Admin:

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

Talk:

Adi Shamir 4pm, Stat Center (32-6449) (Adversarial Examples in ML)

Today:

Block Ciphers

✓ DES (incl. diff. cryptanalysis, remake by Adi Shamir)

AES

next time

Ideal cipher

Modes of operation (ECB, CTR, CBC)

Readings:

Ferguson Ch 3

Paar Ch 3, 4

Katz Ch 5

Wikipedia: "Block cipher modes of operation"

"Ciphertext stealing"
Block ciphers:

\[ \text{key } K \rightarrow \text{Enc} \rightarrow C \]

Fixed-length P, C, K:

- DES: \[ |P| = |C| = 64 \text{ bits} \quad |K| = 56 \text{ bits} \]
- AES: \[ |P| = |C| = 128 \text{ bits} \quad |K| = 128, 192, 256 \text{ bits} \]

Use a "mode of operation" to handle variable-length input.
"Data Encryption Standard"
Standardized in 1976. Now deprecated in favor of AES.

"Feistel structure":

```
L0  +  f  +  L1  +  ...  +  L16
/      \                     /      \                    /
\      /                     \      /                    /
R0  -  \                     -  R1  -  ...  -  R16
\    /                     /    \                    /    
   `--'                     `--'                       `--'
```

plaintext 64 bits

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

ciphertext

---

Note: Invertible for any \( f \) and any key schedule.

\( f \) uses 8 `S-boxes` mapping 6-bits \( \Rightarrow \) 4 bits non-linearly.

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

Subject to differential attacks:

\[
M \leftrightarrow M \oplus \Delta \\
\Downarrow \\
K \xrightarrow{\text{DES}} k \xrightarrow{\text{DES}} C \leftrightarrow C \oplus \delta
\]

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

Subject to linear attacks:

\[ M_3 \oplus M_{15} \oplus C_0 \oplus C_7 \oplus K_{14} = 0 \] (eqn on bits)

with prob \( p = \frac{1}{2} + \varepsilon \)

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