Wheatstone, and was used the British during World War I. The key of this cipher is given by a 5 by 5 matrix of 25 letters (J was not used), such as the one shown below.

Key for Playfair cipher

Y	A	R	M	O
L	I	K	B	C
D	E	F	G	H
V	N	P	Q	S
T	U	W	X	Z

Playfair cipher enciphering rule

Each pair of plaintext letters $m_1 m_2$ is enciphering according to the following rules:

1. If m_1 and m_2 are in the same row, then c_1 and c_2 are the two characters to the right of m_1 and m_2 , respectively, where the first column is considered to be to the right of the last column.

2. If m_1 and m_2 are in the same column, then c_1 and c_2 are the two characters below m_1 and m_2 ,

respectively, where the first row is considered to be below last row.

3. If m_1 and m_2 are in different rows and columns, then c_1 and c_2 are the other two corner of the rectangle having m_1 and m_2 , as corners, where c_1 is m_1 's row and c_2 is in m_2 's row.

4. If $m_1 = m_2$, a null letter (e.g., X) is inserted into the plaintext between m_1 and m_2 to eliminate the double.

5. If the plaintext has an odd number of characters, a null letter is appended to the end of the plaintext.

2. Encryption Algorithms

2.6. Polygram Substitution Cipher

Playfair has inspired some related *bigraphic* ciphers that, on the one hand, improve security by involving multiple, unrelated alphabets, but on the other hand, are simpler in that they use fewer rules than Playfair.

In the Four-Square cipher, two squares are used to find the two plaintext letters, and two others are used to find the two ciphertext letters:

M	W	X	Y	M	E	P	T	O	L
R	J	E	K	I	C	V	I	Y	Z
U	V	<u>H</u>	P	S	R	M	A	G	B
A	L	B	Z	N	F	W	J	H	S
G	C	O	F	T	U	N	D	X	K
<hr/>					<hr/>				
J	T	B	U	E	V	I	M	A	G
Z	H	N	D	X	S	<u>W</u>	P	O	H
L	A	F	R	G	U	T	Z	K	E
P	M	I	Y	C	N	R	D	X	Y
V	S	K	W	O	B	J	L	C	F

Thus, the diagram $m_1m_2=HW$ becomes $c_1c_2=MN$.

Encryption Algorithms *Bifid Cipher*

The first of the three rules for Playfair encipherment changes one two-letter group, or digraph, to another by exchanging column co-ordinates. This suggests using row and column co-ordinates in a more general fashion. Let's take the 5 by 5 square above, but number the rows and the columns, like this:

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

Then, another method of encipherment would be as follows: Divide a message into groups of letters of a fixed length, say five letters, and write the row and then the column co-ordinate of each letter beneath it, like this:

T	H	I	S	I	S	M	Y	S	E	C	R	E	T	M
<hr/>					<hr/>					<hr/>				
1	1	5	5	5	5	2	4	5	3	4	1	3	1	2
1	4	5	3	5	3	3	4	3	5	1	5	5	1	3

E	S	S	A	G	E
<hr/>					<hr/>
3	5	5	4	4	3
5	3	3	5	2	5

and then, going across within each group, read the numbers in order, and turn them, in pairs, into letters: that is, read 11555 14535 52453 33435... and turn them into the letters corresponding to 11, 55, 51, 45, 35, 52, and so on.

11	55	51	45	35	52	45	33	34	35	41	31	21	55	13	35	54	45	33	52	35
T	I	F	A	E	B	A	O	J	E	C	N	L	I	V	E	D	A	O	B	E

Encryption Algorithms

Trifid Cipher

This is the *Bifid cipher* of Delastelle, and the general principle of this form of cipher is called *seriation*. This is one of the most secure pencil-and-paper ciphers that is still used by hobbyists as a puzzle. It isn't hard to make this kind of cipher just a little bit more complicated, and thereby obtain one that is genuinely secure. It belongs to the class of cipher methods known as *fractionation*, where letters are divided into smaller pieces, or "fractions". Just as two symbols from 1 to 5 give 25 letters, three symbols from 1 to 3 give 27 letters; and five binary bits provide a 32-character alphabet.

The *Trifid*, also due to Delastelle, is the analogous cipher using a 27-letter alphabet represented by three symbols from 1 to 3:

W 111 N 211 C 311 A 112 E 212 X 312 K 113 Q 213 I 313
M 121 O 221 T 321 & 122 V 222 J 322 B 123 R 223 F 323
Z 131 L 231 U 331 Y 132 P 232 G 332 H 133 S 233 D 333

to encipher a message by seriation like this:

T	H	I	S	I	S	M		Y	S	E	C	R	E	T		M	E	S	S	A	G	E
3	1	3	2	3	2	1		1	2	2	3	2	2	3		1	2	2	2	1	3	2
2	3	1	3	1	3	2		3	3	1	1	2	1	2		2	1	3	3	1	3	1
1	3	3	3	3	3	1		2	3	2	1	3	2	1		1	2	3	3	2	2	2

which again is read off horizontally after being written in vertically, yielding a cipher message like this: 313-I, 232-P, 123-B, 131-Z, 321-T, 333-D, 331-U, 122-&, 322-J, 333-D, 112-A 122-&, 321-T, 321-T, 122-&, 213-Q, 221-O, 331-U, 311-C, 233-S, 222-V.

Encryption Algorithms

The Straddling Checkerboard

Some ciphers actually used by Soviet spies used a square like this:

	9	8	2	7	0	1	6	4	3	5
	A	T		O	N	E		S	I	R
2	B	C	D	F	G	H	J	K	L	M
6	P	Q	U	V	W	X	Y	Z	.	/

Eight of the most common letters are translated to a single digit. The two digits not used in this way begin two-digit combinations that stand for the remaining letters. This is an example of a *variable length code* with the *prefix property*. When it is possible to tell, from the digits one has already seen of a symbol, whether or not one needs to include the next digit in the symbol, then spaces between the digits of a symbol are not needed, and this is what is known as the prefix property.

Of course, the second digit of a two-digit combination could also have stood, by itself, for another letter; but because when you start from the beginning and move forwards, there is no chance of confusion, this is a workable and usable system. Thus, the message SENDMONEY would become 4 1 0 22 25 7 0 1 66, or, rather, 41022 25701 66 because spaces to show where the letters begin are not needed; the first digit representing a letter determines if its substitute is one or two digits long. More complicated codes that work this way, using only the two binary digits 0 and 1, are used as a form of data compression. The most famous variable-length prefix-property binary codes are the Huffman codes;