Proceedings of the Iowa Academy of Science

Volume 60 | Annual Issue Article 62

1953

A Cryptographic Machine

Harry Goheen
Iowa State College

A Cryptographic Machine

By Harry Goheen

In a recent textbook (1) on the theory of numbers Professor B. M. Stewart suggests the usefulness of the algebra of matrices over a finite field for encoding messages. The procedure is as follows. First the message is written as a normal message. Then each letter of the alphabet and each punctuation mark is associated with an element of a finite field F. Then the message is broken up into blocks, each block being a square matrix, and each matrix is premultiplied (or postmultiplied) by a non-singular scrambling matrix C whose elements are in the field, F. Each resulting matrix is translated into its alphabetical and punctuated form and the resulting code message is transmitted. On the receiving end, the code message is translated into a collection of matrices again and the matrices are premultiplied (or postmultipled) by the inverse of C. The resulting matrices are translated into blocks of punctuated and spaced words forming the message. Of course, C must be nonsingular and C^{-1} must be known to the receiver.

If the dimension of the matrices is small and the number of messages sent with the same scrambling C matrix is large, then as Stewart remarks, the skilled analyst will be able to break the code. However, if the dimension is large and suitable precautions are observed, this is not the case. In this case, a machine is necessary to do the computations and the description of a possible such machine is the purpose of this note. The author chooses to describe a machine which does arithmetic in the field of integers modulo 31, rather than the suggested 29. The prime number 31 is chosen since it is 2^5-1 and the properties of the binary representatation with five columns can be used.

The letters, space, and punctuation, are put into one-to-one correspondence with the integers modulo 31. These integers themselves are represented by five columns of binary digits. This gives an extra possibility, but the convention is observed that 0 has two representations, namely 00000 and 11111. The remaining numbers are represented by the binary equivalents of the corresponding natural numbers. It is clear that the representation, of -a(modulo 2^5-1) is obtained by replacing 0's with 1's and vice versa in the representation of a. Addition is accomplished, modulo 2^5-1, by ordinary binary addition with "end around carry" in which whenever it is nec-

essary to carry from the far left column the carry unit is propagated into the far right column. The fact that such a procedure will actually accomplish addition is the field is well-known as are also devices for accomplishing the routine. (2)

Multiplication is more difficult. It is desirable that as little extra equipment as possible be used in multiplying. The following scheme appears to be a good one. Let a be the multiplicand and b the multiplier in a product. Then either b or -b has at most two 1's in its representation. Call b* that representative which has at most two 1's. Let *a* be shifted in a circular fashion to the left, with the digit in the far left column being shifted end around to the right column, a number of places equal to the number of columns from the right of the first "1" in b*. Since shifting is equivalent to multiplication by two, and since ordinarily, the digit would be shifted into the nonexistent sixth column where it would have the weight 32, it is legitimate to shift it to the first column with weight one, one and 32 being the same, modulo 31. The resulting number is to be used as one of the augends of the partial product, or as the partial product itself. The other augend does not exist if b* has only the single "1" otherwise it is obtained by further shifting *a* cyclically until the total number of shifts is equal to the number of the column from the right in which the other "1" of b* is located. The two shifted numbers are added in this latter case just as in binary arithmetic or the single shifted number is used to form a partial product. The true product is the partial product if b* is b; it is the negative of the partial product if b* is -b.

Division is accomplished by Fermat's minor theorem which in this case states that $a^{30} = 1$ and hence $a^{29} = \frac{1}{a}$. The reciprocal of *a*, in case *a* is nonzero, is developed by storing successive powers of *a*. This may be done is sevaral ways. It requires seven distinct multiplications at least and working storage of two storage spaces as well as storage for the answer.

Since any command must specify at least an address in the memory at which a field element is located as well as a code indicating operation on this element, and since it is reasonable to suppose that there will exist several hundred such storage addresses, the commands cannot be stored in the momory. Possibilities for storing the commands are punched cards of the Hollerith or Powers type on each of which several distinct commands can be stored or on punched cards of a larger capacity on which entire routines can be stored. Because of the availability of the Hollerith and Powers card

readers, perhaps these are the cheaper devices, but the number of commands on each card in this case is severely limited and, since the cards feed slowly, the operating speeds are slow.

If the routine for multiplying two matrices is known, then the inverse of a matrix all of whose elements below the main diagonal are zero can be obtained by Hotelling iteration using as first approximation the diagonal matrix whose elements are the reciprocals of the corresponding elements of the original matrix. Then since the process is an error-squaring process and E_0 is a nilpotent matrix of index at most n, the dimension of the matrix, the k^{th} iterate will be exactly correct if $k \geqslant \log_2 n$. Similarly for a matrix whose elements above the main diagonal are zero. Then if one knows the inverse of A and of B the inverse of AB can be obtained and AB will be a general matrix.

If in addition, one has a routine for obtaining the inverse of a given martix, one can send a perfectly innocent looking message; for suppose given the message written in the form of a square matrix C, and a completely innocent message A is written as a similar square matrix. Then a scrambling matrix could be obtained as the solution

$$AX = C$$

or

$$XA = C.$$

This implies, of course, that both A and C are nonsingular, a situation which can be forced in general.

The message could also send the matrix X above in some fixed code Y. Then the innocent appearing message would not be suspect, whereas the matrix X would be doubly complicated, first as a scrambled matrix and second as a scrambling matrix.

References Cited

(1) B. M. Stewart. Theory of Numbers. New York, 1952.

(2) Harvard Computation Laboratory. Manual of Operations for the Automatic Sequence-Controlled Calculator. Cambridge, 1946.

DEPARTMENTS OF MATHEMATICS AND STATISTICS
IOWA STATE COLLEGE
AMES, IOWA