Cryptography and Network Security

DATA ENCRYPTION STANDARD

Session Meta Data

Author	**Dr T Sree Sharmila**
Reviewer	
Version Number	1.0
Release Date	1 July 2018

Revision History

Revision Date	Details	Version no.
		1.0

Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

Introduction

- one of the most widely used types of cryptographic algorithms
- provide secrecy and/or authentication services
- in particular will introduce DES (Data Encryption Standard)

Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

Block vs Stream Ciphers

- block ciphers process messages into blocks, each of which is then en/decrypted
- like a substitution on very big characters
  - 64-bits or more
- stream ciphers process messages a bit or byte at a time when en/decrypting
- many current ciphers are block ciphers
- hence are focus of course

Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

Block Cipher Principles

- most symmetric block ciphers are based on a **Feistel Cipher Structure**
- needed since must be able to **decrypt** ciphertext to recover messages efficiently
- block ciphers look like an extremely large substitution
- would need table of 2^{64} entries for a 64-bit block
- instead create from smaller building blocks
- using idea of a product cipher

Claude Shannon and Substitution-Permutation Ciphers

- in 1949 Claude Shannon introduced idea of substitution-permutation (S-P) networks
  - modern substitution-transposition product cipher
- these form the basis of modern block ciphers
- S-P networks are based on the two primitive cryptographic operations we have seen before:
  - *substitution* (S-box)
  - *permutation* (P-box)
- provide *confusion* and *diffusion* of message

Confusion and Diffusion

- cipher needs to completely obscure statistical properties of original message
- a one-time pad does this
- more practically Shannon suggested combining elements to obtain:
- **diffusion** – dissipates statistical structure of plaintext over bulk of ciphertext
- **confusion** – makes relationship between ciphertext and key as complex as possible

Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

Feistel Cipher Structure

- Horst Feistel devised the **feistel cipher**
  - based on concept of invertible product cipher
- partitions input block into two halves
  - process through multiple rounds which
  - perform a substitution on left data half
  - based on round function of right half & subkey
  - then have permutation swapping halves
- implements Shannon's substitution-permutation network concept

