A NOTE ON 'NON-SECRET ENCRYPTION'

by C C Cocks, 20 November 1973

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

Note on "Non–Secret Encryption"

1. In [1] J H Ellis describes a theoretical method of encryption which does not necessitate the sharing of secret information between the sender and receiver. The following describes a possible implementation of this.

a. The receiver picks 2 primes P, Q satisfying the conditions

i. P does not divide Q-1.

ii. Q does not divide P-1.

He then transmits N = PQ to the sender.

b. The sender has a message, consisting of numbers C1, C2, ... Cr with 0 < Ci < N

He sends each, encoded as Di where Di = CiN reduced modulo N.

c. To decode, the receiver finds, by Euclid's Algorithm, numbers P', Q' satisfying

i. P P' = 1 (mod Q - 1)

ii. Q Q' = 1 (mod P - 1)

Then Ci = DiP' (mod Q) and Ci = DiQ' (mod P) and so Ci can be calculated.

Processes Involved

2. There is an algorithm, involving work of the order of log M, to test if M is prime, which usually works but can fail to give an answer. Hence as the density of primes is $(\log M)^{-1}$, picking primes is a process of order $(\log M)^k$ where k is a small integer.

3. Also, computing C_i^N (mod N) is of order $(\log N)^{k'}$ and the computation of $D_i^{P'}$ and $D_i^{Q'}$ even smaller; hence coding and decoding is a process requiring work of order $(\log N)^k$ where k will be about 2 or 3.

4. However, factorising N is a process requiring work of order $N^{1/4} (\log N)^k$, where k is a small integer (alternatively computing C from C^N (mod N) requires work of order N if the factorization of N is not known); so decoding for an interceptor of the communication is a process of order about $N^{1/4}$.

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

Note: There is no loss of security in transmitting $C_1 \ldots C_r$ all using the same N. Even if the enemy can guess a crib for eg $C_1 \ldots C_{r-1}$, this gives no information of use in decoding D_r etc. He could in any case provide himself with as many pairs (C_i, D_i) as he pleases, since the encryption process is known to him as well as to the transmitter!