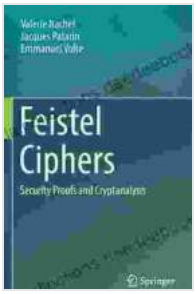
Feistel Ciphers: Security Proofs and Cryptanalysis

Feistel ciphers are a class of block ciphers that are widely used in cryptography. They were first introduced by Horst Feistel in 1973, and have since been used in a variety of applications, including the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES).



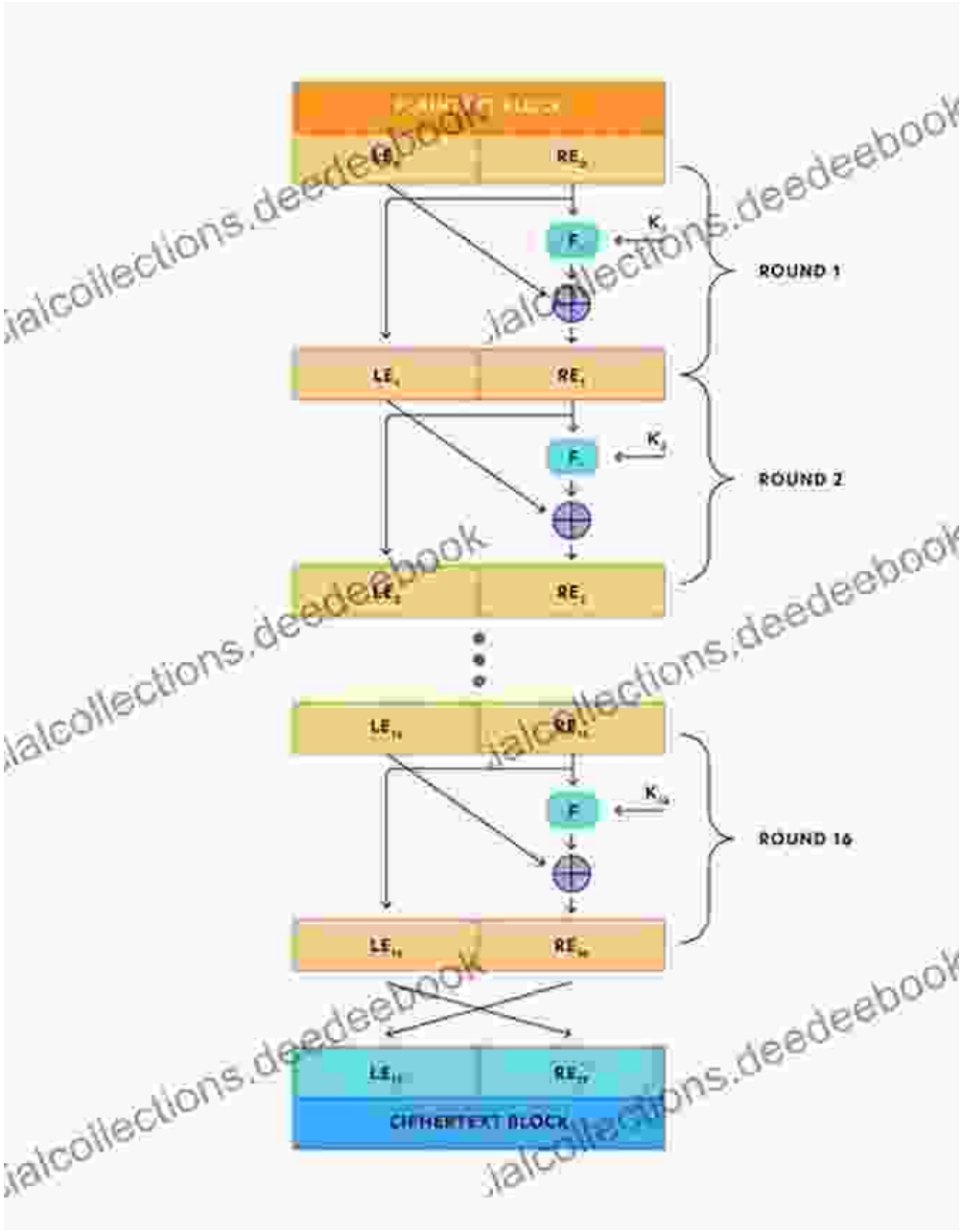
Feistel Ciphers: Security Proofs and Cryptanalysis

by George Borrow

★★★★★ 5 out of 5

Language	: English
File size	: 11967 KB
Text-to-Speech	: Enabled
Screen Reader	: Supported
Enhanced typesetting	: Enabled
Print length	: 519 pages
Paperback	: 132 pages
Item Weight	: 7.1 ounces
Dimensions	: 5.63 x 0.47 x 8.9 inches

Feistel Cipher Structure



A Feistel cipher consists of a number of rounds, each of which consists of two sub-rounds. In each sub-round, the input block is divided into two halves, and each half is processed by a separate function. The outputs of the two sub-rounds are then combined to form the input to the next round.

The key schedule for a Feistel cipher is typically generated from the secret key using a key expansion algorithm. The key expansion algorithm is

designed to produce a different key for each round of the cipher.

