FAST DECRYPTION ALGORITHM FOR THE KNAPSACK CIPHER

By
P. S. Henry and R. D. Nash

ABSTRACT

A fast decryption algorithm is described which permits use of the knapsack cipher (a public-key cryptosystem) at data rates in the neighborhood of 10 Mbit/sec. This high-speed capability can be used to incorporate the security and flexibility of public-key cryptosystems into a wide variety of real-time communications applications. Implementation of the algorithm using Very Large Scale Integration appears attractive: The circuit functions required are approximately 56 kilobits of memory and a small amount of arithmetic logic.

A real-time speech privacy system has been built using a Digital Signal Processor chip and a doubly-iterated knapsack cipher. The encryption vector is stored in a lookup table and used to encrypt 32-bit blocks of 64 kb/s PCM speech; decryption is performed in two pipelined stages.