Jan 31, 2005 -- Lecture 6

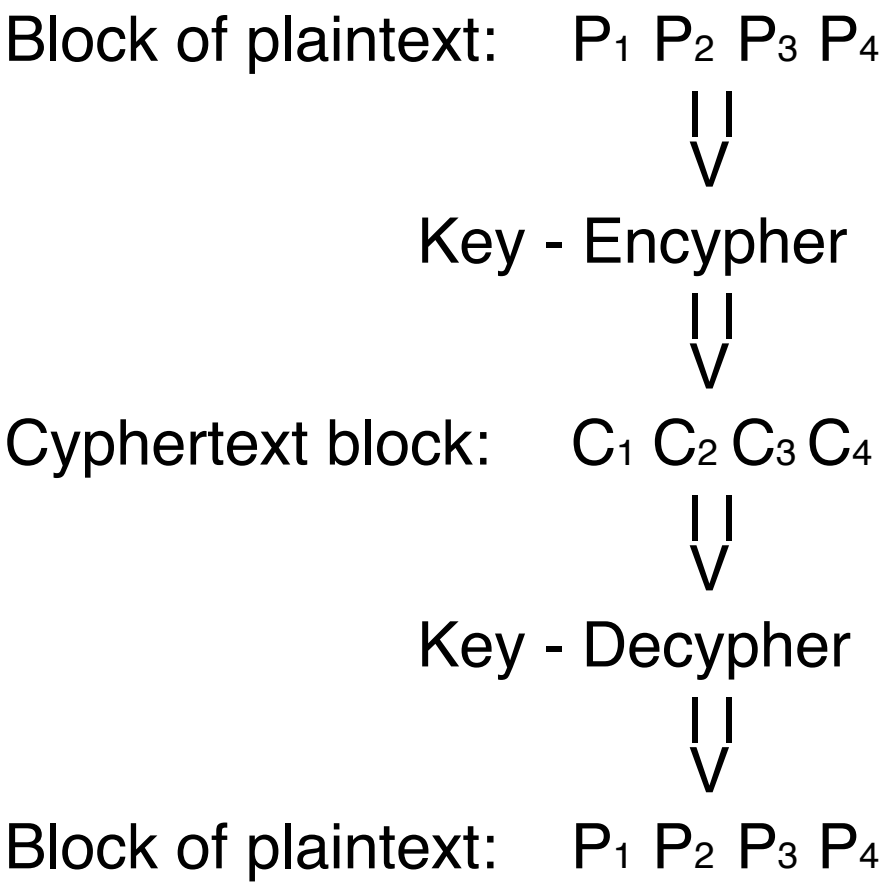
22C:169
Computer Security

Douglas W. Jones

Department of Computer Science

Block Cyphers

An Idea for Symmetric Key Cyphers



Characteristics of Block Cyphers

For each key, encypher and decypher are
One to One functions

There are 2^n! one to one mapping on n bits
Ideally, key simply selects the mapping

How do you select a mapping?
Hard work!

Block Cypher Issues

Block size:

- *Same plaintext likely twice in message,*
  - Too Small
- *Much larger than key size,*
  - Limits universe of mappings
- *Typically*
  - Similar to key size

DES - First widely used block cypher

1974, adopted as FIPS 46, 1977

Developed by IBM with NSA "help"

Block size = 64 bits

Key size = 48 bits (why so short?)

Idea: Multiround permutation and XOR

EFF built a DES cracking engine, 1998

cost: *under $250,000*

speed: *3 days to crack*

DES, the idea:

Generate the key schedule

16 keys, 48 bits each

Each key is function of original key

Apply keys in succession

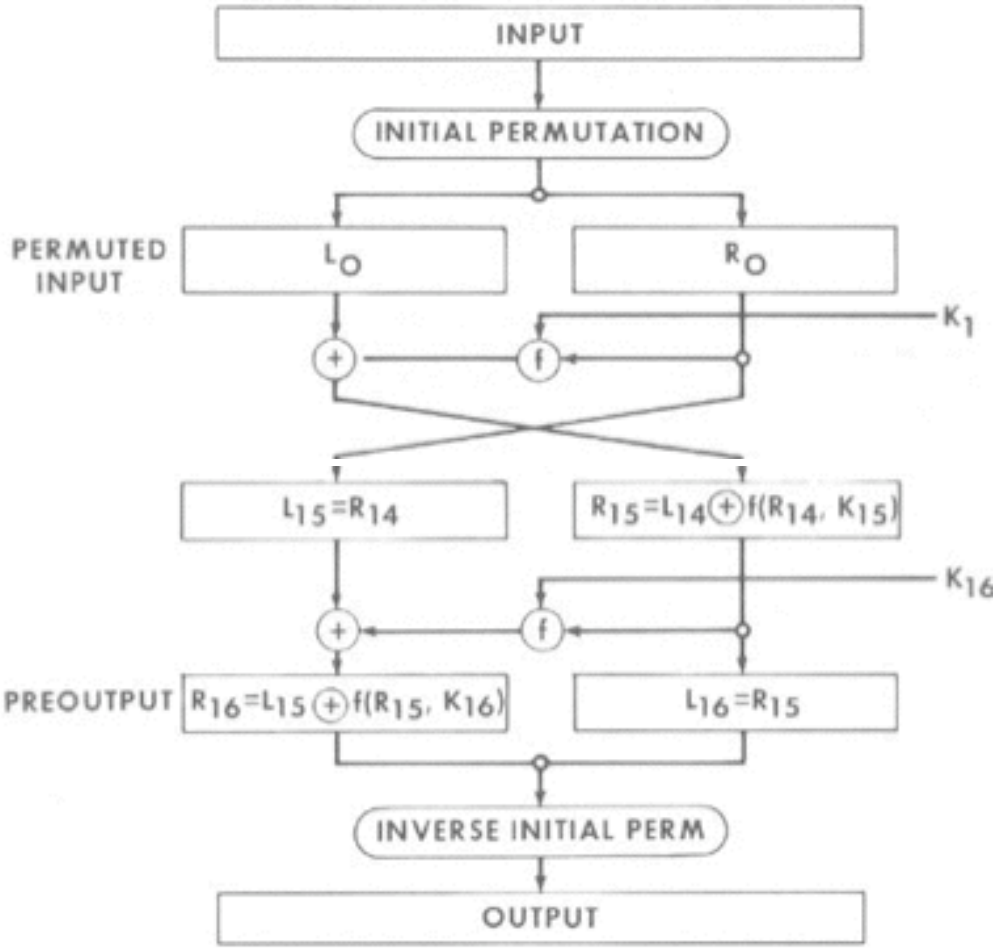
16 rounds of encryption

