Introduction to Cryptology

Lecture 16

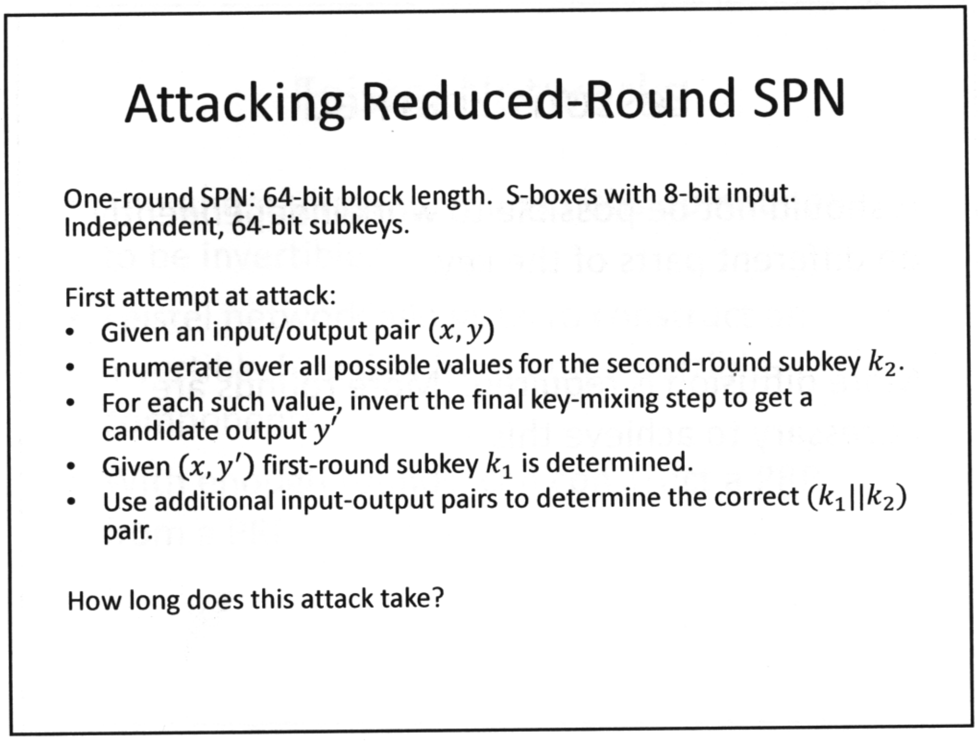
Announcements

- HW6 due today
- HW7 due Thursday 4/12
- Sign up for Extra Credit Opportunity
  - Link to sign up sheet sent in a Canvas announcement
  - See instructions on course webpage
  - Due on last day of class.

Agenda

- Last time
  - Finished RC4 (K/L 6.1)
  - SPN (K/L 6.2)

- This time
  - Finish up SPN (K/L 6.2)
  - Feistel Networks (K/L 6.2)
  - More details on AES/DES (K/L 6.2)



