NASA TECH BRIEF

NASA Pasadena Office

Generation of Key in Cryptographic System for Secure Communications

A number of general-purpose digital computers are used for gathering, categorizing, and storing confidential data. When these data are transmitted to a remotely located terminal, unauthorized access to it may be prohibited by using cryptographic encipherment. An encipherment with a particular key is illustrated as follows:

```
Sequence: 0 1 1 0 1 0 1 1 1 1 0 1 1 0 0
     Key: 1 1 1 1 0 1 0 1 1 0 0 1 0 0 0
  Cipher: 1 0 0 1 1 1 1 1 0 0 1 0 0 1 0 0
```

The transformation consists of a bit-by-bit modulo 2 sum (i.e., EXCLUSIVE-OR) of the data sequence with the key.

An authorized user would have a priori knowledge of the key and of the corresponding inverse transformation. Thus deciphering proceeds as follows:

```
  Cipher: 1 0 0 1 1 1 1 1 0 0 1 0 0 1 0 0
     Key: 1 1 1 1 0 1 0 1 1 0 0 1 0 0 0
Sequence: 0 1 1 0 1 0 1 1 1 1 0 1 1 0 0
```

Decipherment involves an inverse transformation whereby the key is subtracted bit-by-bit modulo 2 from the cipher, yielding the data sequence.

The cipher described is known as the Vigenere cipher. A Vigenère cipher with a key of unlimited length (i.e., nonrepeating) is called a Vernam system.

A report has been published which discusses key generation for the Vigenère, the compound Vigenère (where two or more combined sequences comprise the key), and the Vernam systems, using feedback shift registers (FSR's). The report discusses the theoretical considerations necessary for key generation. One major topic includes binary FSR's, particularly the nonsingular FSR's. The key sequences are generated using nonsingular FSR's. These FSR's are determined from factors of de Bruijn graphs of order r. A section of the report is devoted to linear feedback shift registers (LFSR's) and their role in generating binary sequences. These are compared with nonlinear FSR's.

A number of feedback functions are discussed for the generation of long key sequences. The long sequences can be split and then rejoined to create additional nonrepetitive sequences. The report includes a number of examples. Projections for future work are also discussed.

Note:

Requests for further information may be directed to:

Technology Utilization Officer
NASA Pasadena Office
4800 Oak Grove Drive
Pasadena, California 91103
Reference: TSP75-10278

Patent status:

This invention has been patented by NASA (U.S. Patent No. 3,911,330). Inquiries concerning nonexclusive or exclusive license for its commercial development should be addressed to:

Patent Counsel
NASA Pasadena Office
4800 Oak Grove Drive
Pasadena, California 91103

Source: Marvin Perlman of
Caltech/JPL
(NPO-13451)

Categories: 09 (Mathematics and
Information Sciences)
02 (Electronics Systems)