CS553 Cryptography

BitBees

Question 1

Question 1

The encryption processes uses both the Feistel structure and SPN structure consist of multiple rounds of processing of the plaintext, each round consisting of a "substitution" step followed by a permutation step. Difference lies in how the data flows from one layer to the next.

Feistel Networks

In **Feistel Networks**, the input block to each round is divided into two halves that can be denoted as L and R for the left half and the right half. In each round, the right half of the block, R, goes through unchanged. But the left half, L, goes through an operation that depends on R and the encryption key. First, we apply an encrypting function 'f' that takes two input the key K and R. The function produces the output f(R,K). Then, we XOR the output of the mathematical function with L.
Here are some examples:

DES

Like everyone and everything, this was the father of all ciphers, until it wasn't. The Data Encryption Standard used a Feistel network. It was developed in the early 1970s at IBM and based on an earlier design by Horst Feistel.
Block Length: 64 bits
Key Length: 56 bits
Rounds: 16

Blowfish

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in many cipher suites and encryption products. Blowfish provides a good encryption rate in software, and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives

more attention, and Schneier recommends Twofish for modern applications.
Block Length: 64 bits
Key Length: 32-448 bits
Rounds: 16

Lucifer

Lucifer uses a combination of transposition and substitution crypting as a starting point in decoding ciphers. Lucifer was the name given to several of the earliest civilian block ciphers, developed by Horst Feistel and his colleagues at IBM. Lucifer was a direct precursor to the Data Encryption Standard.
Block Length: 48, 32, 128 bits
Key Length: 48, 64, 128 bits
Rounds: 16

LOKI97

LOKI97 is a block cipher which was a candidate in the Advanced Encryption Standard competition. It is a member of the LOKI family of ciphers, with earlier instances being LOKI89 and LOKI91. LOKI97 was designed by Lawrie Brown, assisted by Jennifer Seberry and Josef Pieprzyk.
Block Length: 128 bits
Key Length: 128, 192, 256 bits
Rounds: 16

Camellia

Camellia is a symmetric key block cipher jointly developed by Mitsubishi Electric and NTT of Japan. The cipher was designed to be suitable for both software and hardware implementations, from low-cost smart cards to high-speed network systems. It is part of the Transport Layer Security (TLS) cryptographic protocol designed to provide communications security over a computer network such as the Internet.
Block Length: 128 bits
Key Length: 128, 192, 256 bits
Rounds: 18 or 24

SP-Networks

AES

The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES is available in many different encryption packages, and is the first (and only) publicly accessible cipher approved by the U.S. National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module.
Block Length: 128 bits
Key Length: 128, 192, 256 bits
Rounds: 10, 12, 14

Kuznyechik

Kuznyechik is a symmetric block cipher. It is defined in the National Standard of the Russian Federation GOST R 34.12-2015 and also in RFC 7801. The name of the cipher can be translated from Russian as grasshopper, however, the standard explicitly says that the English name for the cipher is Kuznyechik. The designers claim that by naming the cipher Kuznyechik they follow the trend of difficult to pronounce algorithm names set up by Rijndael and Keccak. :-)

FYI: Kuznyechik is based on a substitution–permutation network, though the key schedule employs a Feistel network.

Block Length: 128 bits
Key Length: 256 bits
Rounds: 10

PRESENT

PRESENT is a lightweight block cipher, developed by the Orange Labs (France), Ruhr University Bochum (Germany) and the Technical University of Denmark in 2007. PRESENT was designed by Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. The algorithm is notable for its compact size (about 2.5 times smaller than AES).
Block Length: 64 bits
Key Length: 80, 128 bits
Rounds: 31

SHARK

In cryptography, SHARK is a block cipher identified as one of the predecessors of Rijndael (the Advanced Encryption Standard). It is a six-round SP-network which alternates a key mixing stage with linear and non-linear transformation layers. The linear transformation uses an MDS matrix representing a Reed–Solomon error correcting code in order to guarantee good diffusion.
Block Length: 64 bits
Key Length: 128 bits
Rounds: 6

Square

In cryptography, Square (sometimes written SQUARE) is a block cipher invented by Joan Daemen and Vincent Rijmen. The design, published in 1997, is a forerunner to Rijndael, which has been adopted as the Advanced Encryption Standard. Square was introduced together with a new form of cryptanalysis discovered by Lars Knudsen, called the "Square attack".
FYI: Square isn't patented.

Block Length: 128 bits
Key Length: 128 bits
Rounds: 8