Pset #2 out. 857coin up!

Next week: Mon: Zeldovich
          Wed: Edgar
Post project ideas on Piazza by March 7th (turn in paper by 3/18)

- Shamir's secret sharing
- Block ciphers
  - DES
  - AES
  - modes of operation
    - ECB, CTR, CBC, CFB,...

Readings:

Ferguson: Ch 3, Ch 21.9
Page: Ch 3, 4
Katz: ch 6.2.3, 6.2.5, 13.3
Key management

Start with "secret sharing" (threshold cryptography).
- Assume Alice has a secret $s$, (e.g. a key)
- She wants to protect $s$ as follows:
  - She has $n$ friends $A_1, A_2, \ldots, A_n$
  - She picks a "threshold" $t$, $1 \leq t \leq n$
  - She wants to give each friend $A_i$
    a "share" $s_i$ of $s$, so that
      - any $t$ or more friends can reconstruct $s$
      - any set of $< t$ friends can not.

Easy cases:
- $t = 1$: $s_i = s$
- $t = n$: $s_1, s_2, \ldots, s_{n-1}$ random
  $s_n$ chosen so that
  $s = s_1 \oplus s_2 \oplus \ldots \oplus s_n$

What about $1 < t < n$?
Shamir's method ("How to Share a Secret", 1979)

Idea:
1. 2 points determine a line
2. 3 points determine a quadratic
3. t points determine a degree (t-1) curve

Let $f(x) = a_{t-1} x^{t-1} + a_{t-2} x^{t-2} + \ldots + a_1 x + a_0$

There are $t$ coefficients. Let's work modulo prime $p$.

We can have $t$ points: $(x_i, y_i)$ for $1 \leq i \leq t$

They determine coefficients, and vice versa.

Polynomial Evaluation

\[
\{ (x_i, y_i) \} \rightarrow (a_{t-1}, a_{t-2}, \ldots, a_1, a_0)
\]

$t$ Pt/value pairs

Polynomial Interpolation

$t$ Coefficients

To share secret $s$ (here $0 \leq s < p$):

Let $y_0 = a_0 = s$

Pick $a_1, a_2, \ldots, a_{t-1}$ at random from $\mathbb{Z}_p$

Let share $s_i = (i, y_i)$ where $y_i = f(i)$.\text{\textsf{Evaluation is easy.}}
Interpolation

Given \((x_i, y_i)\) \(1 \leq i \leq t\) (\(w\)log)

Then \(f(x) = \sum_{i=1}^{t} f_i(x) \cdot y_i\)

where \(f_i(x) = \begin{cases} \frac{1}{\prod_{j \neq i} (x-x_j)} & \text{at } x=x_i \\ 0 & \text{for } x=x_j, j \neq i, 1 \leq j \leq t \end{cases}\)

Furthermore:

\(f_i(x) = \frac{\prod_{j \neq i} (x-x_j)}{\prod_{j \neq i} (x_i-x_j)}\)

This is a polynomial of degree \(t-1\). So \(f\) also has degree \(t-1\).

Evaluating \(f(0)\) to get \(s\) simplifies to

\[s = f(0) = \sum_{i=1}^{t} y_i \cdot \frac{\prod_{j \neq i} (-x_j)}{\prod_{j \neq i} (x_i-x_j)}\]

Theorem: Secret sharing with Shamir's method is information-theoretically secure. Adversary with \(< t\) shares has no information about \(s\).

Pf: A degree \(t-1\) curve can go through any point \((0, s)\)

as well as any given \(d\) pts \((x_i, y_i)\), if \(d < t\).

Refs: Reed-Solomon codes, erasure codes, error correction, information dispersal (Rabin).
Block ciphers:

\[
\begin{align*}
\text{key } K & \rightarrow \text{Enc} \\
& \quad \downarrow \\
& \quad C \\
& \quad \text{plaintext block} \\
& \quad \text{ciphertext block}
\end{align*}
\]

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

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

Ideal block cipher:

For each key \( K \), mapping \( \text{Enc}(K, \cdot) \) is a random independent permutation of message/ciphertext space to itself.

(Similar to RO model for hash fns.)
"Data Encryption Standard"
Standardized in 1976. Now deprecated in favor of AES.

"Feistel structure":

\[
\begin{align*}
L_0 & \rightarrow F \rightarrow K_1 & \text{plaintext 64 bits} \\
R_0 & \rightarrow -32 & \\
L_1 & \rightarrow F \rightarrow K_1 & \text{all 16 round keys derived from 64-bit encryption key (only 56 bits are really used) via "key schedule"}
\end{align*}
\]

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:

\[
\begin{align*}
M & \rightarrow M + A \\
\rightarrow \text{DES} & \rightarrow C \\
\rightarrow \text{DES} & \rightarrow C + \delta \\
2^{47} \text{ chosen pairs (Biham/Shamir)}
\end{align*}
\]

Subject to linear attacks:

\[
\begin{align*}
e.g., \text{if } M_3 \oplus M_15 \oplus C_6 \oplus K_{14} = 0 \quad (e.g. 0-bits) \\
\text{with prob } p = \frac{1}{2} + \varepsilon
\end{align*}
\]

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