2. Encryption Algorithms

2.1. 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 DRAH EDOC ROF YNAM ELPOEP
Message: THIS IS HARD CODE FOR MANY PEOPLE

Reading SIHT backwards yields the answer THIS.

2. Encryption Algorithms

2.1. 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. The key consisted of the figure together with the write-in and take-off paths.

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

1	2	3	4
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.

For decipherment the inverse procedure have to be used.

2. Encryption Algorithms

2.1. 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

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

is enciphered as

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

Decipherment uses the inverse permutation.

Example 2.2. Suppose that $d=4$ and the function of permutation *f* has a form

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

The preceding ciphertext is broken into groups of four letters only for clarity; the actual ciphertext would be transmitted as a continuous stream of characters to hide the period.

2. Encryption Algorithms

2.1. 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 2.3. Suppose that *d=12* and the geometric figure is matrix 4 column by 3 rows and function of columns permutation *f* has a form

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

thus, the plaintext is divide into the blocks with 12 bits each, then every block is written as a matrix 3×4, then third column of matrix is written as a row to the first position of ciphertext, the first column is written to the second position an and so forth.

M= HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION⇒

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			

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

2. Encryption Algorithms

2.1. Transposition Cipher

The best-known modification of transpositions method is simple columnar transposition, works like this:

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 2.4. Then, write in the message under the keyword, writing across - but take out columns, in numerical order, reading down. Thus: the plaintext message M=HERE IS A SECRET MESSAGE ENCIPHERED BY TRANSPOSITION

C	***O***	***N***	***V***	***E***	***N***	***I***	***E***	***N***	***C***	***E***
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 RNTO ASAES RMPN SSRO EEBT ETIA EEHS

2. Encryption Algorithms

2.1. Transposition Cipher

Example 2.5. Another method of transposition is a Variant of column transposition that produces a different cipher:

C	***O***	***N***	***V***	***E***	***N***	***I***	***E***	***N***	***C***	***E***
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								

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

Here, the first row is filled in only up to the column with the key number 1; the second row is filled in only up to the column with the key number 2; and so on. Of course, one still stops when one runs out of plaintext, so the eighth row stops short of the key number 8 in this example. This method has the advantage of dividing the text being transposed in a more irregular fashion than ordinary columnar transposition.

2. Encryption Algorithms

2.1. 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.

In World War I, the Germans used turning grilles with an odd number of holes on each side as well as with an even number; to do this, they marked the square in the center, which was always punched, with a black border to indicate it was only to be used in one of the grille's positions.

Example 2.6. Example of a turning grille and its use:

Grid numbering:

1	2	3	4	1
4	5	6	5	2
3	6	9	6	3
2	5	6	5	4
1	4	3	2	1

Layout:

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

2. Encryption Algorithms

2.1. Transposition Cipher

Example 2.6. Example of a turning grille and its use for message: M=HERE IS A SECRET MESSAGE WRITE

First Round

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

H		E		
				R
		E	I	
	S			
	A			

Second Round

1	2	3	4	***1***
4	***5***	6	5	*2*
3	6	*	6	***3***
2	5	***6***	5	4
1	4	3	***2***	1

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

2. Encryption Algorithms

2.1. Transposition Cipher

Example 2.6. M=HERE IS A SECRET MESSAGE WRITE

Third Round

1	2	3	***4***	1
4	5	6	***5***	2
3	***6***	*	6	3
2	5	6	5	4
1	4	***3***	2	***1***

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

Fourth Round

1	***2***	3	4	1
4	5	***6***	5	2
3	6	*	6	3
2	5	6	***5***	***4***
1	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

Ciphertext is C=HEEMS ECWER RSEIR SSEIR SSEIT EAATG

2. Encryption Algorithms

2.2. 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 to encipher an entire message.

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* ((typically *C* is a simple rearrangement of the lexicographic order of the characters in *A*). Suppose *A* is an *n*-character alphabet $\{a_0,a_1,...,a_n\}$, then *C* is an *n*-character alphabet $\{f(a_0),f(a_1),...,f(a_n)\}$, where $f:A-->C$ is a one-to-one mapping of each character of *A* to the corresponding character of *C*. The key to the cipher is given by *C* or, equivalently, by the function *f*.

To encipher, a plaintext message $M=m_1m_2...$ is written as the ciphertext message $E_K(M)=f(m_1)f(m_2)...$

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

A:*ABCDEFGHIJKLMNOPQRSTUVWXYZ*

C:*YARMOLIKBCDEFGHJNPQSTUVWXZ*

then the plaintext CRYPTOGRAPHY is enciphered as: $E_K(M)=RPXJSHIPYJKX$.