Security Proofs

There are a number of security proofs that have been developed for Feistel ciphers. These proofs show that Feistel ciphers are resistant to a variety of cryptanalytic attacks, including differential cryptanalysis, linear cryptanalysis, and impossible differential cryptanalysis.

Differential cryptanalysis

Differential cryptanalysis is a cryptanalytic technique that exploits the differences between the outputs of a cipher for two different inputs. In order to be resistant to differential cryptanalysis, a cipher must have a high diffusion rate. This means that the output of the cipher should be highly sensitive to changes in the input.

Feistel ciphers have a high diffusion rate because the input block is divided into two halves in each round, and each half is processed by a separate function. This means that any change in the input block will propagate through the cipher in a complex way, making it difficult to predict the output.

Linear cryptanalysis

Linear cryptanalysis is a cryptanalytic technique that exploits the linear relationships between the input and output of a cipher. In order to be resistant to linear cryptanalysis, a cipher must have a low linearity. This means that the output of the cipher should not be linearly related to the input.

Feistel ciphers have a low linearity because the two sub-rounds in each round are independent of each other. This means that the output of the

cipher is not simply a linear combination of the inputs to the two sub-rounds.

Impossible differential cryptanalysis

Impossible differential cryptanalysis is a cryptanalytic technique that exploits the fact that certain combinations of inputs and outputs are impossible for a given cipher. In order to be resistant to impossible differential cryptanalysis, a cipher must have a high probability of producing all possible outputs.

Feistel ciphers have a high probability of producing all possible outputs because the two sub-rounds in each round are independent of each other. This means that the output of the cipher is not simply a deterministic function of the input.

Cryptanalysis

Despite the security proofs that have been developed for Feistel ciphers, there have been a number of successful cryptanalytic attacks on Feistel ciphers. These attacks have shown that Feistel ciphers are not perfect, and that they can be broken with sufficient effort.

Weak key attacks

Weak key attacks are cryptanalytic attacks that exploit weaknesses in the key schedule of a cipher. These attacks can be used to recover the secret key from a known plaintext-ciphertext pair.

Feistel ciphers are particularly vulnerable to weak key attacks because the key schedule is typically generated from the secret key using a simple

algorithm. This makes it possible for an attacker to find weak keys by brute force.

Related-key attacks

Related-key attacks are cryptanalytic attacks that exploit the relationships between different keys. These attacks can be used to recover the secret key from a known plaintext-ciphertext pair, even if the keys are not related in a known way.

Feistel ciphers are particularly vulnerable to related-key attacks because the key schedule is typically generated from the secret key using a simple algorithm. This makes it possible for an attacker to find related keys by brute force.

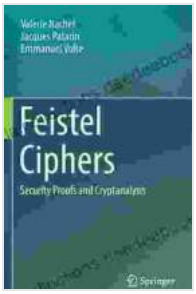
Side-channel attacks

Side-channel attacks are cryptanalytic attacks that exploit information that is leaked from the implementation of a cipher. These attacks can be used to recover the secret key from a known plaintext-ciphertext pair, even if the cipher is implemented correctly.

Feistel ciphers are particularly vulnerable to side-channel attacks because they are often implemented in software. This makes it possible for an attacker to use timing attacks or power analysis to extract information about the secret key.

Feistel ciphers are a widely used class of block ciphers that are resistant to a variety of cryptanalytic attacks. However, there have been a number of successful cryptanalytic attacks on Feistel ciphers, and it is important to be

aware of these attacks when using Feistel ciphers in cryptographic applications.

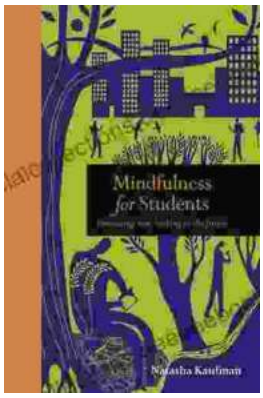


Feistel Ciphers: Security Proofs and Cryptanalysis

by George Borrow

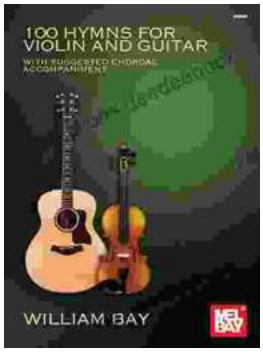
★★★★★ 5 out of 5

Language	: English
File size	: 11967 KB
Text-to-Speech	: Enabled
Screen Reader	: Supported
Enhanced typesetting	: Enabled
Print length	: 519 pages
Paperback	: 132 pages
Item Weight	: 7.1 ounces
Dimensions	: 5.63 x 0.47 x 8.9 inches



Embracing Now: Embark on a Mindfulness Journey for a Fulfilling Future

In a world characterized by constant distraction, stress, and anxiety, mindfulness has emerged as a beacon of hope for those seeking inner...



100 Hymns for Violin and Guitar: A Comprehensive Guide to Inspiring Melodies

The violin and guitar are two of the most versatile and expressive musical instruments. When combined, they create a rich and evocative sound that is...