

6.857 Computer and Network Security  
Lecture 8

Note:

- RSA conference, Discussion of dual-ec-drbg

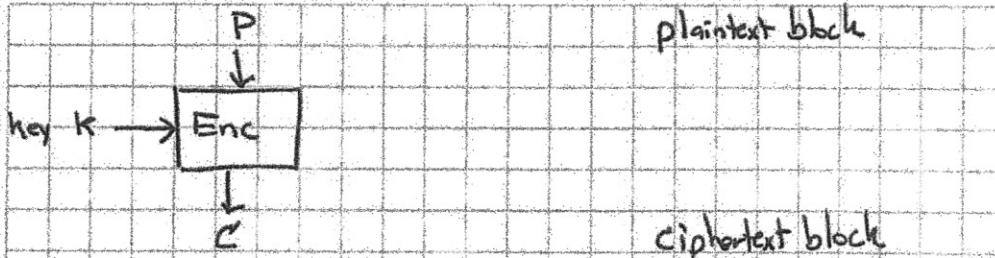
Project Idea:

- “Security of routers”

Today: Block Ciphers

- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)
- Ideal Block Cipher
- “Modes of Operation,” ECB, CTR, CBC, CFB
- IND-CCA security definition
- UFE mode

Block ciphers:



fixed-length P, C, K

DES:  $|P| = |C| = 64$  bits  $|K| = 56$  bits

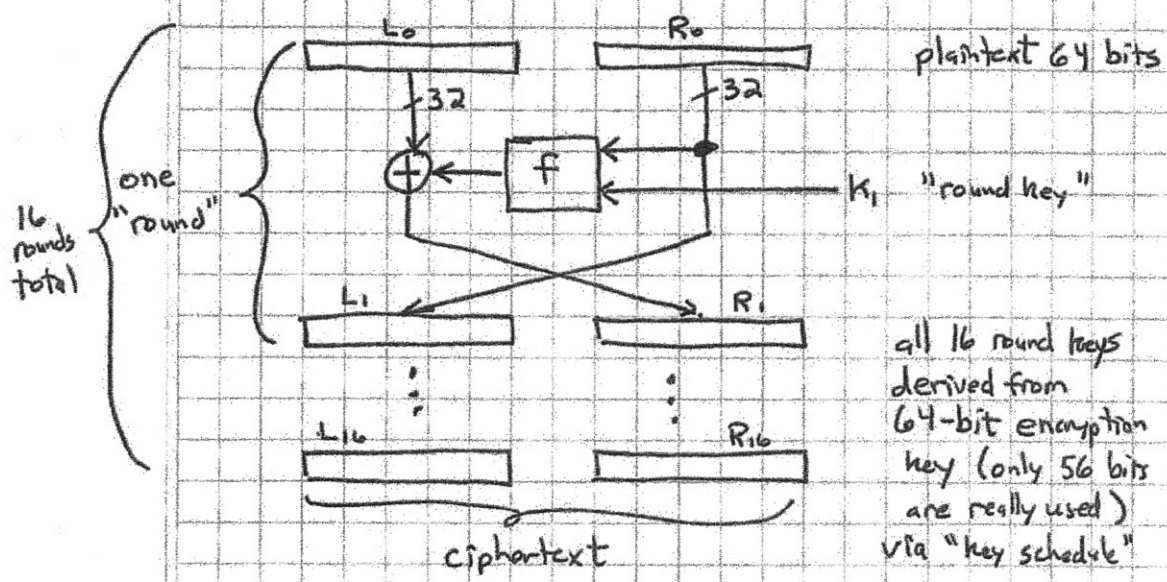
AES:  $|P| = |C| = 128$  bits  $|K| = 128, 192, 256$  bits

Use a "mode of operation" to handle variable-length input.

DES

"Data Encryption Standard"  
Standardized in 1976. Now deprecated in favor of AES.