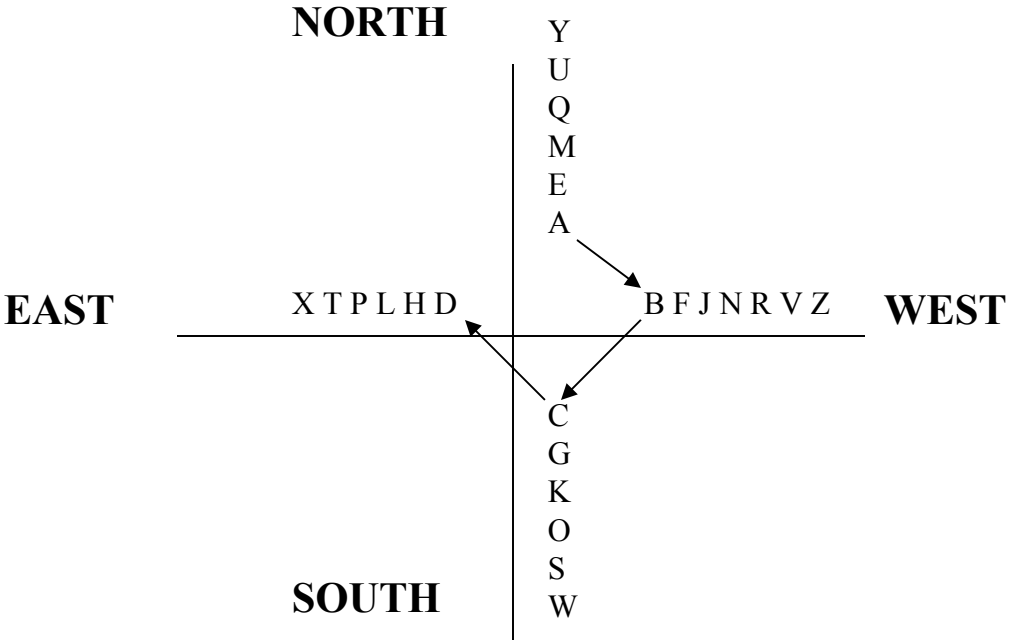
The preceding example uses a keyword mixed alphabet: the cipher alphabet is constructed by first listing the letter of a keyword (in this case YARMOLIK), omitted duplicates, and then listing the remaining letters of the alphabet in order.

2. Encryption Algorithms

2.2. Simple Substitution Ciphers

Compass Cipher-A Method for Alphabet Substitution

There are lots of ways to create a compass cipher key. One way as shown below, is to make a cross in the centre of your paper and write out the letters of the alphabet along each line, spiralling outwards.



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. Finally, write out the plain alphabet below it to come up with an alphabet substitution cipher!

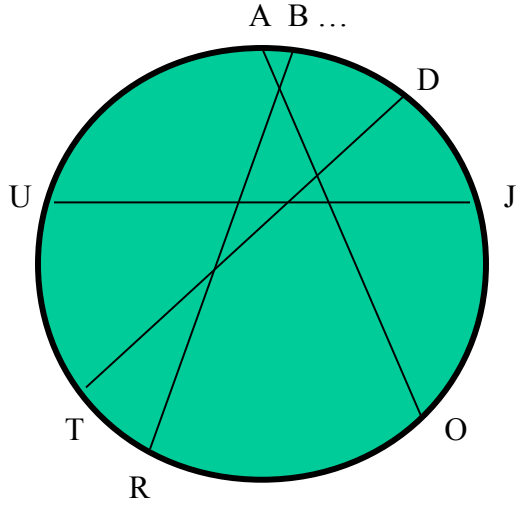
Copass Key: YUQMEAZVRNJFBWSOKGCXTPLHD

2. Encryption Algorithms

2.2. 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".

2. Encryption Algorithms

2.2. 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.

2. Encryption Algorithms

2.2. 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 phase 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	

2. Encryption Algorithms

2.2. Simple Substitution Ciphers

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

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

where k_1 and n are relatively prime.

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

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

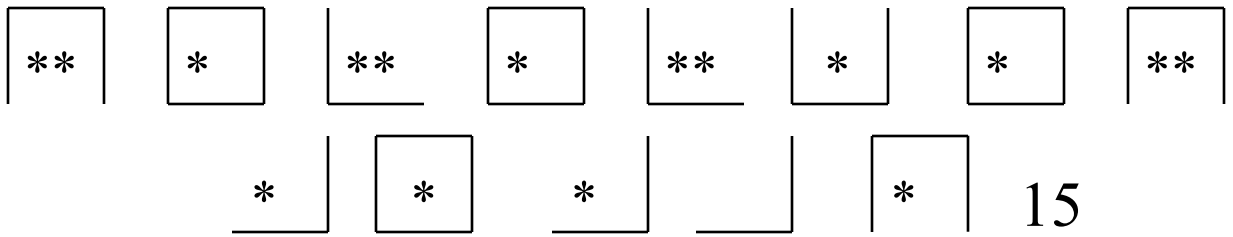
Some substitution cipher use nonstandard ciphertext alphabet. The Churchyard cipher shown below was engraved on a tombstone in Trinity Churchyard, New York, in 1794.

