Parabola Volume 36, Issue 2 (2000)

Cryptography

Rod. James[1]

Htsi si na raitlcf ero aparobal no oht wb oerka oceds.

I am sure that, like me, your immediate reaction to the above sentence was to try to "decipher" the message (i.e. find out its hidden meaning). In fact this message is one of the simplest examples of cryptography which literally means "hidden writing" (from the Greek words $\kappa\rho\upsilon\pi\tau\omega$ and $\gamma\rho\alpha\phi\eta$). Cryptography varies from simple forms based on rearranging the letters of the message (as in the sentence above, where each pair of letters was transposed) to highly sophisticated ones used by Military Intelligence and the banking system. In fact the security of your PIN at an ATM depends on a method of encryption.

Another simple cryptic code was invented by Julius Caesar, who replaced each letter of a message by the letter 3 places along in the alphabet, with X replaced by A, Y by B and Z by C. This can be described mathematically by replacing each letter by its place in the alphabet (for example A is replaced by 1 and Z by 26) and then adding 3 to that number. For example the sentence Veni, Vidi, Vici (I came, I saw, I conquered) would be encrypted as follows:

	V	E	N	I		V	I	D	I		V	I	C	I
	22	5	14	9		22	9	4	9		22	9	3	9
+3 :	25	8	17	12		25	12	7	12		25	12	6	12
	Y	H	Q	L		Y	L	G	L		Y	L	F	L

This does not work for the letters X, Y, Z since (for example)

$$Z \to 26 \xrightarrow{+3} 29 \to ???$$

We overcome this by subtracting 26 from any number greater than 26. This process will be indicated by writing $(\text{mod } 26)$ on the end. Thus

$$Z \to 26 \xrightarrow{+3} 3 \ (\text{mod } 26) \to C$$

This code is obviously easy to decode. Since it consists of replacing a message letter m by a coded letter $c = m + 3 \ (\text{mod } 26)$, all we have to do is solve this equation to get $m = c - 3 \ (\text{mod } 26)$, where $(\text{mod } 26)$ now means add 26 if necessary. If the encryption used a different number a instead of 3, then $c = m + a \ (\text{mod } 26)$ and we could find a (and hence "break the code") by subtracting $(\text{mod } 26)$ the numbers $a = 1, 2, \ldots 26$ until a meaningful message appears. One aid for doing this was developed by the French cryptographer Vigenère, who wrote out a table of possible "Caesar ciphers":

[1]Rod James is a lecturer in Mathematics at UNSW and is the editor of Parabola.

A	B	C	D	...	Z
A	B	C	D	...	Z
B	C	D	E	...	A
C	D	E	F	...	B
	...		...	...	
Z	A	B	C	...	Y

Also a mechanical device for doing this was constructed many years ago by the US army. It consisted of two concentric rings containing the alphabet. Each Caesar cipher can then be achieved by rotating one of the rings while leaving the other one fixed.

Alphabetic Codes

Clearly encryption based on the Caesar cipher is too easy to break and so we look for a more complicated code, where we will from now on assume that each letter is replaced by a number (its position in the alphabet). Instead of **adding** a number to the message letter m, we could **multiply** m by some numbers. (again doing so mod 26). For example, if we doubled each letter, then

$$A \to 1 \xrightarrow{\times 2} 2 \to B \ldots \qquad \ldots \qquad \ldots N \to 14 \xrightarrow{\times 2} 2 \pmod{26} \to B.$$

Now we have a problem : even the person we have trusted with the code cannot decipher a message since they cannot decide whether A or N was replaced by B (and similarly whether B or O was replaced by D etc.). In general, if we use a "multiplication cipher" $c = am$ then *we must choose a to be coprime to* 26
(i.e. have no factors in common with 26).
The above two encryptions can be combined to yield "linear transformation ciphers":

$$c = am + b \pmod{26}$$

which are deciphered by solving this equation:

$$m = a^{-1}(c - b) \pmod{26}.$$

where a^{-1} means the number which yields $1 \pmod{26}$ when multiplied by a. For example $3^{-1} = 9 \pmod{16}$ since $3 \times 9 = 27 = 1 \pmod{26}$.
Questions:

1. Can you show that this is always possible if a is coprime to 26?
2. Can you find a way of breaking these codes if you are given the original message letters corresponding to two enciphered letters?