Feistel Cipher Structure

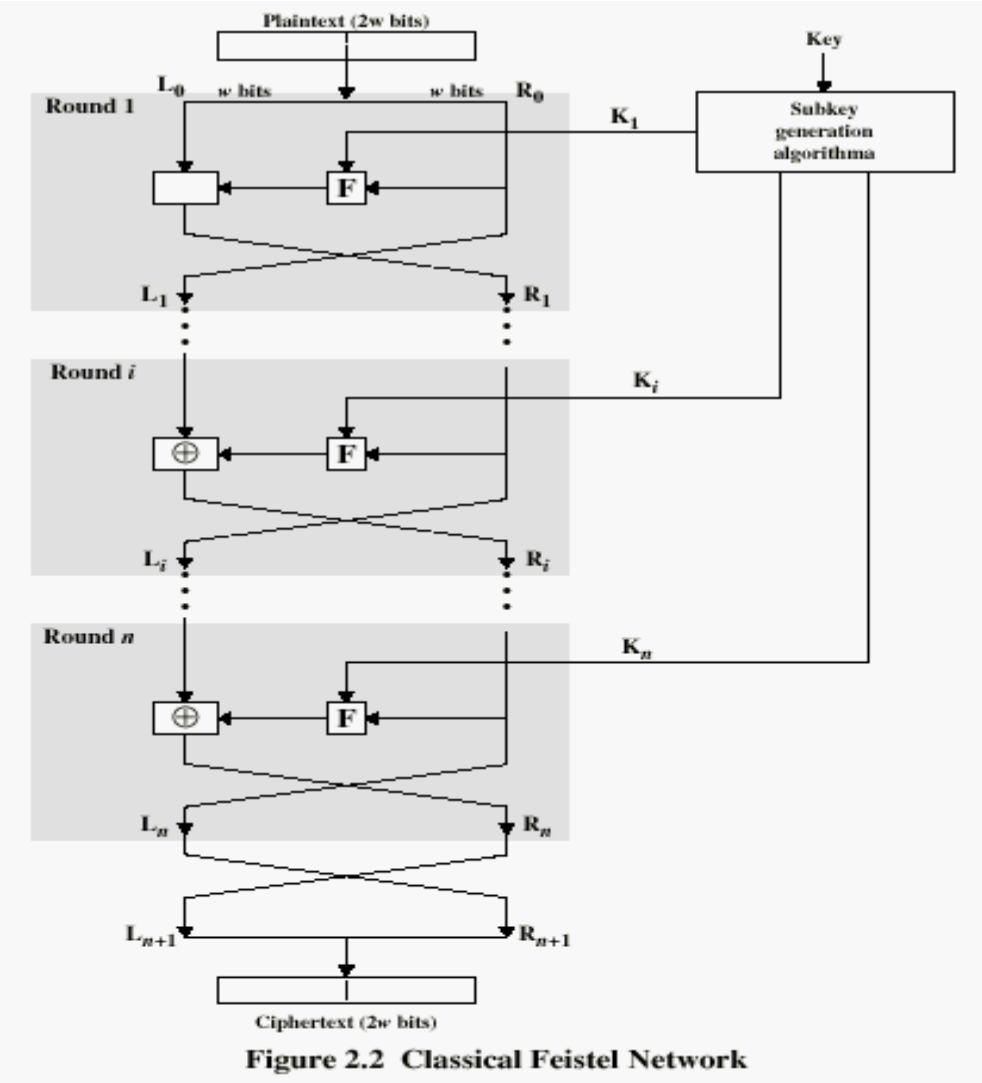


Figure 2.2 Classical Feistel Network

v 1.0

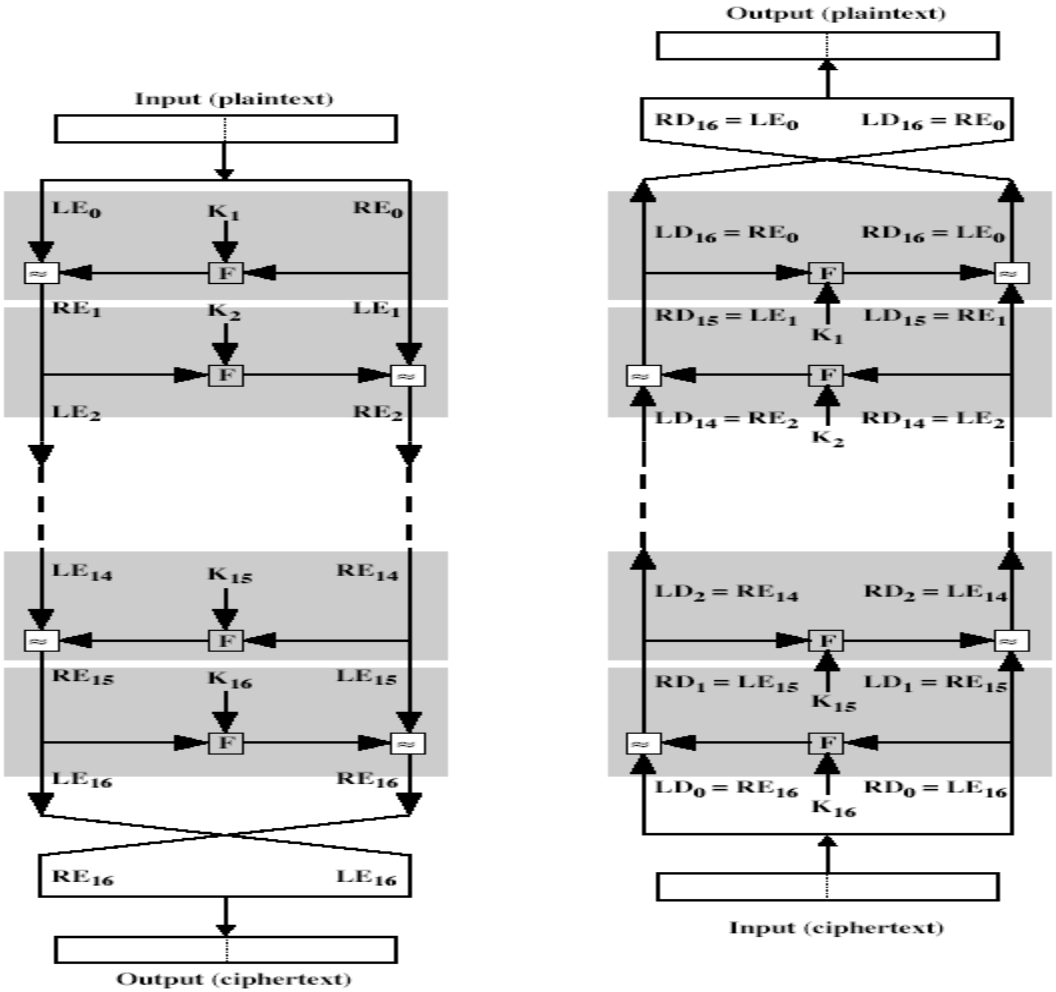
Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

Feistel Cipher Design Principles

- **block size**
  - increasing size improves security, but slows cipher
- **key size**
  - increasing size improves security, makes exhaustive key searching harder, but may slow cipher
- **number of rounds**
  - increasing number improves security, but slows cipher
- **subkey generation**
  - greater complexity can make analysis harder, but slows cipher
- **round function**
  - greater complexity can make analysis harder, but slows cipher
- **fast software en/decryption & ease of analysis**
  - are more recent concerns for practical use and testing