A*	B*	C*
D*	E*	F*
G*	H*	I-J*

K**	L**	M**
N**	O**	P**
Q**	R**	S**

T	U	V
W	X	Y
Z		

What is the plaintext corresponding to the next ciphertext?



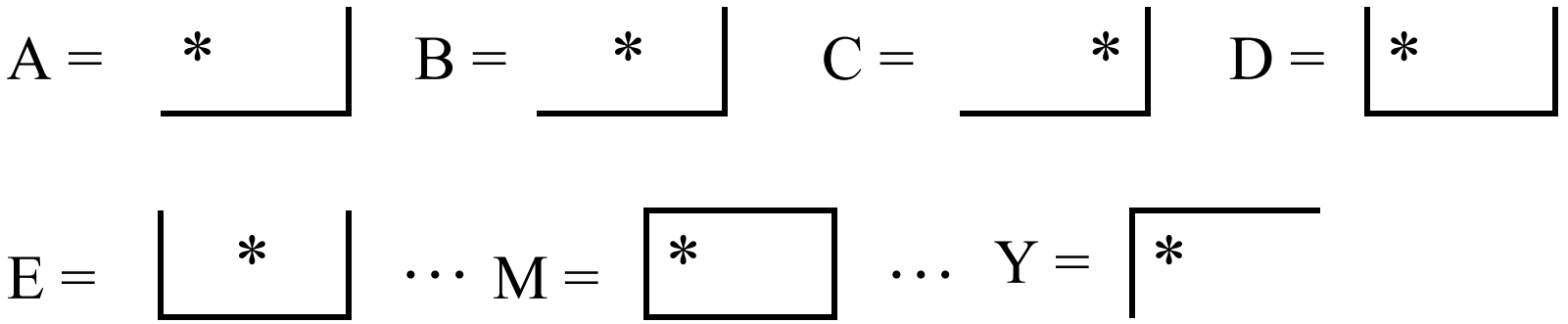
2. Encryption Algorithms

2.2. Simple Substitution Ciphers

Pig Pen Cipher

By creating a matrix of the alphabet within a tic-tac-toe box a pig pen cipher can be created. This method of enciphering was developed by Baptista del Porta in the 1699's. Each symbol is created by referencing a letter position with the lines:

ABC	DEF	GHI
JKL	MNO	PQR
STU	VWX	YZ



2. Encryption Algorithms
2.3. 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 cryptoanalyst can match the ciphertext letter with the plaintext letters. Digram 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

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

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

$$10=(4k_1+k_0) \mod 26,$$

$$19=(9k_1+k_0) \mod 26,$$

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

2. Encryption Algorithms
2.4. 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 $M=m_1m_2...$ is enciphered as $C=c_1c_2...,$ where each c_i is picked at random from the set of homophones $f(m_i)$.

Example 2.8. 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, 88, 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 massage is:

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

2. Encryption Algorithms
2.5. 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:

M =	P	L	A	I	N
C =	13	42	81	08	44

2. Encryption Algorithms

2.6. 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 cryptoanalysis 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, Charls 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_1m_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.

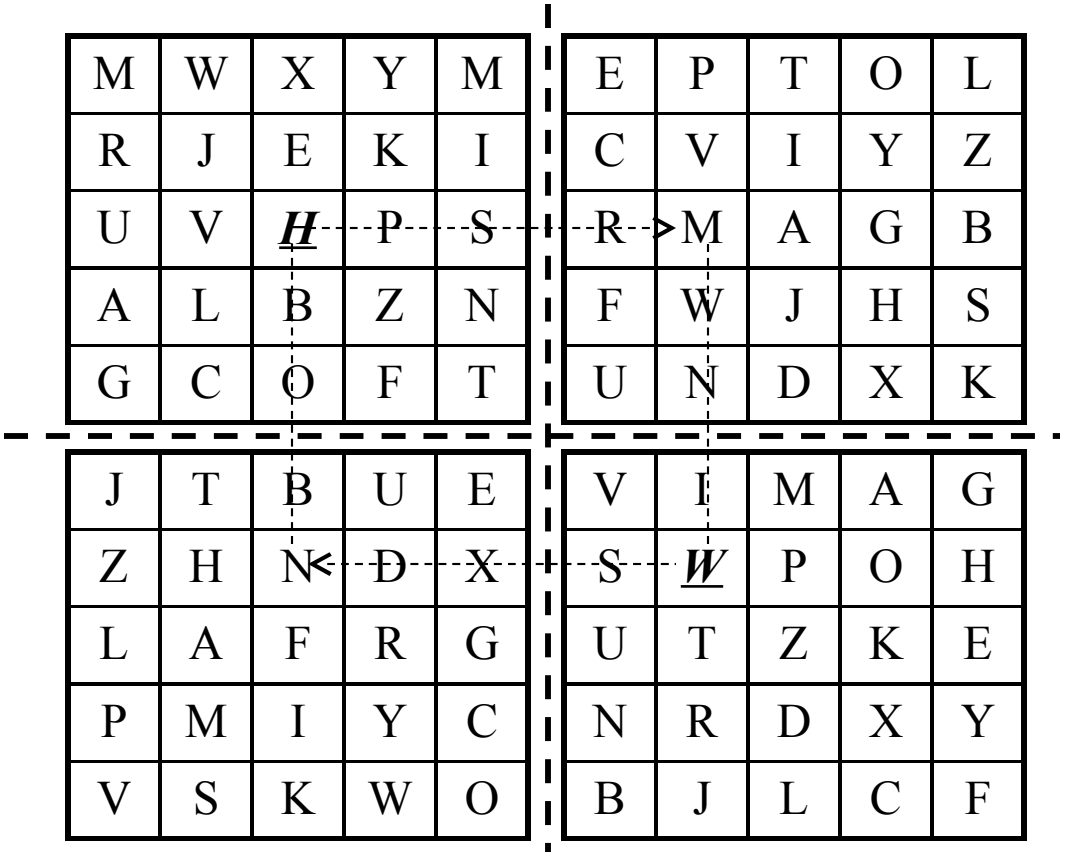
5. If the plaintext has an odd number of characters, a null letter is appended to the end of the plaintext.

