MULTIPLEXED SEQUENCES: SOME PROPERTIES
OF THE MINIMUM POLYNOMIAL

S.M. Jennings,
Racal Research Ltd.,
Worton Grange Industrial Estate,
Reading, Berks. RG2 0SB,
England.

1. INTRODUCTION

In recent years considerable interest has been shown in the
generation of binary sequences which have good randomness properties.
Such sequences play an important role in cipher systems. In many
situations the enciphering process begins with the conversion of the
plaintext into a string of bits by means of a binary "alphabet". The
sequence is then added to the plaintext bit by bit, using modulo 2
arithmetic and the resulting ciphertext is then transmitted. De-
cipherment is accomplished simply by adding the sequence to the cipher-
text in a similar manner.

Any sequence generated by a finite-state machine cannot be
considered truly random, since if the input is ultimately periodic then
the output must be also. An interceptor who knows the plaintext
equivalent of k bits of ciphertext also knows k bits of the sequence.
If it takes less than k bits of sequence to determine its entirety, then
the whole message may be discovered. If the generated sequence has
minimum polynomial of degree d, then knowledge of any 2d consecutive
bits is sufficient to determine it completely. Thus we have three
important requirements for a sequence used in a cipher system:--

1. The period of the sequence must be long (at least as long
   as any message to be enciphered).

2. The sequence should have a minimum polynomial of large degree.

3. The sequence must appear random.

It must be emphasized that for a good sequence generator within a
cipher system, these requirements are certainly necessary but clearly
not sufficient (for example see [Beker & Piper, 1982]).

In this paper we show how a special class of sequences, called multiplexed sequences, satisfy the first two requirements. This provides some evidence that multiplexed sequences may be eligible for use as a building block ([Beker & Piper, 1982]) towards a complete sequence generator. In practice, a sequence used in a cipher system would be far more complex than those we shall consider here.

This work is contained in my Ph.D. thesis entitled "A Special Class of Binary Sequences" submitted to the University of London in 1980. I would like to thank Dr. Henry Beker and Professor Fred Piper for their invaluable advice and encouragement and Racal Electronics Ltd. for their help and support.