"Feistel structure":

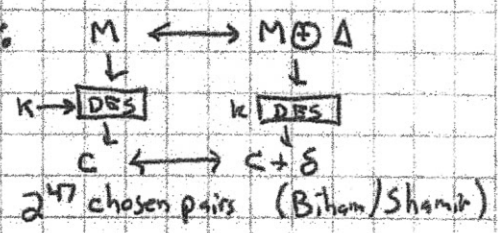


Notes: Invertible for any  $f$  and any key schedule.

$f$  uses 8 "S-boxes" mapping 6-bits  $\Rightarrow$  4 bits nonlinearly.

Key is too short! (Breackable now quite easily by brute-force)

Subject to differential attacks:



Subject to linear attacks:

e.g. if  $M_3 \oplus M_{15} \oplus C_2 \oplus K_{14} = 0$  (eqn on bits)  
with prob  $p = 1/2 + \epsilon$

then need  $1/\epsilon^2$  samples to break (Matsui,  $2^{43}$  PT/CT pairs)

AES

"Advanced Encryption Standard" (U.S. govt)

Replaces DES

AES "contest" 1997-1999:

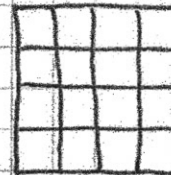
15 algorithms submitted: RC6, Mars, Twofish, Rijndael, ...  
 Winner = Rijndael (by Joan Daemen & Vincent Rijmen, Belgians)

Specs: 128-bit plaintext/ciphertext blocks  
 128, 192, or 256-bit key  
 10, 12, or 14 rounds (dep. on key length)

Byte-oriented design (some math done in Galois field  $GF(2^8)$ )

View input as 4x4 byte array:

$4 \times 4 \times 8 = 128$



For version with 128-bit keys, 10 rounds:

- Derive 11 "round keys", each 128 bits (4x4x byte)

- In each round:
  - ① XOR round key
  - ② Substitute bytes (lookup table)
  - ③ Rotate rows (by different amt)
  - ④ Mix each column (by linear opn)

- Output final state

See readings for details.

There are very fast implementations. Also Intel has put supporting hardware into its CPUs.

Security: Good; perhaps # rounds should be a bit larger..

For practical purposes, can treat AES as ideal block cipher:

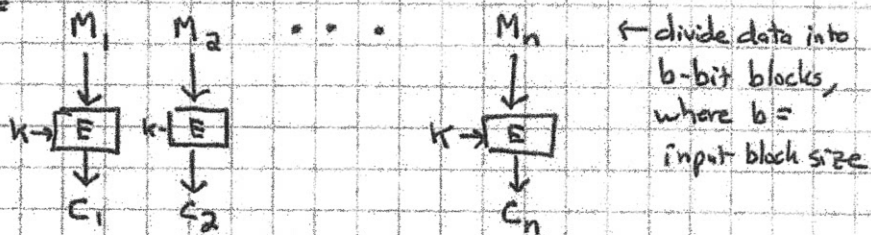
[ For each key, mapping  $Enc(K, \cdot)$  is a random independent permutation of  $\{0,1\}^{128}$  to itself.

Modes of Operation:

How to encrypt variable-length messages? (using AES)

- "ECB" = "Electronic code book"
- "CTR" = "Counter mode"
- "CBC" = "Cipher-block chaining" (& CBC-MAC)
- "CFB" = "Cipher feedback"
- ... (others...)

ECB:



To handle data that is not a multiple of  $b$  bits in length:

- ↳ Append a "1" bit (always)
- ↳ Append enough "0" bits to make length a multiple of  $b$  bits.

This gives invertible (1-1) "padding" operation.

Pad before encryption; unpad after decryption.

ECB preserves many patterns: repeated message blocks  
 ⇒ repeated ciphertext blocks

ECB really only good for encrypting random data  
 (e.g. keys)

MIT OpenCourseWare  
<http://ocw.mit.edu>

6.034: Introduction to Algorithms  
Spring 2014

For information about citing these materials or our Terms of Use, visit: <http://ocw.mit.edu/terms>.