

# A NOTE ON 'NON-SECRET ENCRYPTION'

by C C Cocks

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  $C_1, C_2, \dots, C_r$  with  $0 < C_i < N$   
 He sends each, encoded as  $D_i$  where  $D_i = C_i^N$  reduced modulo  $N$ .
- c. To decode, the receiver finds, by Euclid's Algorithm, numbers  $P', Q'$  satisfying
  - i.  $PP' = 1 \pmod{Q-1}$
  - ii.  $QQ' = 1 \pmod{P-1}$
 Then  $C_i = D_i^{P'} \pmod{Q}$  and  $C_i = D_i^{Q'} \pmod{P}$  and so  $C_i$  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  $C_i^N \pmod{N}$  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  $C^N \pmod{N}$  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  $C_1 \dots C_r$  all using the same  $N$ . Even if the enemy can guess a crib for eg  $C_1 \dots C_{r-1}$ , 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!