Cryptography IV: Block Ciphers

Noah Singer

Montgomery Blair High School Cybersecurity Team

March 29, 2017

Message indistinguishability

1. Adversary submits two plaintexts m_0 and m_1 to challenger.
2. Challenger selects $b \in \{0, 1\}$ at random and finds $C = E(m_b, k)$ for key k.
3. Adversary guesses the value of b from C.

Definition (Advantage (symmetric cryptosystems))

For some adversary A, $Adv(A) = |P(A(m_b) = b) - \frac{1}{2}|$.

Definition (Semantic security (symmetric cryptosystems))

A symmetric cryptosystem is **semantically secure** iff there exists no adversary A with non-negligible advantage.

Product ciphers

Definition (Product cipher)

A cipher that consists of several simpled units chained together.

Product ciphers generally have algorithms called **key schedules** that expand the **master key** into several smaller **subkeys** for each **round**.

Confusion: relationship between ciphertext and key as complex as possible

Diffusion: non-uniformities in plaintext are spread over ciphertext structure

Block ciphers

Definition (Block cipher)

A cipher that splits the plaintext into a series of fixed-length *blocks* and then encrypts each individually.

To encrypt ciphertexts that are longer than one block, a cipher **mode of operation** must be used. To encrypt ciphertexts that aren't a multiple of the block size, a **padding scheme** must be used.

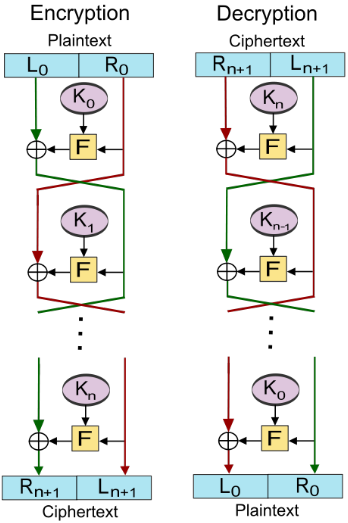
Feistel ciphers

- Popular in algorithms like DES
- Require a one-way function F (how to actually find this is a topic for another lecture)
- Also called the **Luby-Rackoff construction**
- Encryption and decryption are essentially identical

Given a master key K and a one-way function F,

1. Split K into n round keys $K_0, K_1, \ldots, K_{n-1}$
2. Split plaintext in halves into (L_0, R_0).
3. For any i, let $L_{i+1} = R_i$ and $R_{i+1} = L_i \oplus F(R_i, K_i)$.

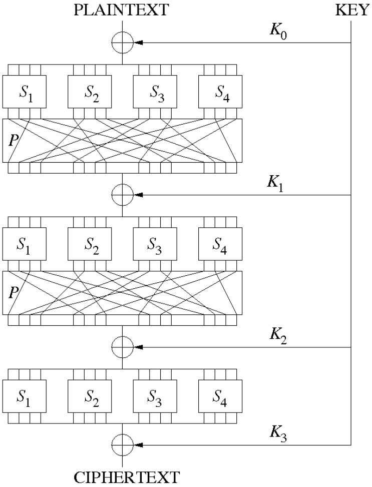
Diagram


Encryption
Plaintext
L_0
R_0
K_0
F
K_1
F
K_n
F
R_{n+1}
L_{n+1}
Ciphertext
Decryption
Ciphertext
R_{n+1}
L_{n+1}
K_n
F
K_{n-1}
F
K_0
F
L_0
R_0
Plaintext

Substitution-permutation networks

- The basis for most modern block ciphers, like AES
- Alternating layers of *P-boxes* and *S-boxes*
- *P-boxes* permute the bits, while *S-boxes* substitute one set of bits for another in an invertible function
- *S-boxes* must satisfy the *avalanche effect*: changing one bit should change roughly half the bits of the result
- Similar to a series of consecutive substitution and transposition ciphers

Diagram


PLAINTEXT
KEY
K_0
S_1
S_2
S_3
S_4
P
K_1
S_1
S_2
S_3
S_4
P
K_2
S_1
S_2
S_3
S_4
K_3
CIPHERTEXT