ABSTRACT

IMPLEMENTATION OF A HYBRID RSA/DES KEY MANAGEMENT SYSTEM

A electronic mail ring-topology network has been implemented at M/A-COM Labs to demonstrate the feasibility and security of a hybrid RSA/DES encryption system. The RSA public key scheme is used for the generation and management of encryption keys while DES is used for the encryption/decryption of data.

System hardware consists of a 16 bit 8 MHz μP System with a single chip DES processor, fast RAM, and a 16 x 16 hardware multiplier. A total of 3 nodes are implemented in the network. Each node is capable of acting as a Key Distribution Center, a wire-tap center, and/or a normal user node. System software consists of a round robin executive and a number of interrupt handlers. A message originated from a node passes through all other nodes before terminating in the original node in this ring-topology network.

With this implementation, generation of a 16 word block public key pair takes approximately 11 minutes. Public key encryption of a 15-word data block takes 4.6 seconds. Using the "signature" properties of the RSA Scheme, call set up time takes up to 21 seconds. Once a session is established, however, data encryption can be performed at high speed, depending on the DES chip chosen.

In most operational environments, the generation and distribution of public keys need only be done infrequently, thus the time it takes to generate public keys is not critical. Call set up time, on the other hand, is more critical. This problem will become less formidable, however, with the development of VLSI RSA circuits.

Authors: Y. A. Lau, T. R. McPherson