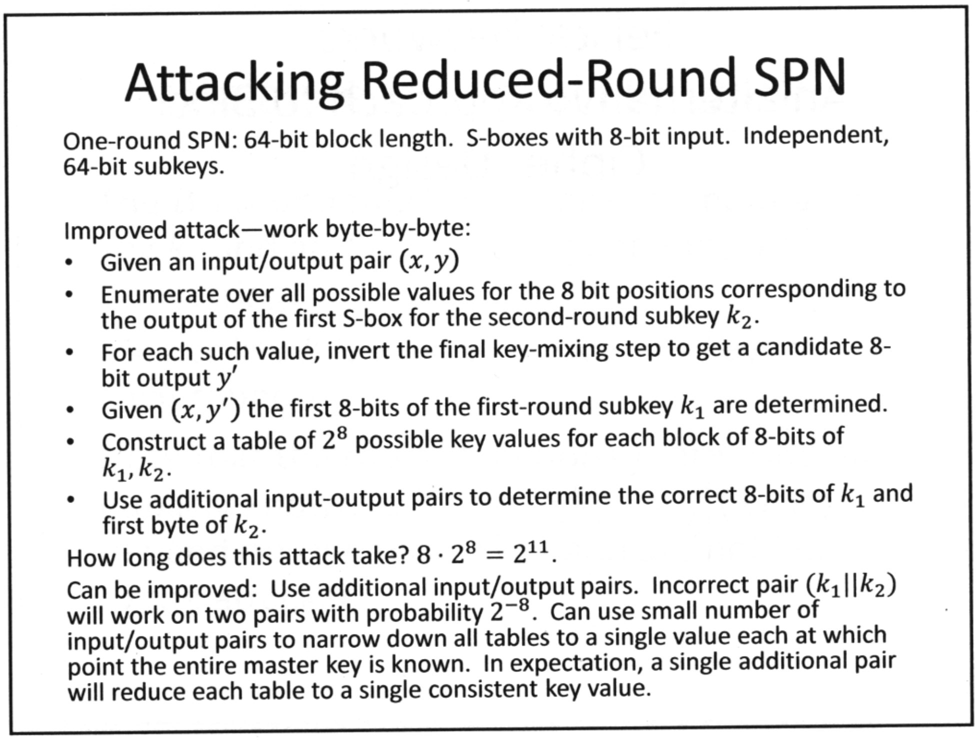
Attacking Reduced-Round SPN

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

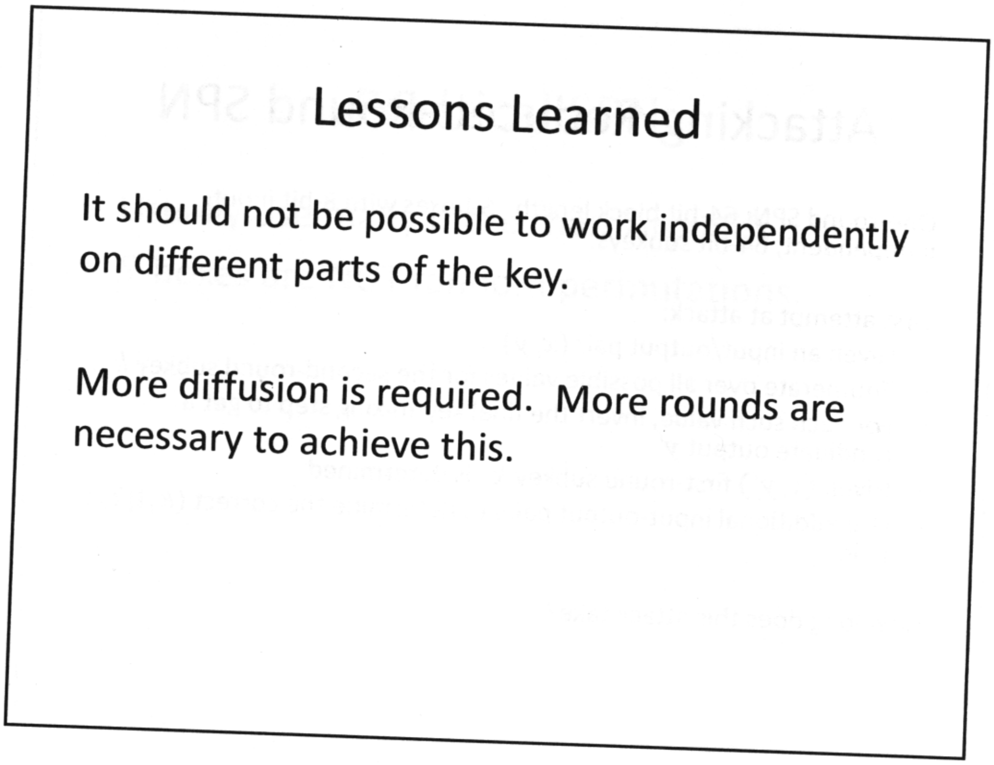
One-round SPN: 64-bit block length. S-boxes with 8-bit input. Independent, 64-bit subkeys.

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? $8 \cdot 2^8 = 2^{11}$.

