Ms. Susan L. Graham
Computer Science Division-EECS
University of California, Berkeley
Berkeley, California 94720

Dear Ms. Graham,

Thank you very kindly of your communication of October 7 with the enclosed paper on "Secure Communications over Insecure Channels". I am sorry to have to inform you that the paper is not in the main stream of present cryptography thinking and I would not recommend that it be published in the Communications of the ACM, for the following reasons:

1. The paper proposes to describe cryptographic security by transmitting under various unrealistic working assumptions puzzles conveying key information. A puzzle is just another word to talk about a crypto system. The strength of the system hinges strongly on the quality of the puzzle transformations. These are not defined.

2. Experience shows that it is extremely dangerous to transmit key information in the clear. Such practices of the legitimate user open the set-up to illegitimate test procedures, which only a very strong system could resist. Again the nature of the cryptographic system is not specified.