Tech Info Library

# AppleTalk: Where to Find Encryption Algorithm Information

Revised: 4/30/90
Security: Everyone

AppleTalk: Where to Find Encryption Algorithm Information

======================================================================

This article last reviewed: 3 April 1990

TOPIC --------------------------------------------

I am putting together a file server on a mainframe and need information on the password encryption algorithm Apple uses.

Does Apple publish that information?

DISCUSSION ---------------------------------------

Inside AppleTalk (Addison Wesley, ISBN #0-201-19257-8), pages 13-28 to 13-30, discusses user authentication methods. Pages 13-29 and 13-30 discuss the AFP random exchange authentication method, which uses the NBS DES (National Institute of Standards and Technology Data Encryption Standard) algorithm.

For more specific answers about this algorithm -- or to get the algorithim itself -- contact the National Institute of Standards and Technology.

We also found a DES encryption program written in C starting on page 262 of a book called "UNIX System Security". The book, written by Patrick H. Wood and Stephen G. Kochan, is published by Hayden Books (ISBN #0-8104-6267-2).

For more information, search under: "National Institute of Standards and Technology"

Tech Info Library Article Number:5056