COMMUNICATIONS OF THE ACM *A Publication of the Association for Computing Machinery*

acm

1133 AVENUE OF THE AMERICAS NEW YORK, NEW YORK 10036 212 265-6300

R. L. ASHENHURST, Editor-in-Chief
MYRTLE R. KELLINGTON, Executive Editor

Reply to:

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

October 22, 1975

Mr. Ralph C. Merkle
2441 Haste St., #19
Berkeley, Ca. 94704

Dear Ralph:

Enclosed is a referee report by an experienced cryptography expert on your manuscript "Secure Communications over Insecure Channels." On the basis of this report I am unable to publish the manuscript in its present form in the Communications of the ACM.

I also read the paper myself and was particularly bothered by the fact that there are no references to the literature. Has anyone else ever investigated this approach. If they consider it and reject it, why? Also, have you considered the fact that E may be willing to devote substantial resources to breaking the code? What makes you think an N^2 amount of effort is a deterrent, particularly since your solution allows E to set N code-breakers to work in parallel, each requiring N units to solve one of the puzzles?

I hope these comments and those of the referee will be of help to you in future work on the subject.

Thank you for submitting your manuscript for publication. Your interest is greatly appreciated.

Sincerely yours,

Sue

Susan L. Graham
Editor, Programming Techniques

SLG:bb
Encl.