Cryptography

Lecture 16

Announcements

- HW5 due today
- HW6 due Wednesday 4/10
- New Office: IRB 5238

Agenda

- Last time
  - Practical constructions of Stream Ciphers (K/L 6.1)
  - SPN (K/L 6.2)

- This time
  - Current Events
  - Go over RC4 Class Exercise
  - Finish up SPN (K/L 6.2)
  - Feistel Networks (K/L 6.2)

Attacking Reduced-Round SPN

One-round SPN: 64-bit block length. S-boxes with 8-bit input. Independent, 64-bit subkeys.

First attempt at attack:
- Given an input/output pair (x, y)
- Enumerate over all possible values for the second-round subkey k_2.
- For each such value, invert the final key-mixing step to get a candidate output y'
- Given (x, y') first-round subkey k_1 is determined.
- Use additional input-output pairs to determine the correct $(k_1||k_2)$ pair.

How long does this attack take?

Attacking Reduced-Round SPN

One-round SPN: 64-bit block length. S-boxes with 8-bit input. Independent, 64-bit subkeys.

Improved attack—work byte-by-byte:
- Given an input/output pair (x, y)
- Enumerate over all possible values for the 8 bit positions corresponding to the output of the first S-box for the second-round subkey k_2.
- For each such value, invert the final key-mixing step to get a candidate 8-bit output y'
- Given (x, y') the first 8-bits of the first-round subkey k_1 are determined.
- Construct a table of 2^8 possible key values for each block of 8-bits of k_1, k_2.
- Use additional input-output pairs to determine the correct 8-bits of k_1 and first byte of k_2.

How long does this attack take? $8 \cdot 2^8 = 2^{11}$.

Can be improved: Use additional input/output pairs. Incorrect pair $(k_1||k_2)$ will work on two pairs with probability 2^{-8}. Can use small number of input/output pairs to narrow down all tables to a single value each at which point the entire master key is known. In expectation, a single additional pair will reduce each table to a single consistent key value.

Lessons Learned

It should not be possible to work independently on different parts of the key.

More diffusion is required. More rounds are necessary to achieve this.

Feistel Networks
An alternative approach to Block Cipher Design

Feistel Networks

- The underlying round functions do not need to be invertible.
- Feistel network allows us to construct an invertible function from non-invertible components.
- With enough rounds, can construct a PRP from a PRF

(Balanced) Feistel Network

- The ith round function $\hat{f}_i$ takes as input a sub-key k_i and an $\ell/2$-bit string and outputs a $\ell/2$-bit string.
- Master key k is used to derive sub-keys for each round.
- Note that the round functions $\hat{f}_i$ are fixed and publicly known, but the $f_i(R) \coloneqq \hat{f}_i(k_i, R)$ depend on the master key and are not known to the attacker.

i-th Feistel Round

- If the block length of the cipher is ℓ bits, then L_{i-1} and R_{i-1} each has length $\ell/2$.
- The output (L_i, R_i) of the round is:

  $L_i := R_{i-1}$ and $R_i := L_{i-1} \oplus f_i(R_{i-1})$

A three-round Feistel Network

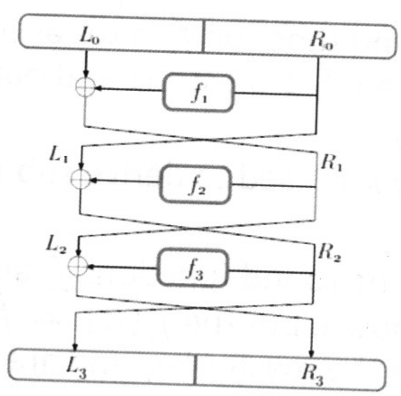

FIGURE 6.4: A 3-round Feistel network.

Feistel Networks are invertible

Proposition: Let F be a keyed function defined by a Feistel network. Then regardless of the round functions $\{\hat{f}_i\}$ and the number of rounds, F_k is an efficiently invertible permutation for all k.