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:



Thus, the diagram m_1m_2=***HW*** becomes c_1c_2= ***MN***

2. Encryption Algorithms
2.7. 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
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
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

2. Encryption Algorithms

2.7. 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.

2. Encryption Algorithms

2.8. 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	.	/

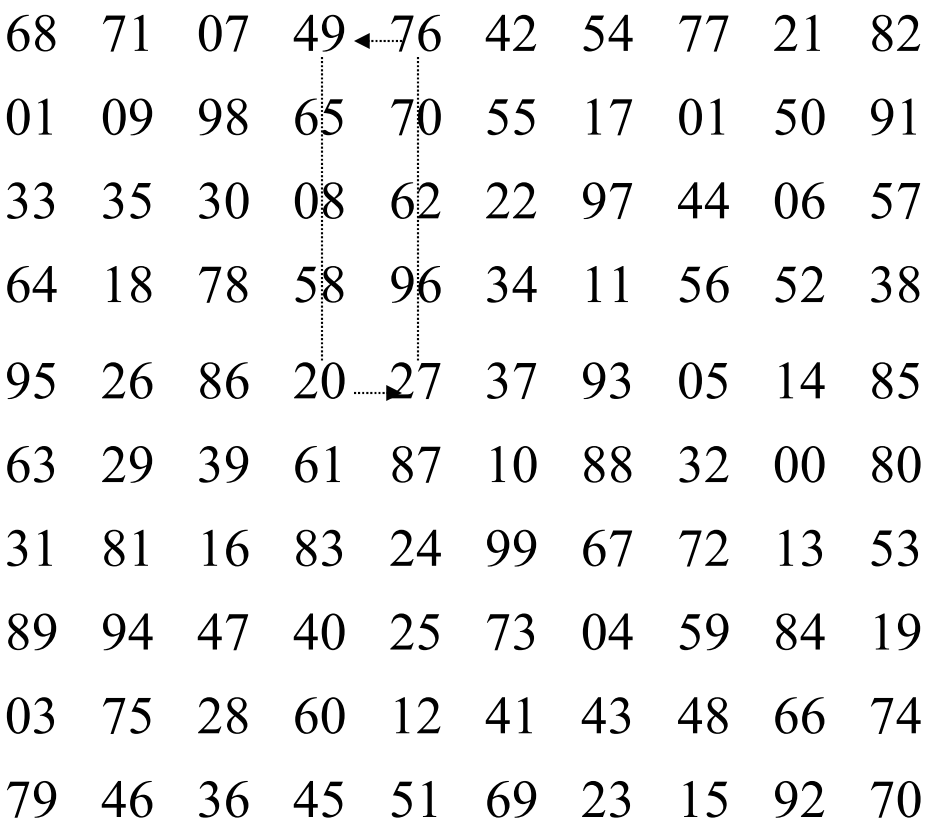
Eight of the most common letters are translated to a single digit. The two digits not used in this way begin two-digit combinations that stand for the remaining letters. This is an example of a ***variable length code*** with the ***prefix property***. When it is possible to tell, from the digits one 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;

2. Encryption Algorithms

2.9. Giant Playfair

Another technique I once described involved first using the straddling checkerboard to encipher a message as digits, and then to use Playfair to encipher it. But instead of using the Playfair technique over a 5 by 5 square of letters, one uses a 10 by 10 square containing digit pairs, like the following



68	71	07	49	76	42	54	77	21	82
01	09	98	65	70	55	17	01	50	91
33	35	30	08	62	22	97	44	06	57
64	18	78	58	96	34	11	56	52	38
95	26	86	20	27	37	93	05	14	85
63	29	39	61	87	10	88	32	00	80
31	81	16	83	24	99	67	72	13	53
89	94	47	40	25	73	04	59	84	19
03	75	28	60	12	41	43	48	66	74
79	46	36	45	51	69	23	15	92	70

Thus, the four digits 2076 would encipher to 2749 with this square.

