NON-SECRET ENCRYPTION USING A FINITE FIELD

by M J Williamson, 21 January 1974

A possible implementation is suggested of J H Ellis's proposed method ofencryption involving no sharing of secret information (key lists, machine set-ups, pluggings etc) between sender and receiver.

Summary

A method for non-secret encryption (see [1] and [2]) is herein expounded. Non-secret encryption is a way of passing a message securely without the need for information (eg a machine set-up) known to the sender and recipient but not to any interceptor.

Introduction

The method set out below is a modification of my original idea suggested by J H Ellis. It is rather neater but presents the same problem to an interceptor as the original.

The method

The initial requirements for encryption are:

1. A shift register generating a linear recursive sequence of length p (prime).
2. Different random number generators held by the sender and recipient.

The sender wishes to send a fill A of the shift register and the encryption proceeds as follows:

a. The sender generates a random number k and calculates Ak which he transmits.

b. The recipient generates a random number l and calculates (Ak)l = Akl which he transmits.

c. The sender solves the Euclidean algorithm to find K such that Kk = 1 (mod p) and calculates (Akl)K =Al which he transmits.

d. The recipient solves the Euclidean algorithm to find L such that Ll =1 (mod p) and calculates (Al)L = A which is the message the sender wanted to give him.

The interceptor's problem

The interceptor trying to read the traffic is now presented with the problem:

c. Given A^k, A^l and A^{kl}, find A.

If he can solve the distance problem for the recursive sequence used he can find x, y, z such that

- $A^k = B^x$
- $A^l = B^y$
- $A^{kl} = B^z$

(B is the basic root of the recursion) and now A = Bw where w = xy/z.

Unfortunately a solution to the interceptor's problem does not seem to yield a solution to the distance problem.

Remarks

1. The security of the system depends upon no one discovering a good algorithm to solve the interceptor's problem, but any method of encryption must depend upon something of this sort.

2. p need not necessarily be prime, but if it is not, then care must be taken that k and l are coprime to p.

3. The information rate of the system is low in that 3 bits are broadcast for every 1 of the message.
(The ratio in the method of [2] is 2 for 1).

References

[1] The possibility of Non-Secret digital encryption. J H Ellis, CESG Research Report, January 1970

[2] A note on non-secret encryption. C C Cocks, November 1973.