Mike Mudge introduces readers to the elementary concepts of cryptology in this month's 'not-so-secret' Numbers Count.

The need for secret communication in diplomacy and military affairs is readily appreciated. Now that electronic mail, electronic banking and other computer-based business transactions are part of everyday life, the need for security of information is clear to us all. The purpose of this article is to indicate certain aspects of number theory which are the foundations of elementary ciphers (or codes), to display examples of their use, and to invite readers to submit a working coder and decoder package with a specimen message.

It must be emphasised that the types of cipher discussed are elementary and bear little relation to those used in an ultimate security environment; however, they can form part of a challenge among, for example, computer club members: 'How do you go about cracking (even an elementary) code?' This aspect will not be considered here, but may form the subject of a future column, depending upon the response to this article.

Character ciphers

Stage 1 Translate the letters of the alphabet into their numerical equivalents 1–25.

Stage 2 Transform the numerical equivalent, m, of each letter in the message into another number, c, using an 'affine transformation' of the type: $c = am + b$ (modulo 26) where a and b are integers having no common factor. Note that since modulo 26 means retain only the remainder after division by 26, it follows that c lies between 0 and 25 inclusive.

Stage 3 Return each c to its equivalent letter using the reverse process to that described at stage 1; and group into convenient, ordered sets, say, of five to yield the code.

The particular affine transformation in which $a = 1$ is called a 'shift transformation' and clearly corresponds to replacing each letter of the message by that found by shifting b places through the alphabet.

For example, under the affine transformation $c = 7m + 10$ (modulo 26), the message 'PLEASE SEND MONEY' becomes the code 'LJMKG MGXFQ EXMW'!

Block ciphers

Stage 1 Group the letters of the message into convenient, ordered sets — say, for example, pairs. For example: 'PLEASE SEND MONEY' becomes 'PL EA SE SE ND MO NE Y'.

Stage 2 Transform the numerical equivalent, m_1m_2, of each pair in the message into another number pair, c_1c_2, using a pair of affine transformations of the type: $c_1 = a_1m_1 + b_1m_2$ (modulo 26), $c_2 = a_2m_1 + b_2m_2$ (modulo 26).

Stage 3 Return each c_1c_2 to its equivalent letter pair using the inverse translation process. For example: 'STOP PAYMENT' block ciphered in triples using the affine transformations:

$c_1 = 11m_1 + 2m_2 + 19m_3$ (modulo 26)

$c_2 = 5m_1 + 23m_2 + 25m_3$ (modulo 26)

$c_3 = 20m_1 + 7m_2 + m_3$ (modulo 26)

becomes 'ITN NEP ACW ULA'.

Exponentiation ciphers

Invented in 1978 by S Pohlig and M Hellman (see *IEEE Transactions on Information Theory* (vol 24, 1978, pp106–110)) this begins by translating the letters of the message into numerical equivalents, using A,B,C, ... Y,Z becomes 00,01,02, ... 24,25. The resulting numbers are then grouped into blocks of '2s' digits; where 2s is the largest positive even integer, such that all blocks of numerical equivalents corresponding to s letters (viewed as a single integer with 2s decimal digits) is less than an odd prime p. Associated with p is the *enciphering key* k, a positive integer which has no common factors with $p - 1$.

For each message block M, which is an integer with 2s digits, form a code block C using the transformation:

$C = M^k$ (modulo p), O C p.

For example, if $p = 2633$ and $k = 29$, then to encipher:

'THIS IS AN EXAMPLE OF AN EXPONENTIATION CIPHER', first convert to two-digit numerical equivalents, then group in blocks of size four: 1907 0818 0818 ... 0704 1723. The final 23 being an X added to complete a block of four.

Now use $C = M^{29}$ (modulo 2633) to obtain the code:

2199 1745 1745 ... 1841 1459.

Readers are invited to send an encoder, a decoder and a specimen message to Mike Mudge, 'Square Acre', Stourbridge Road, Penn, South Staffordshire WV4 5NF, or phone (0902) 892141 by 1 July 1988.

It would be appreciated if such submissions contained a brief description of the enciphering theory and any peculiarities of the programming, in a form suitable for publication in *PCW*. These submissions will be judged using subjective criteria, and a prize will be awarded by *PCW* to the 'best' contribution received by the closing date.

Please note that submissions can be returned only if a suitable stamped addressed envelope is provided.

Review: October '87

Space restrictions prevent a detailed review of a very popular topic. Refer to Don Thomasson, *Computing Today*, January 1984, pp52–53, and to this month's worthy prizewinner, Bill Hamley, of Church Lane, Scotter, Gainsborough, Lincolnshire DN21 3RZ.

John Gale of Hemel Hempstead is to be congratulated on his n-dimensional graphics on an Amstrad PC1512 SD, invoking the recursive powers of Pascal. Details on request.

Factorisation of Fermat Numbers, Review, September 1987

The factorisation of fermat numbers, $F_m = 2^{2^m} + 1$, proved to be a very difficult exercise even with the assistance of Theorem 3 (*PCW*, September 1987, page 214).

The table shown here is due to Professor Wilfrid Keller of the University of Hamburg and summarises the state of the art at 1980. This table accompanied the then new results that $1985 \times 2^{933} + 1$ is a factor of F_{931}, $19 \times 2^{6838} + 1$ is a factor of F_{6835}, while $19 \times 2^{9450} + 1$ is a factor of F_{9448}.

Values of m	Character of F_m
0, 1, 2, 3, 4	Prime
5, 6, 7, 8	Composite and completely factored
12*	Four prime factors known
10*, 11*, 19, 30, 36, 38, 150	Two prime factors known
9*, 13*, 15, 16, 17, 18, 21, 23, 25, 26, 27, 29, 32, 39, 42, 52, 55, 58, 62, 63, 66, 71, 73, 77, 81, 91, 93, 99, 117, 125, 144, 147, 201, 207, 215, 226, 228, 250, 255, 267, 268, 284, 287, 298, 316, 329, 416, 452, 544, 556, 692, 744, 931, 1551, 1945, 2023, 2456, 3310, 4724, 6537, 6835, 9448	Only one prime factor known
14	Composite but no factor known
20, 22, 24, 28, 31, 33, 34, 35, etc.	Character unknown

*Cofactor known to be composite

Subsequently GB Gostin and PB McLaughlin (*Math Comp* vol 18, No 158, April 1982 pp645–649) published a new prime factor for each of F_{29}, F_{36}, F_{99}, F_{147}, F_{150} and F_{201}. It is certain that further results exist in the literature and readers are invited to comment on any which they can locate.

Using the flexibility of the 'subjective criteria' this month's prizewinner is Andrew Slodkiewicz of 25 Taylors Road, St Albans, 3021 Victoria, Australia.

Andrew uses string handling routines in Turbo Pascal to manipulate numbers up to 256 digits. Unfortunately his hardware is undefined; however, the calculation of Euler Number E_{152} having 238 digits (for definitions see *PCW*, January 1987) took in excess of four hours to calculate. 'String division is performed using multiple subtractions, then shifting the numerator to the left, and so on. It takes about three seconds per unit in each decimal place.'

Readers may like to write to Andrew with advice or to obtain further details of his work in this area.

Mike Mudge welcomes correspondence on any subject within the areas of number theory and other computational mathematics. Particularly welcome are suggestions, either general or specific, for future Numbers Count articles; all letters will be answered in due course.

Isolated readers can be put in contact with others sharing the same interests. However, greater efficiency regarding published problems should result from contacting the prizewinner.