Each round looks relatively weak

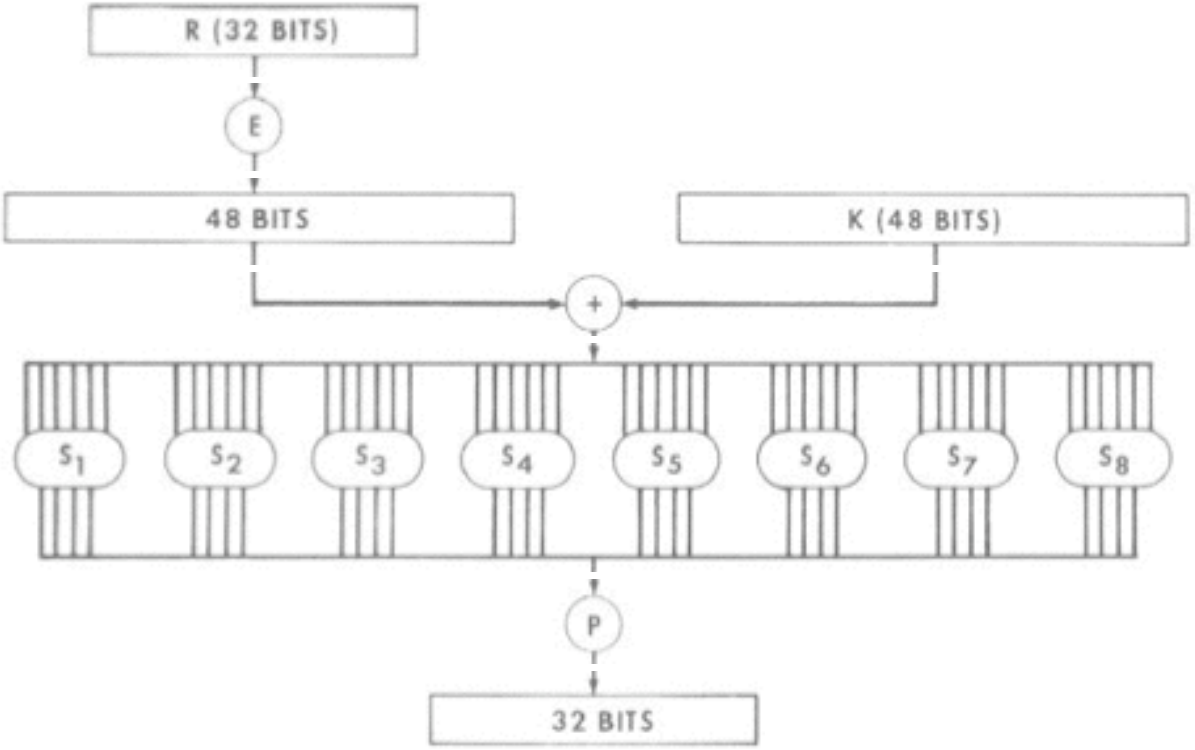
Design emphasis

Easy hardware implementation

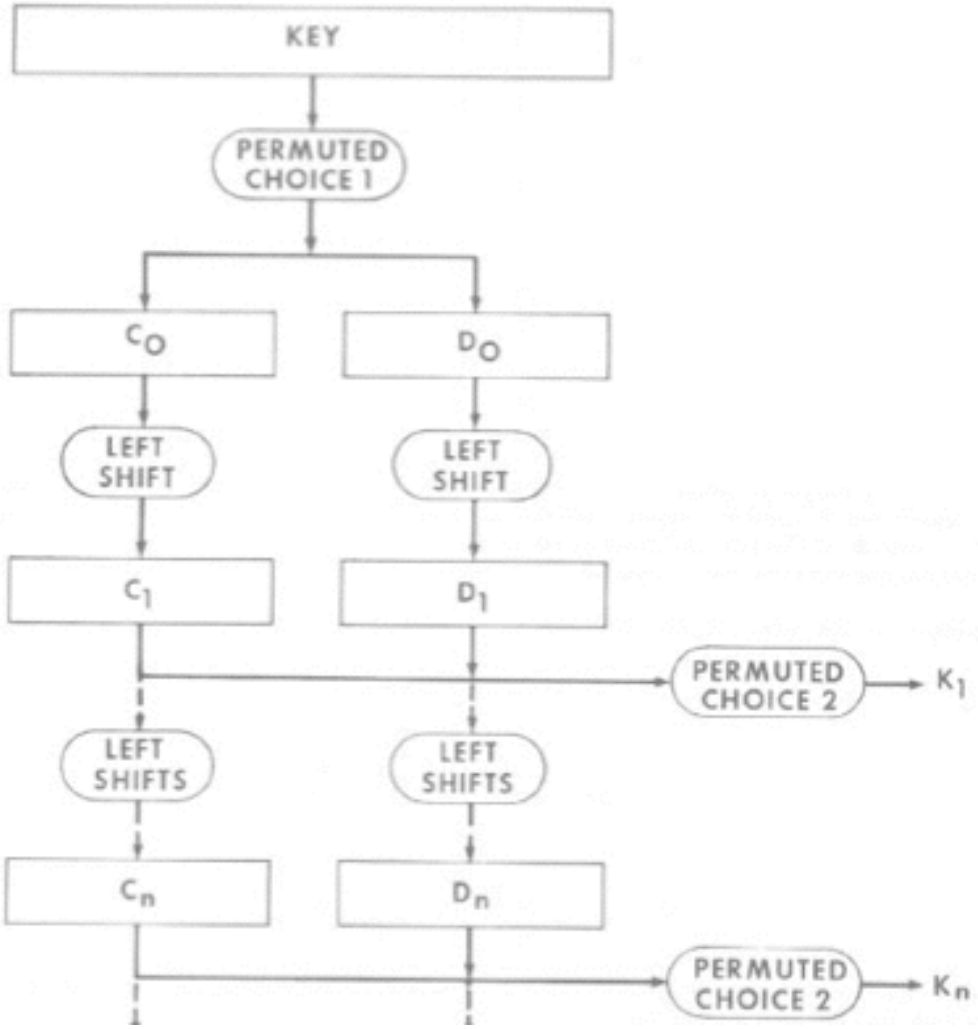
Top level view of DES (2-round version)