2. Encryption Algorithms

2.10. The VIC Cipher

The VIC cipher is an intricate cipher issued by the Soviet Union to at least one of its spies. It is of interest because it seems highly secure, despite being a pencil-and-paper cipher. It was the cipher in which a message was written which was found on a piece of microfilm inside a hollowed-out nickel by a newspaper boy in 1953.

The VIC cipher, which we will demonstrate here adapted to the sending of English-language messages, begins with an involved procedure to produce ten pseudorandom digits. The agent must have memorized six digits (which were in the form of a date), and the first 20 letters of a key phrase (which was the beginning of a popular song) and must think of five random digits for use as a message indicator.

Let the date be July 4, 1776, to give the digits 741776. (Actually, the Russians used their customary form of dates, with the month second.) And let the random indicator group be 77651.

The first step is to perform digit by digit subtraction (without carries) of the first five digits of the date from the indicator group:

```
  77651
(-)
  74177
  -------
  03584
```

The second step is to take the 20-letter keyphrase, and turn it into 20 digits by dividing it into two halves, and within each half, assigning 1 to the letter earliest in the alphabet, and so on, treating 0 as the last number, and assigning digits in order to identical letters. Thus, if our keyphrase is "I dream of Jeannie with t", that step proceeds: I D R E A M O F J E A N N I E W I T H T

6 2 0 3 1 8 9 5 7 4 1 6 7 4 2 0 5 8 3 9

2. Encryption Algorithms
2.10. The VIC Cipher

The result of the first step is then expanded to ten digits through a process called ***chain addition.*** Starting with a group of a certain number of digits (in this case five, and later we will do the same thing with a group of ten digits), add the first two digits in the group together, take only the last digit of the result and append it to the end of the group, then ignore the first digit, and repeat the process.

The 10 digit result 0 3 5 8 4 3 8 3 2 7 is then added, digit by digit, ignoring carries, to the first 10 digits produced from the keyphrase to produce a ten-digit result, as follows: 6 2 0 3 1 8 9 5 7 4 + 0 3 5 8 4 3 8 3 2 7 = 6 5 5 1 5 1 7 8 9 1.

And these 10 digits are then encoded by encoding 1 as the first of the 10 digits produced from the second half of the keyphrase, 2 as the second, up to 0 as the tenth.

Index	*1 2 3 4 5 6 7 8 9 0*
Second half	1 6 7 4 2 0 5 8 3 9
Ten-digits result	6 5 5 1 5 1 7 8 9 1
Result	**0 2 2 1 2 1 5 8 3 1**

This ten digit number is used by chain addition to generate 50 pseudorandom digits for use in encipherment: 0 2 2 1 2 1 5 8 3 1 * 2 4 3 3 3 6 3 1 4 3 * 6 7 6 6 9 9 4 5 7 9 * 3 3 2 5 8 3 9 2 6 2 * 6 5 7 3 1 2 1 8 8 * 1 2 0 4 3 3 9 6 6 9

The last row (10 digits) of these digits (which will still be used again) is used like the letters in a keyword for transposition to produce a permutation of the digits 1 through 9 (with 0 last again): 1 2 0 4 3 3 9 6 6 9 ⇒1 2 0 5 3 4 8 6 7 9 and those digits are used as the top row of numbers for a straddling checkerboard:

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

2. Encryption Algorithms

2.11. Porta Table

Giovanni Baptista della Porta developed the Porta Table cipher method in 1565. The table uses a keyword and the table below to encipher message.

AB	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
CD	A	B	C	D	E	F	G	H	I	J	K	L	M
	Z	N	O	P	Q	R	S	T	U	V	W	X	Y
EF	A	B	C	D	E	F	G	H	I	J	K	L	M
	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
GH	A	B	C	D	E	F	G	H	I	J	K	L	M
	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
IJ	A	B	C	D	E	F	G	H	I	J	K	L	M
	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
KL	A	B	C	D	E	F	G	H	I	J	K	L	M
	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
MN	A	B	C	D	E	F	G	H	I	J	K	L	M
	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
OP	A	B	C	D	E	F	G	H	I	J	K	L	M
	T	U	V	W	X	Y	Z	N	O	P	Q	R	S
QR	A	B	C	D	E	F	G	H	I	J	K	L	M
	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
ST	A	B	C	D	E	F	G	H	I	J	K	L	M
	R	S	T	U	V	W	X	Y	Z	N	O	P	Q

2. Encryption Algorithms
2.11. Porta Table

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

To begin, write out your plain message and write out the keyword above it, as shown below:

Keyword: JACKET

Message: LOOK UNDER THE COUCH

J	A	C	K		E	T	J	A	C		K	E	T		J	A	C	K	E
L	O	O	K		U	N	D	E	R		T	H	E		C	O	U	C	H

The next step is to use the Porta table to create the enciphered message. Use the letters from the keyword (JACKET in the example above) to locate the correct line to use in the Porta table. In the example above “J” is the first keyword letter. Thus, locate “J” on the left hand side of the Porta table. Once you locate the “J”, the 5th set of letters in the Porta table, you use the letter from the plain message to find the enciphered letter above or below it. In this example the value for “L” in the “J” set is “U”.

