ABSTRACT

A system for encrypting or decrypting a digital message comprising a linear driving subsystem (4) for generating a pseudo random data sequence, a non-linear feedback subsystem (6) for producing a cipher stream from said pseudo random data sequence, and an encryption processor (26) for encrypting or decrypting a message by combining it with said cipher stream, the non-linear feedback subsystem comprising a non-linear feedback processing means (10) for generating a feedback sequence (12) by applying a non-linear function to at least one value from said pseudo-random data sequence and at least one previous value of the feedback sequence, and a cipher stream generating means (10) for generating said cipher stream by summing products of pairs of values of said pseudo random data sequence together with a value from said feedback sequence, the pairs of values being chosen such that the difference in sequence position as between each member of a pair is different as between each pair.

This Sheet Has Been Replaced

