Lecture 4: Striving for Confusion

Structures have been found in DES that were undoubtedly inserted to strengthen the system against certain types of attack. Structures have also been found that appear to weaken the system.

Lexar Corporation, "An Evalution of the DES", 1976.

CS588: Security and Privacy
University of Virginia
Computer Science

David Evans
http://www.cs.virginia.edu/~evans

Menu

- Projects
- Enigma Continued
- Block Ciphers

Operation

- Day key (distributed in code book)
- Each message begins with message key (“randomly” choosen by sender) encoded using day key
- Message key sent twice to check
- After receiving message key, re-orient rotors according to key