Ciphertext: UBCS JJZRF LSU YBIXS

2. Encryption Algorithms
2.12. Vigenere Cipher

	ABCDEFGHIJKLMNOPQRSTUVWXYZ
A	ABCDEFGHIJKLMNOPQRSTUVWXYZ
B	BCDEFGHIJKLMNOPQRSTUVWXYZA
C	CDEFGHIJKLMNOPQRSTUVWXYZAB
D	DEFGHIJKLMNOPQRSTUVWXYZABC
E	EFGHIJKLMNOPQRSTUVWXYZABCD
F	FGHIJKLMNOPQRSTUVWXYZABCDE
G	GHIJKLMNOPQRSTUVWXYZABCDEF
H	HIJKLMNOPQRSTUVWXYZABCDEFG
I	IJKLMNOPQRSTUVWXYZABCDEFGH
J	JKLMNOPQRSTUVWXYZABCDEFGHI
K	KLMNOPQRSTUVWXYZABCDEFGHIJ
L	LMNOPQRSTUVWXYZABCDEFGHIJK
M	MNOPQRSTUVWXYZABCDEFGHIJKL
N	NOPQRSTUVWXYZABCDEFGHIJKLM
O	OPQRSTUVWXYZABCDEFGHIJKLMN
P	PQRSTUVWXYZABCDEFGHIJKLMNO
Q	QRSTUVWXYZABCDEFGHIJKLMNOP
R	RSTUVWXYZABCDEFGHIJKLMNOPQ
S	STUVWXYZABCDEFGHIJKLMNOPQR
T	TUVWXYZABCDEFGHIJKLMNOPQRS
U	UVWXYZABCDEFGHIJKLMNOPQRST
V	VWXYZABCDEFGHIJKLMNOPQRSTU
W	WXYZABCDEFGHIJKLMNOPQRSTUV
X	XYZABCDEFGHIJKLMNOPQRSTUVW
Y	YZABCDEFGHIJKLMNOPQRSTUVWX
Z	ZABCDEFGHIJKLMNOPQRSTUVWXY

Example 2.9. The encipher of the word CRYPTOGRAPHY under the key RAND is shown below

M = CRYP TOGR APHY

K = BAND BAND BAND

$E_K(M)$*=DRLS UOTU BPUB*

In this example, the first letter of each four-letter group is shifted (mod 26) by 1, the second by 0, the third by 13, and the fourth by 3.

2. Encryption Algorithms
2.12. Vigenere Cipher

The message "Wish you were here" can be encrypted by the three possible methods, using SIAMESE as the keyword:

Straight keyword:

Message:	W	I	S	H	Y	O	U	W	E	R	E	H	E	R	E
Key:	S	I	A	M	E	S	E	S	I	A	M	E	S	E	S
Cipher:	O	Q	S	T	C	G	Y	O	M	R	Q	L	W	V	W

Progressive key:

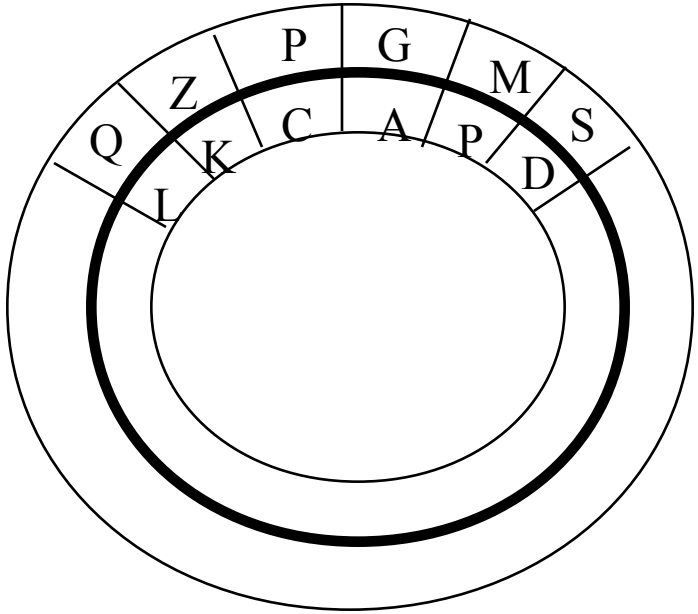
Message:	W	I	S	H	Y	O	U	W	E	R	E	H	E	R	E
Key:	S	I	A	M	E	S	E	T	J	B	N	F	T	F	U
Cipher:	O	Q	S	T	C	G	Y	P	N	S	R	M	X	W	Y

