COMP 3704 Computer Security

Christian Grothoff
christian@grothoff.org

http://grothoff.org/christian/

Design Criteria for Block Ciphers

- Algorithm must have "high level of security"
- Algorithm must be completely specified and easy to understand
- Security must reside in key, not secrecy of algorithm
- Algorithm must be widely available
- Algorithm must be efficient to use
- Algorithm must be economically implementable
- Algorithm must be validated

Feistel Networks

Feistel networks combine multiple rounds of repeated operations, primarily:

- Permutation
- Substitution
- XOR

These operations are used to implement a function f.

Feistel Networks: Encryption

Given f and a key K, the plaintext is split into two halves L_0 and R_0. The main computation is then

$$L_i := R_{i-1} \tag{1}$$

$$R_i := L_{i-1} \oplus f(R_{i-1}, K_i) \tag{2}$$

producing ciphertext L_n and R_n after n rounds.

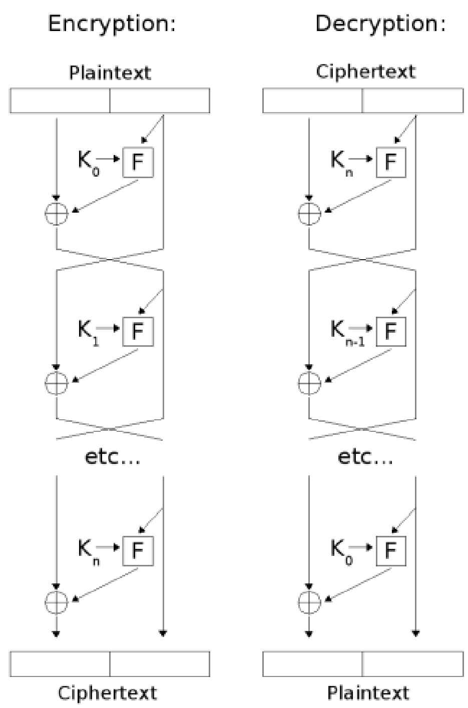
Feistel Networks: Decryption

Decryption is accomplished as follows:

$$R_{i-1} := L_i \tag{3}$$

$$L_{i-1} := R_i \oplus f(L_i, K_i). \tag{4}$$

Feistel Networks: Illustration

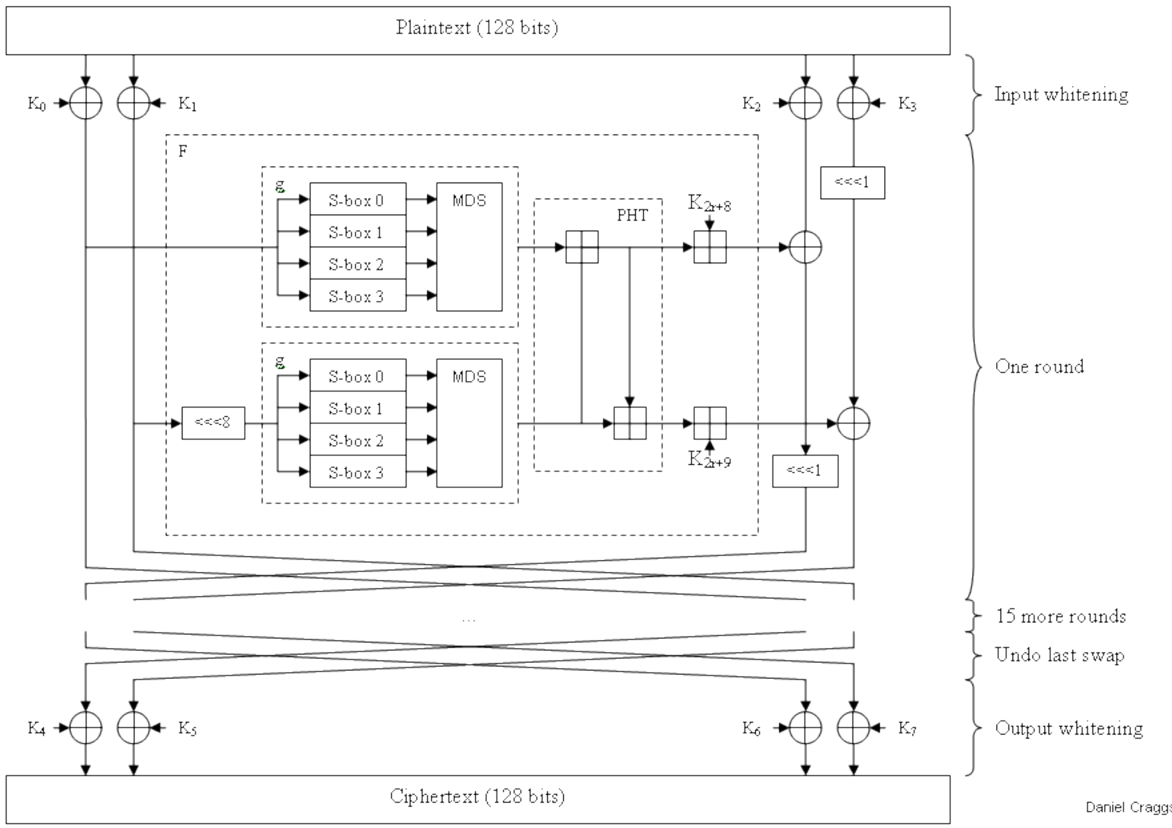


Feistel Cipher

Block Cipher Rounds

- Individual rounds are insufficient to hide patterns
- More rounds allow more key bits
- Re-use of (similar) rounds allows re-use of hardware
- Most algorithms use 16 or more rounds

Example: Twofish



Confusion and Diffusion

The goal of **confusion** is to make the mapping between plaintext, key and ciphertext complex.

The goal of **diffusion** is to hide statistical properties of the plaintext.

The **strict avalance criterion** for diffusion says that flipping one bit in the plaintext changes each output bit with probability $\frac{1}{2}$.

S-Boxes

- Replace one plaintext symbol by another (confusion).
- S = substitution
- Substitution alone achieves little security.
- Some substitutions can be implemented efficiently using modular multiplication.
- Number of output bits maybe smaller than number of input bits (for example, DES has 6-4 S-Boxes).

P-Boxes

- Permutate symbols in the input text.
- Achieves diffusion of statistical properties.
- Permutation alone achieves little security.

S-Box Design Criteria

- Avoid proximity to linear function between input and output
- If an input changes by one bit, at least two bits in the output should change (ideally half)
- Differences between multiple inputs should not result in similar differences in the outputs

P-Box Design Criteria

- Maximize distribution of outputs from one S-Box over inputs into next round of S-boxes
- Change bit-positions between inputs and outputs of S-Boxes

Weak Keys

- Certain keys prevent confusion and diffusion
- Which keys are insecure depends on f
- Often practically impossible to encounter for randomly generated keys with large keysize
- Some cryptography libraries check for weak keys
- Examples for DES are in the book, pages 281-282

Differential Cryptoanalysis

- Analysis of ciphertext pairs where plaintext has particular differences (for example, using XOR)
- Based on ciphertext differences, assign probabilities to candidate keys
- Requires known (or better: chosen) plaintext
- Attack is purely theoretical for good block ciphers

Linear Cryptoanalysis

- XOR certain bits of plaintext and ciphertext
- Result will be XOR of certain key bits with a certain probability
- If probability is $> 50\%$ for a given cipher, this can be used to narrow down the keyspace (given enough data)
- Attack depends on structure of S-Boxes
- Attack requires far too much plaintext to be practical for good block ciphers

Common Block Ciphers

- DES
- IDEA
- Blowfish
- Rijndael/AES

Meet-in-the-middle Attack

Suppose the cipher is:

$$C = E_{K_1}(E_{K_2}(P)) \tag{5}$$

Assume attacker knows P and C so that (5) holds.

