TOPIC: 6.857

DATE: 2/18/2020

FILE UNDER:

PAGE: L05.1

Admin:

Pset #1 due tonight
Pset #2 out tonight
Projects!

Talk:

Adi Shamir, 4pm, Stata Center (32-G449), "Adversarial Examples in ML"

Today:

Block Ciphers

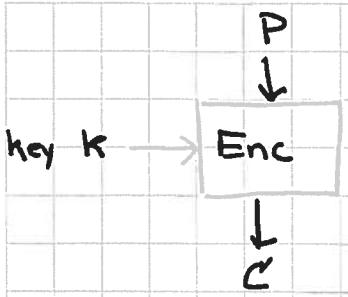
- ✓ DES (incl. diff. cryptanalysis remarks by Adi Shamir)
- AES
- Ideal cipher
- Modes of operation (ECB, CTR, CBC)

next time

Readings:

Ferguson	Ch 3
Paar	ch 3, 4
Katz	Ch 5
Wikipedia	"Block cipher modes of operation"
	"Ciphertext stealing"

Block ciphers:



plaintext block

ciphertext block

fixed-length P, C, K

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

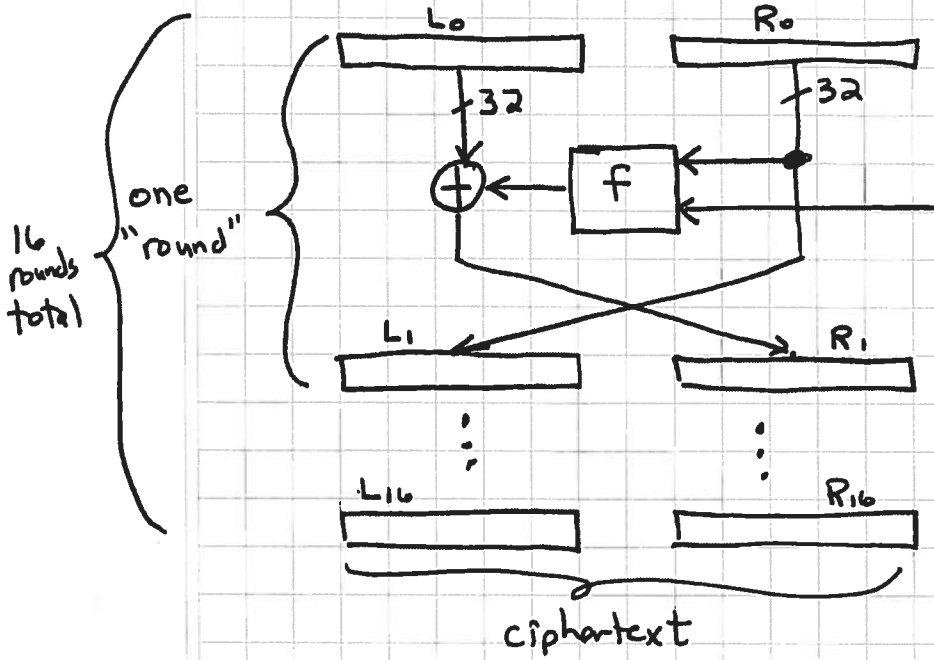
AES: $|P| = |C| = 128$ bits $\quad |K| = 128, 192, 256$ bits

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

DES

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

"Feistel structure":



plaintext 64 bits

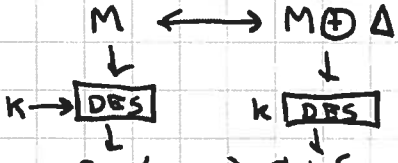
all 16 round keys derived from 64-bit encryption key (only 56 bits are really used) via "key schedule"

Note: Invertible for any f and any key schedule.

f uses 8 "S-boxes" mapping 6-bits ⇒ 4 bits nonlinearly.

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

Subject to differential attacks:



2^{47} chosen pairs (Biham/Shamir)

Subject to linear attacks:

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

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