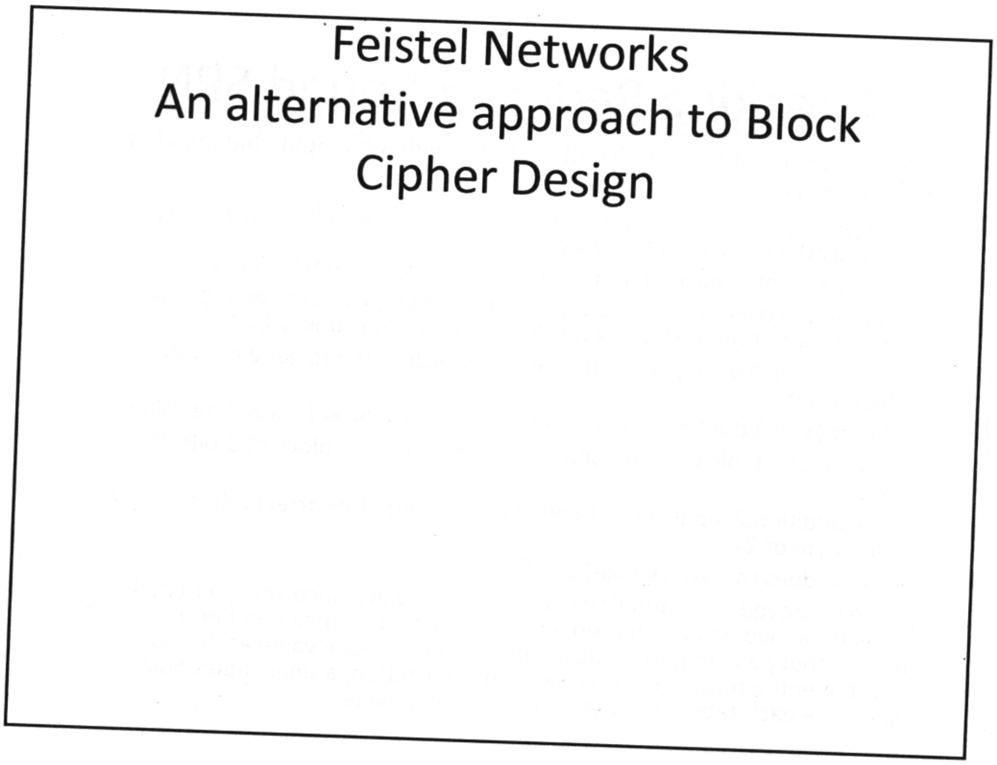
Can be improved: Use additional input/output pairs. Incorrect pair $(k_1 || k_2)$ will work on two pairs with probability 2^{-8}. Can use small number of input/output pairs to narrow down all tables to a single value each at which point the entire master key is known. In expectation, a single additional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



