Differential Cryptanalysis
&
Linear Cryptanalysis

Differential Cryptanalysis

- one of the most significant recent (public) advances in cryptanalysis
- known by NSA in 70's cf DES design
- Murphy, Biham & Shamir published in 90’s
- powerful method to analyse block ciphers
- used to analyze most current block ciphers with varying degrees of success
- DES reasonably resistant to it, cf Lucifer

Differential Cryptanalysis

- a statistical attack against Feistel ciphers
- design of S-P networks has output of function *f* influenced by both input & key
- hence cannot trace values back through cipher without knowing value of the key
- differential cryptanalysis compares two related pairs of encryptions (differential)
- Differential Cryptanalysis compares two related pairs of encryptions, which can leak information about the key, given a sufficiently large number of suitable pairs.

Differential Cryptanalysis Compares Pairs of Encryptions

- Differential cryptanalysis compares two related pairs of encryptions
- with known difference in the input $m_0 \| m_1$
- searching for a known difference in output
- when same subkeys are used

$$\begin{aligned}\Delta m_{i+1} &= m_{i+1} \oplus m'_{i+1} \\ &= [m_{i-1} \oplus \mathrm{f}(m_i, K_i)] \oplus [m'_{i-1} \oplus \mathrm{f}(m'_i, K_i)] \\ &= \Delta m_{i-1} \oplus [\mathrm{f}(m_i, K_i) \oplus \mathrm{f}(m'_i, K_i)]\end{aligned}$$

Differential Cryptanalysis

- have some input difference giving some output difference with probability p
- if find instances of some higher probability input / output difference pairs occurring
- can infer subkey that was used in round
- then must iterate process over many rounds (with decreasing probabilities)

Linear Cryptanalysis

- another fairly recent development
- also a statistical method
- must be iterated over rounds, with decreasing probabilities
- developed by Matsui et al in early 90's
- based on finding linear approximations
- can attack DES with 2^{43} known plaintexts, easier but still in practice infeasible

Linear Cryptanalysis

- The objective of linear cryptanalysis is to find an effective linear equation relating some plaintext, ciphertext and key bits that holds with probability p<>0.5
- find linear approximations with prob p != ½

$$P[i_1, i_2, \ldots, i_a] \oplus C[j_1, j_2, \ldots, j_b] = K[k_1, k_2, \ldots, k_c]$$

- gives linear equation for key bits
- get one key bit using max likelihood alg
- using a large number of trial encryptions

Summary

- have considered:
  - Differential Cryptanalysis
  - Linear Cryptanalysis