Autokey:

Message:	W	I	S	H	Y	O	U	W	E	R	E	H	E	R	E
Key:	S	I	A	M	E	S	E	W	I	S	H	Y	O	U	W
Cipher:	O	Q	S	T	C	G	Y	S	M	J	L	F	S	L	A

2. Encryption Algorithms
2.13. Polyalphabetic Substitution Ciphers

Simple Substitution cipher use a single mapping from plaintext to ciphertext letters, the single-letter frequency distribution of the plaintext letters is preserved in the ciphertext. Homophonic substitution conceal this distribution by defining multiple ciphertext elements for each plaintext letter. ***Polyalphabetic substitution ciphers*** conceal it by using multiple substitutions.



In 1568, Alberty published a manuscript describing a cipher disk that defined multiple substitutions. The disk defined *n* (where *n* is as an example the number of English letters) possible substitutions from the plaintext letters in the outer ring to the ciphertext letters in the inner ring, depending on the position of the disks. Alberti's important insight was his realization that the substitution could be changed during encipherment by turning the inner disk.

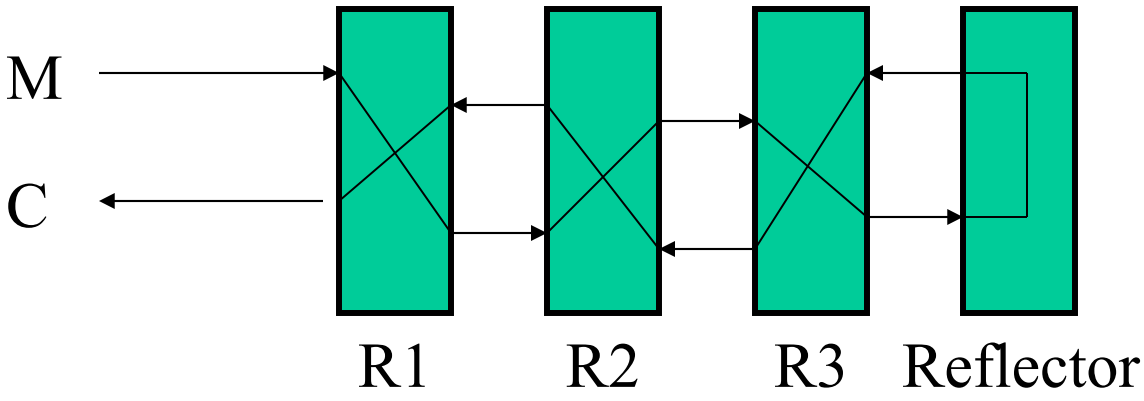
2. Encryption Algorithms

2.14. Rotor's Machines Bases

A rotor is a small disk of insulating material, with perhaps 26 equally-spaced electrical contacts in a circle on each side. The contacts on one side are connected to the contacts on the other side in a scrambled order.

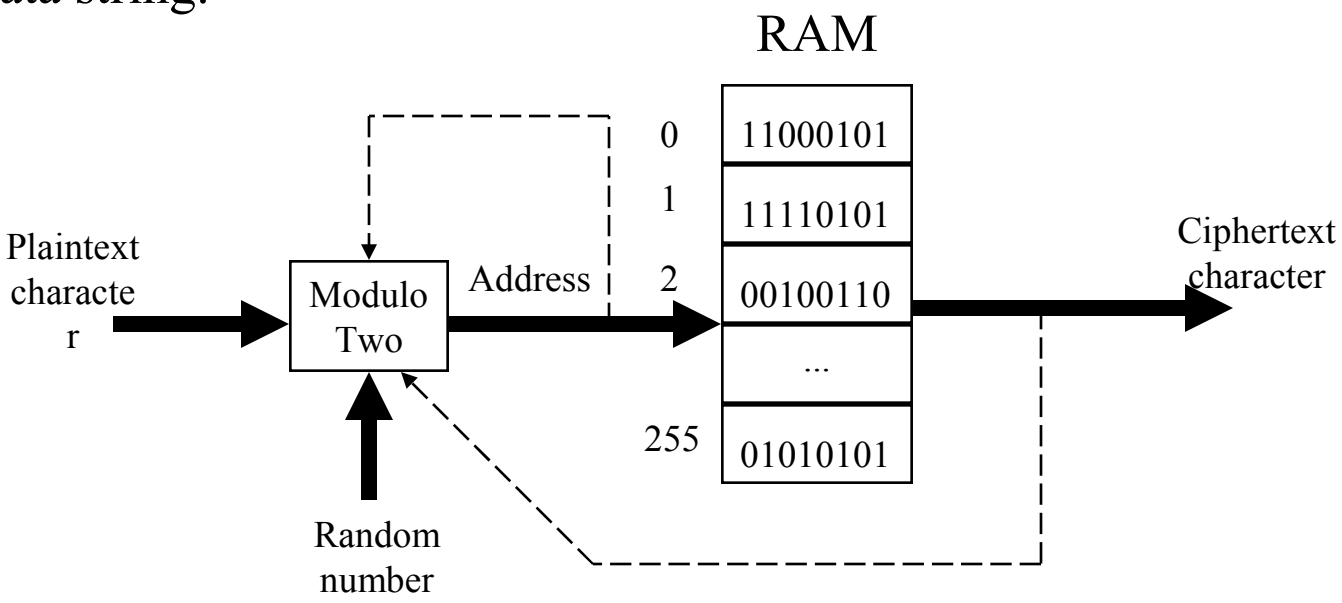
In Hebern machines, the contacts on the rotors were simply flat circles of metal; the machine had ball contacts on springs to make contact with them. This allowed the rotors to be put in upside down, for more possible keys. The Enigma, on the other hand, was built more cheaply; the rotors had plain metal contacts on one side, and spring contacts on the other. This almost halved the number of contacts needed, provided you didn't decide to use a new set of rotors.