Because of the ease of breaking these codes, we now consider the most general possible "monoalphabetic ciphers" possible (i.e. we replace each single letter in the message by some letter, so that the process is reversible but only the encoder and decoder know the process). An example of this might be to take a long "keyword" like MATHEMATICS, remove the repeated letters to get MATHEICS and then replace the letters of the alphabet as follows:

A	B	C	D	E	F	G	H	I	J	K	L	...
M	A	T	H	E	I	C	S	B	D	F	G	...

where the letters from I to Z were replaced by the letters in the alphabet which are *not* in the word.

The amazing thing is that, using "probability" distribution, there *is* a way of deciphering a reasonably long message which has been encrypted by such a code (and so breaking the code). It is known that, in a long passage written in English, letters occur (on average) with the following frequencies per 1000 letters:

Letter	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequency	73	9	30	44	130	28	16	35	74	2	3	35	25
Letter	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequency	78	74	27	3	77	63	93	27	13	16	5	19	1

To see how this works, suppose we have captured the following (encrypted message):

UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX
AIZ VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW
EPYEPOPDZSZUFPO MB ZWP ZPEEMEUOZO UD ZWP FUXXSJP

Frequencies

Letter	A	B	D	E	F	G	H	I	J	M	O
Frequency	2	2	5	9	4	2	4	1	1	5	10
Letter	P	Q	S	T	U	V	W	X	Y	Z	
Frequency	18	2	10	2	9	5	5	5	1	15	

P and Z are clearly the most frequent letters and so they probably represent the letters E and T (not necessarily in that order!) Now notice that the pair ZW occurs 3 times (one of which is at the beginning of a word). Since the most common pairs in English are TH and HE (both approximately 26 in every 1000), this suggests that ZW represents TH (and so P represents E). In fact this is strengthened by the existence of the word ZWP which would represent the word THE.

To see where we are at this point, let us write the encrypted message with our suggestions below (in lower case letters):

```
UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX
 t              e   e te     th  t  e e
AIZ VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW
  t    e  t    t  t  h  e  ee     e   th
EPYEPOPDZSZUFPO MB ZWP ZPEEMEUOZO UD ZWP FUXXSJP
 e  e  e  t t  e     the te        t    the       e
```

We now see that

- ZWSZ obviously represents THAT: so S represents A.
- UZ obviously represents AT or IT: so U represents I
- QUZW now obviously represents WITH: so Q represents W.
- QSO now obviously represents WAS: so O represents S.
- WSFP APPD obviously represents HAVE BEEN.
  So F represents V, A represents B, and D represents N.

I will leave you to finish this, and discover that the original message was:

IT WAS DISCLOSED YESTERDAY THAT SEVERAL INFORMAL BUT DIRECT CONTACTS HAVE BEEN MADE WITH REPRESENTATIVES OF THE TERRORISTS IN THE VILLAGE.

More Complex Codes

Because the above code was so easy to break, the Military Intelligence of both the Nazis and the Allies made up codes during the Second World War which were more complex. Some of the ways they did this are given below.

1. Omit the spaces between the words making it hard to find common words.
2. Group letters in pairs (for example) to create four-digit numbers and add a key to those numbers.

   For example, using the original Caesar cipher, THAT would be encoded by

   $$\text{THAT} \rightarrow \text{TH AT} \rightarrow 2008\ 120 \rightarrow 2011\ 123 \rightarrow \text{TKAW}$$

   Note this time that the two T's were encoded differently.
3. Use a different key for every message, so that a decoder does not have enough letters on which to use a frequency distribution.

In another issue of Parabola, I intend to discuss some of the above ideas and to look briefly at some modern cryptography. Meanwhile you might like to think of ways of breaking codes based on the above ideas or how to make your own. In the (English!) words of Julius Caesar:

KDSSB FRGH EUHDNLQJ !