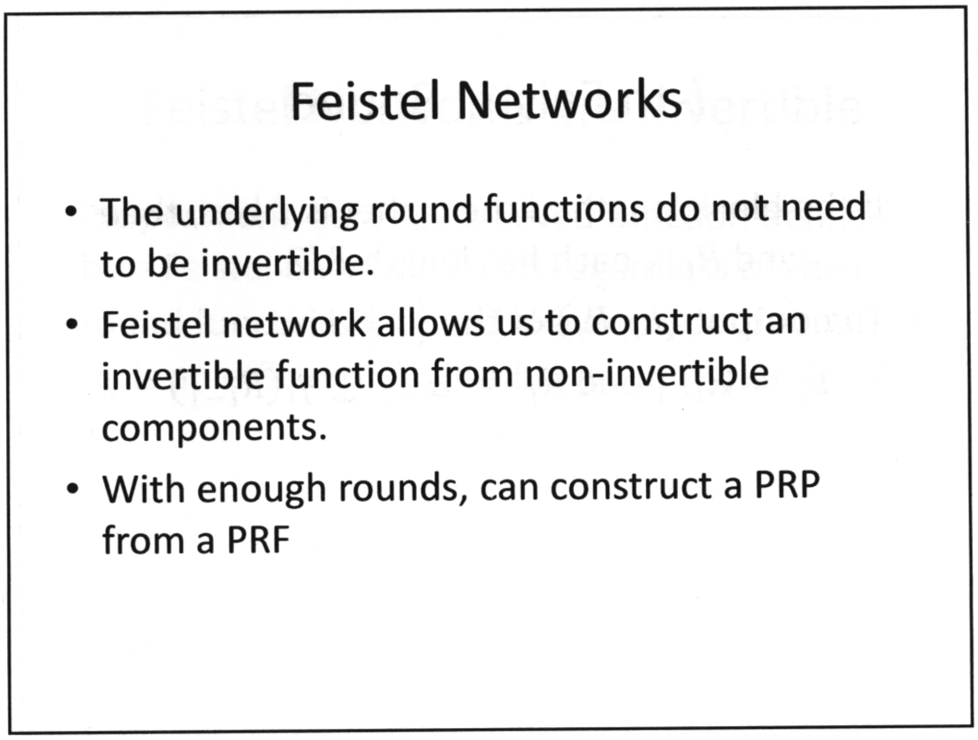
Lessons Learned

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.

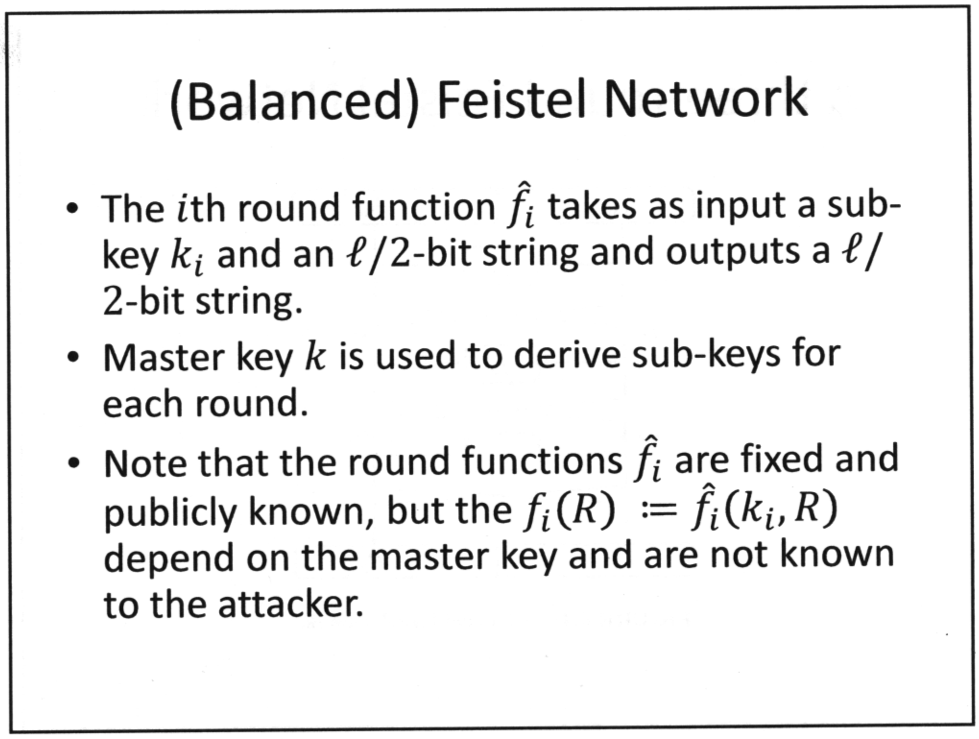


Feistel Networks An alternative approach to Block Cipher Design



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:

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

A three-round Feistel Network

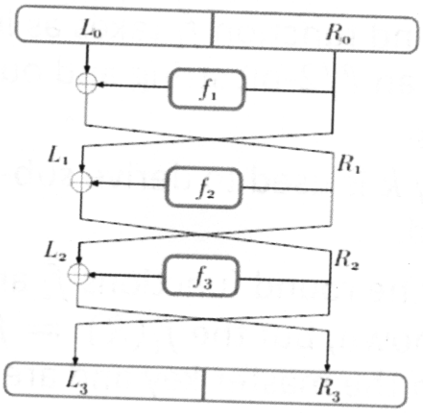
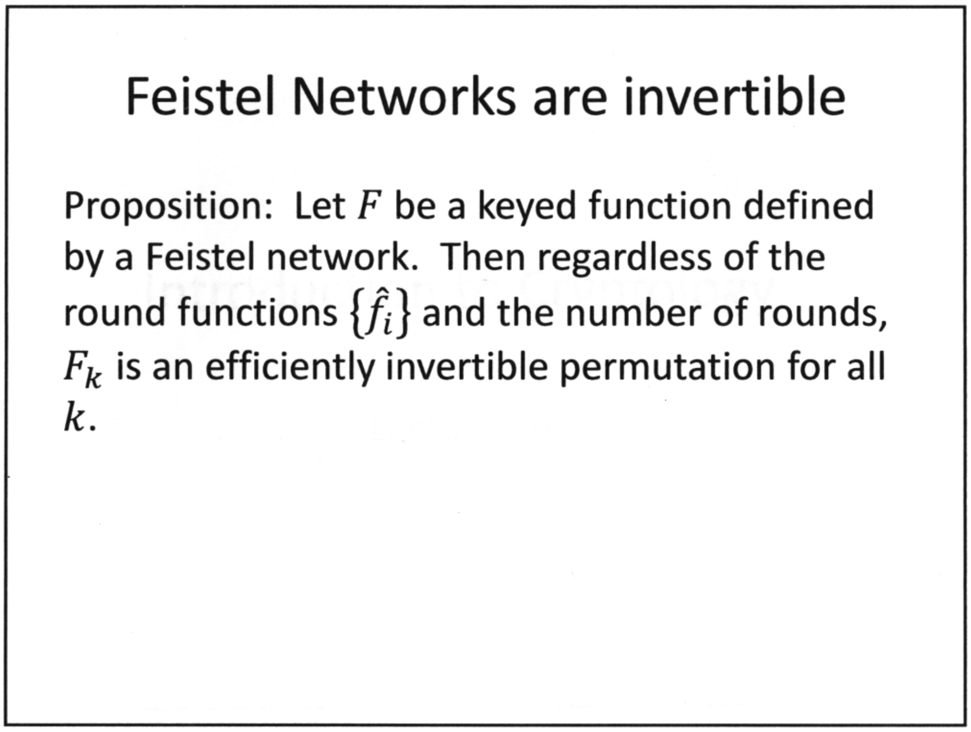


FIGURE 6.4: A 3-round Feistel network.



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.

Details on DES

- The Data Encryption Standard was developed in the 1970s by IBM (with help from the National Security Agency), and adopted in 1977 as a Federal Information Processing Standard for the US.
- DES is no longer considered secure due to its short key length of 56 bits which makes it vulnerable to brute-force attacks.
- It remains in wide use today in the strengthened form of triple-DES, described in Section 6.2.4.
- DES is of great historical significance. It has undergone intensive scrutiny within the cryptographic community, arguably more than any other cryptographic algorithm in history. The common consensus is that, relative to its key length, DES is an extremely well designed cipher.
  - To date, the best known attack on DES in practice is an exhaustive search over all 2^{56} possible keys.

Details on DES

- The DES block cipher is a 16-round Feistel network with a block length of 64 bits and a key length of 56 bits. The same round function $\hat{f}$ is used in each of the 16 rounds.
- Round function takes a 48-bit sub-key and, as in a (balanced) Feistel network, a 32-bit input
- The key schedule of DES is used to derive a sequence of 48-bit sub-keys $k_1, \ldots, k_{16}$ from the 56-bit master key.

Details on DES

- The DES round function $\hat{f}$—the DES mangler function—is constructed using a 1-round substitution-permutation network
- S-boxes are not permutations!!
  - Map 6-bit inputs to 4-bit outputs.

