Using Encryption for Authentication in Large Networks of Computers

Roger M. Needham and Michael D. Schroeder

Definitions:

Authentication: verifying the identity of the communicating principals

Why not just use passwords for authentication?

Public key: Two keys are necessary. One for encryption and one for decryption. The knowledge of one key gives no help in finding the other. The two keys will act as inverses for one another.

Conventional: Shared Key, that is private.

Contribution:

From the abstract: Use of encryption to achieve authenticated communication in computer networks is discussed. Both conventional (symmetric key/private key) and public-key (asymmetric key?) encryption algorithms are considered as the basis for protocols.