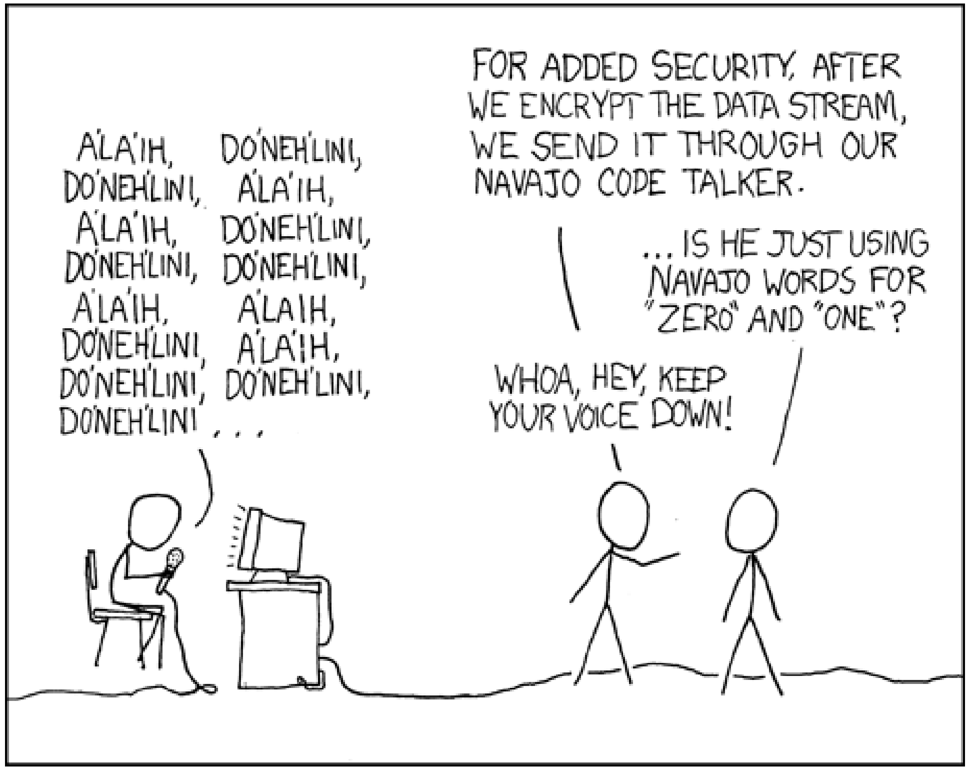
- Brute force would take 2^{2n} attempts for $|K_1| = |K_2| = n$
- Meet-in-the-middle computes $E_K(P)$ and $D_K(C)$ for all possible keys K and finds $E_{K_2}(P) = M = D_{K_1}(C)$
- Uses 2^{n+1} encryptions and $O(2^n)$ space

Triple-Encryption

$$C = E_{K_1}(D_{K_2}(E_{K_1}(M))) \tag{6}$$

- Doubles key size: $K = (K_1, K_2)$
- Resists meet-in-the-middle attack
- Example: 3des
- Alternative: use stronger cipher!

Cascading of Multiple Algorithms



Cascading of Multiple Algorithms

What about encrypting the ciphertext with yet another cipher?

- If the same key is used, resulting security maybe that of the *weakest* algorithm (depending on attacker model)
- If independent keys are used, resulting security should be at least as strong as the *strongest* algorithm

However, remember that for many systems, the security problems are not related to the cipher!

Questions

?

Problem

The description of the non-interactive zero-knowledge proof in section 5.1, page 107 is not precise. What exactly does Peggy commit to in step 2? What do Victor or Carol verify in step 6?

Problem

What are the contents of the messages unblinded by the bank in step 3 in the protocol #4 on page 142-144 in the textbook? What are the precise checks performed by the bank?

Note that the description in the textbook is not entirely correct (or precise). Fill in the gaps to make the protocol secure.