Giới thiệu thuật toán AES(lịch sử, mục tiêu, ứng dụng): gnaS

Ưu điểm, nhược điểm so sánh với DES: ìuQ

Cơ chế hoạt động

**Mã hoá**

* Plaintext, key bit? oaT
* Sử dụng Rounds ? vòng oaT
* Trong 1 Rounds có gì? ( 6 cái ) mỗi tk chọn 2 cái
  + AddRoundKey
  + SubBytes
  + MixColumns
  + ShiftRows Tao
  + KeyExpansion Tao

**Cơ chế Giải mã**

Cơ sơ toán học và hiệu suất

* Phép toán trên trường hữu hạn GF(2^8) ganS
* Rijndael Finite Field ìuQ
* Hiệu suất oaT

Chương trình minh hoạ thuật toán TQS