A rotor provided a changing scrambled alphabet, by (you guessed it!) ***rotating*****.** A rotor with 26 contacts on each side, each corresponding to a letter of the alphabet, that changed E to M before rotating would now change D to L (or F to N, depending on the direction in which it rotated), while E could become any other letter, depending on the way the different wire went that was now brought into position to encipher it.



2. Encryption Algorithms
2.15. Modern Rotor Machine

Modern Rotor Machine is advanced version of the elector-mechanical rotor machines have been used during the second World War. The main element of this methods is electronic rotor implemented based on the Random Access Memory (RAM). As an example let us consider electronic rotor for the case of eight bit input data string.



Plaintext character	Random number	Address	Ciphertext character
10101100	10101101	10101100+ +10101101 =00000001	11110101

2. Encryption Algorithms
2.16. Hill Cipher

The ***Hill cipher*** performs a linear transformation on d plaintext characters to get *d* ciphertext characters. Suppose $d=2$, and let $M=m_1m_2$. M is enciphered as $C=E_K(M)=c_1c_2$, where

$$c_1=(k_{11}\,m_1+k_{12}m_2)\ mod\ n$$
$$c_2=(k_{21}\,m_1+k_{22}m_2)\ mod\ n$$

or in matrix form $C=E_K(M)=KM$ mod n, where K is the matrix of coefficients.

Deciphering is done using the inverse matrix K^{-1}: $D_K(C)=K^{-1}\ C$ mod $n = K^{-1}\ K\ M$ mod $n=M$.

Example 3.6. Let n be 26 and let K and K^{-1} be as follows:

$$\begin{vmatrix} K \\ 3 & 2 \\ 3 & 5 \end{vmatrix} \quad \begin{vmatrix} K^{-1} \\ 15 & 20 \\ 17 & 9 \end{vmatrix} \quad \text{mod } 26 = \quad \begin{vmatrix} I \\ 1 & 0 \\ 0 & 1 \end{vmatrix}$$

Suppose we wish to encipher the plaintext message EG, which corresponds to the column vector (4,6). We compute

$$c_1=(3*4+2*6)\ mod\ 26=24>Y$$
$$c_2=(3*4+5*6)\ mod\ 26=16>Q$$

2. Encryption Algorithms

2.17. Running-Key Ciphers

In a ***running-key cipher***, the key is as long as the plaintext message. One method uses the text in a book (or any other documents) as a key sequence in a substitution cipher based on shifted alphabets. The key is specified by the title of the book and starting position (section, paragraph, etc.)

Example 2.10. Given the starting position of the key: Book "Cryptography and Data Security" section 2.3.1, paragraph 2, and the plaintext message "THE TREASURE IS BURIED..." is enciphered as

M = *THETREASUREISBURIED...*
K = *THESECONDCIPHERISAN...*
EK(M) = *MOILVGOFXTMXZFLZAEQ...*

2.16. Running-Key Ciphers

If the key to a substitution cipher is a random sequence of characters and is not repeated, there is not enough information to break the cipher. Such a cipher is called ***one-time-pad,*** as it is only used once. The implementation of one-time pads in computer systems is based on an ingenious device designed by Gilbert Verman in 1917. Letting $M=m_1m_2...$ denotes a plaintext bit stream and $K=k_1k_2...$ a key bit stream, the Verman cipher generates a ciphertext bit stream $C=E_K(M)=c_1c_2...$, where $c_i=(m_i+k_1)$ mod 2, $i=1,2,...$. The Verman cipher is efficiently implemented in microelectronics by taking the "exclusive-or" of each plaintext/key pair $c_i=m_i+k_i$ Because $k_i+k_i=0$ for $k_i=0$ or 1, deciphering is performed with the same operation: $c_i+k_i = m_i+k_i + k_i=m_i$.