Details on DES

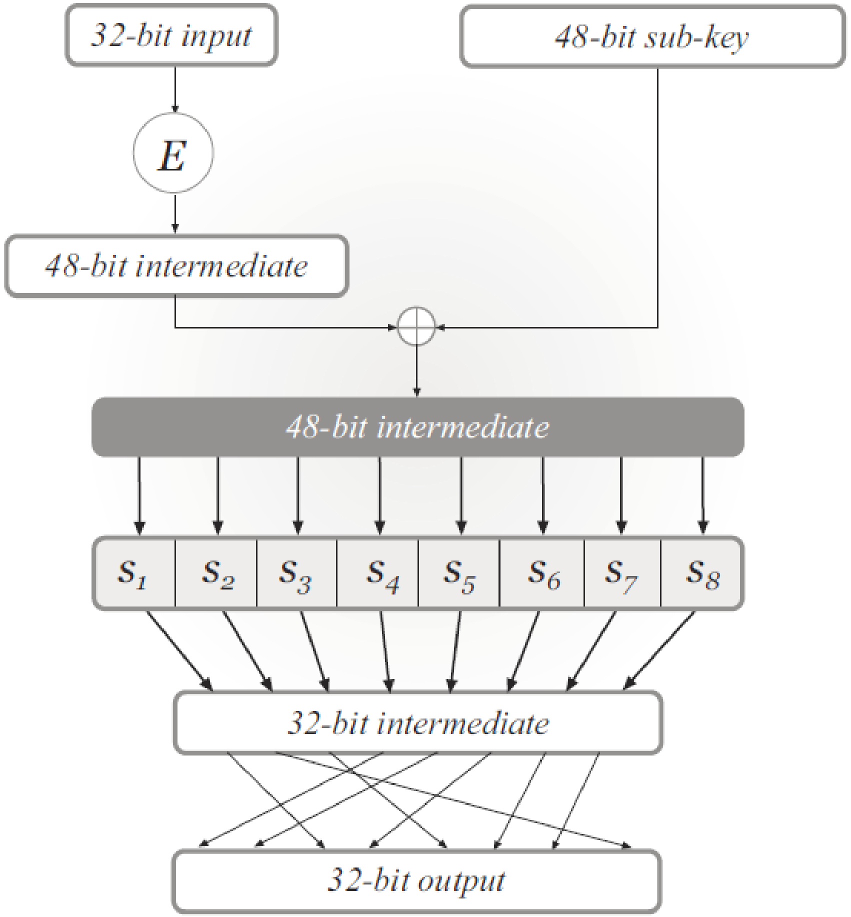


FIGURE 6.5: The DES mangler function.

3DES (Triple Encryption)

- First Idea: increase the key length by doing a double-encryption, thereby increasing complexity of brute-force attack from 2^{56} to 2^{112}.
- Let F be a block-cipher with an n-bit key length and ℓ-bit block length.
  - Define the following block cipher with $2n$-bit key: $F'_{k_1,k_2}(x) \coloneqq F_{k_2}(F_{k_1}(x))$
- Problem: Meet in the middle attack

Meet in the Middle Attack on Double DES

Adversary is given a single input/output pair (x, y) where $y = F_{k^*_1, k^*_2}(x)$ for unknown k_1, k_2. The adversary does the following:

- For each $k_1 \in \{0,1\}^n$, compute $z := F_{k_1}(x)$ and store (z, k_1) in a list L.
- For each $k_2 \in \{0,1\}^n$, compute $z := {F_{k_2}}^{-1}(y)$ and store (z, k_2) in a list L'.
- Sort L and L', respectively, by their first components.
- Entries $(z_1, k_1) \in L$ and $(z_2, k_2) \in L'$ are a match if $z_1 = z_2$. For each match of this sort, add (k_1, k_2) to a set S.

Expected number of elements in S is $2^{2n-\ell}$. Can use a few more input/output pairs to reduce to a single (k_1, k_2) .

Triple DES

Two variants:

- $F'_{k_1,k_2,k_3}(x) \coloneqq F_{k_3}({F_{k_2}}^{-1}(F_{k_1}(x)))$
- $F'_{k_1,k_2}(x) \coloneqq F_{k_1}({F_{k_2}}^{-1}(F_{k_1}(x)))$

- Middle cipher is reversed for backwards compatibility: setting $k_1 = k_2 = k_3$ results in a single invocation of F using key k_1.

Security of Triple-DES

- Security of the first variant: The cipher is susceptible to a meet-in-the-middle attack just as in the case of double encryption, though the attack now takes time 2^{2n}. This is the best known attack.
- Security of the second variant. There is no known attack with time complexity better than 2^{2n} when the adversary is given only a small number of input/output pairs. Thus, two-key triple encryption is a reasonable choice in practice.

Disadvantage of both Triple-DES variants: Fairly slow since it requires 3 invocations of DES.