Function blocks in each stage of DES



Key Schedule Generation



Cracking DES (RSA DES Challenge)

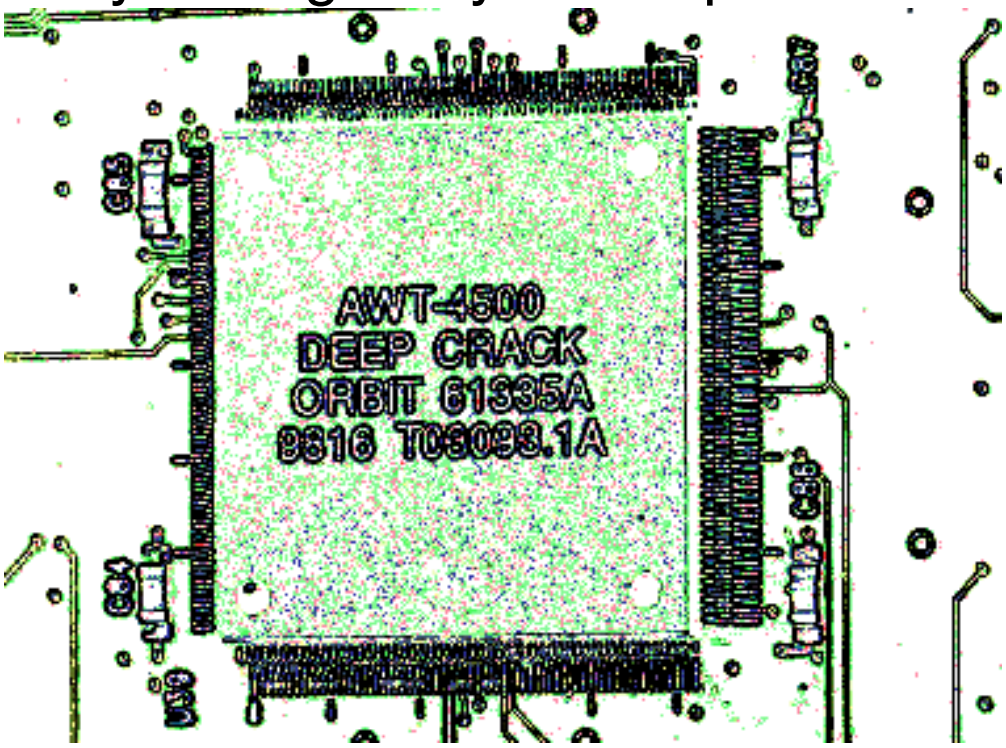
First public crack, 1997

39 days using over 10,000 computers

Team lead by Rocke Verser of Loveland Colorado

Second public crack, 1998

3 days using array of Deep-Crack chips



What To Do?

Triple DES:

$DES(k_1, DES(k_2, DES(k_3,t)))$

Warning: What if

$DES(k_1, DES(k_2, t)) = DES(f(k_1, k_2), t)$

Proofs are difficult!

AES (Rijndael)

Joan Daemen and Vincent Rijmen,
Selected as AES in 2000 in open competition run by NIST

As of 2003

Certified for classified information

As of 2004

No recognized successful attacks

Characteristics:

Block size = 128 bits

Key size = 128, 192 or 256 bits

Multiround with key schedule

One AES Round

Substitute Bytes

Uses a table lookup to do one-to-one

Shift Rows

Shift each 4-byte row

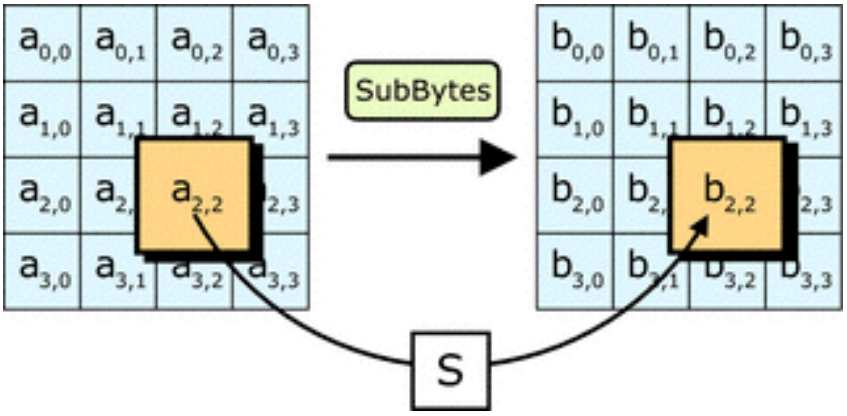
Mix Columns

Linear transformation of 4-byte column

Add Round Key

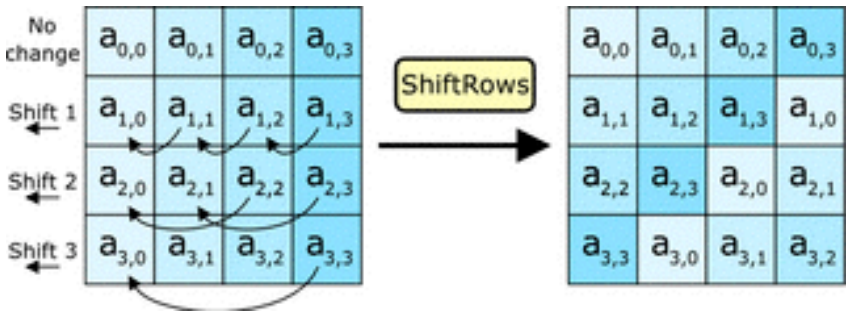
Key for this round combined with bytes

AES Substitute Bytes Step



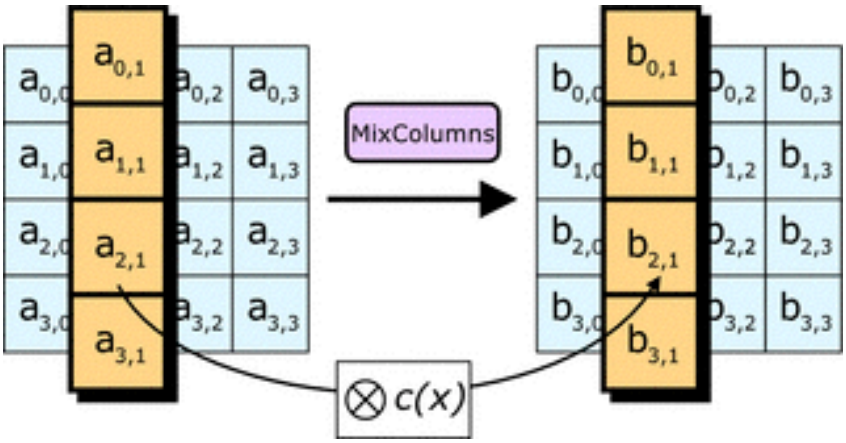
b = S[a], where S is a 265 entry table

AES Shift Rows Stage



This step is as trivial as it looks

The AES Mix Columns Step



Fixed linear transform of 32-bit column

The AES Add Round Key Step