Feistel Cipher Decryption



Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

Data Encryption Standard (DES)

- most widely used block cipher in world
- encrypts 64-bit data using 56-bit key
- has widespread use
- has been considerable controversy over its security

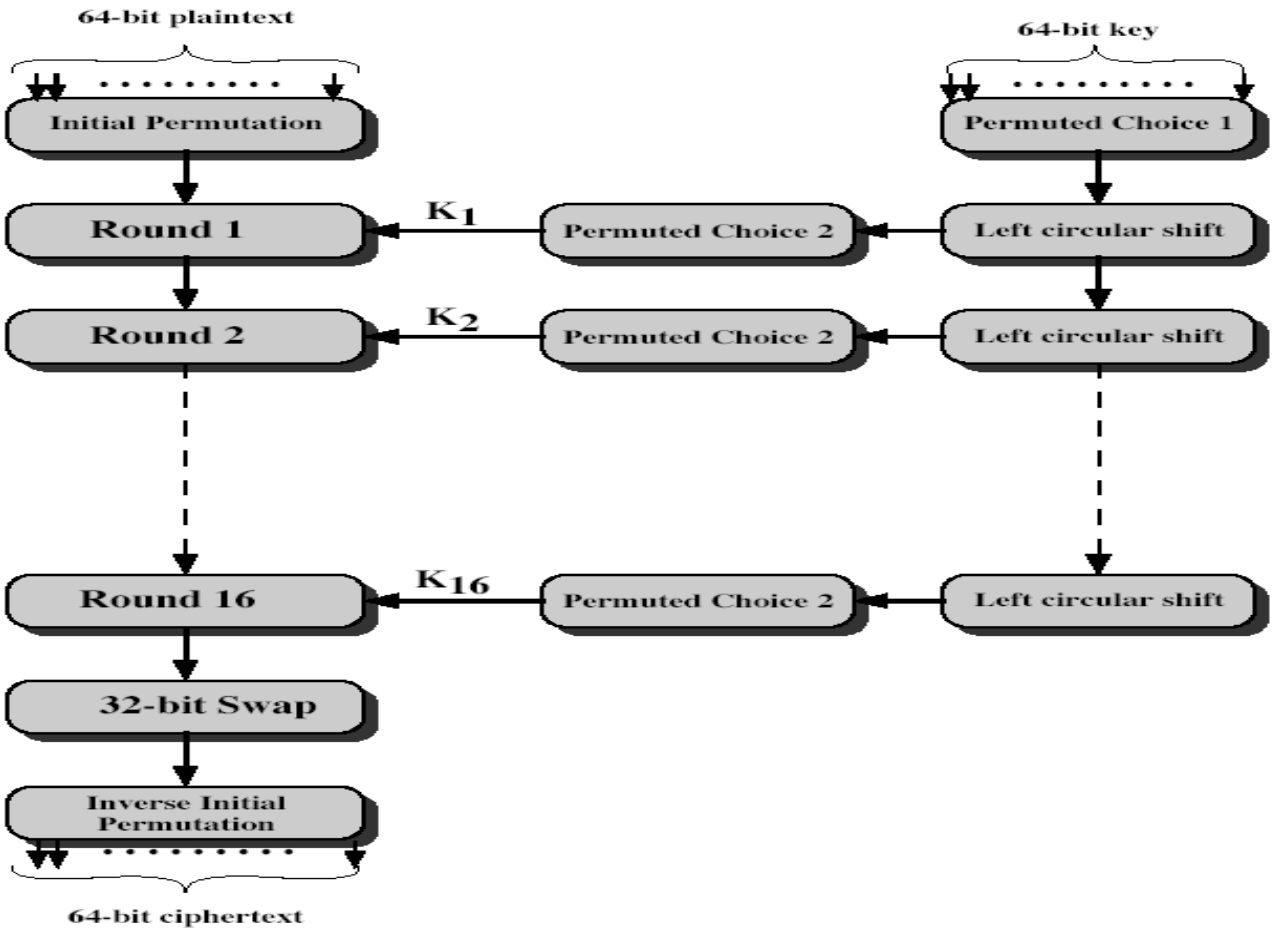
DES Design Controversy

- although DES standard is public
- was considerable controversy over design
  - in choice of 56-bit key (vs Lucifer 128-bit)
  - and because design criteria were classified
- subsequent events and public analysis show in fact design was appropriate
- DES has become widely used in financial applications

Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

DES Encryption



Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

Initial Permutation IP

- first step of the data computation
- IP reorders the input data bits
- even bits to LH half, odd bits to RH half
- quite regular in structure (easy in h/w)

Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

DES Round Structure

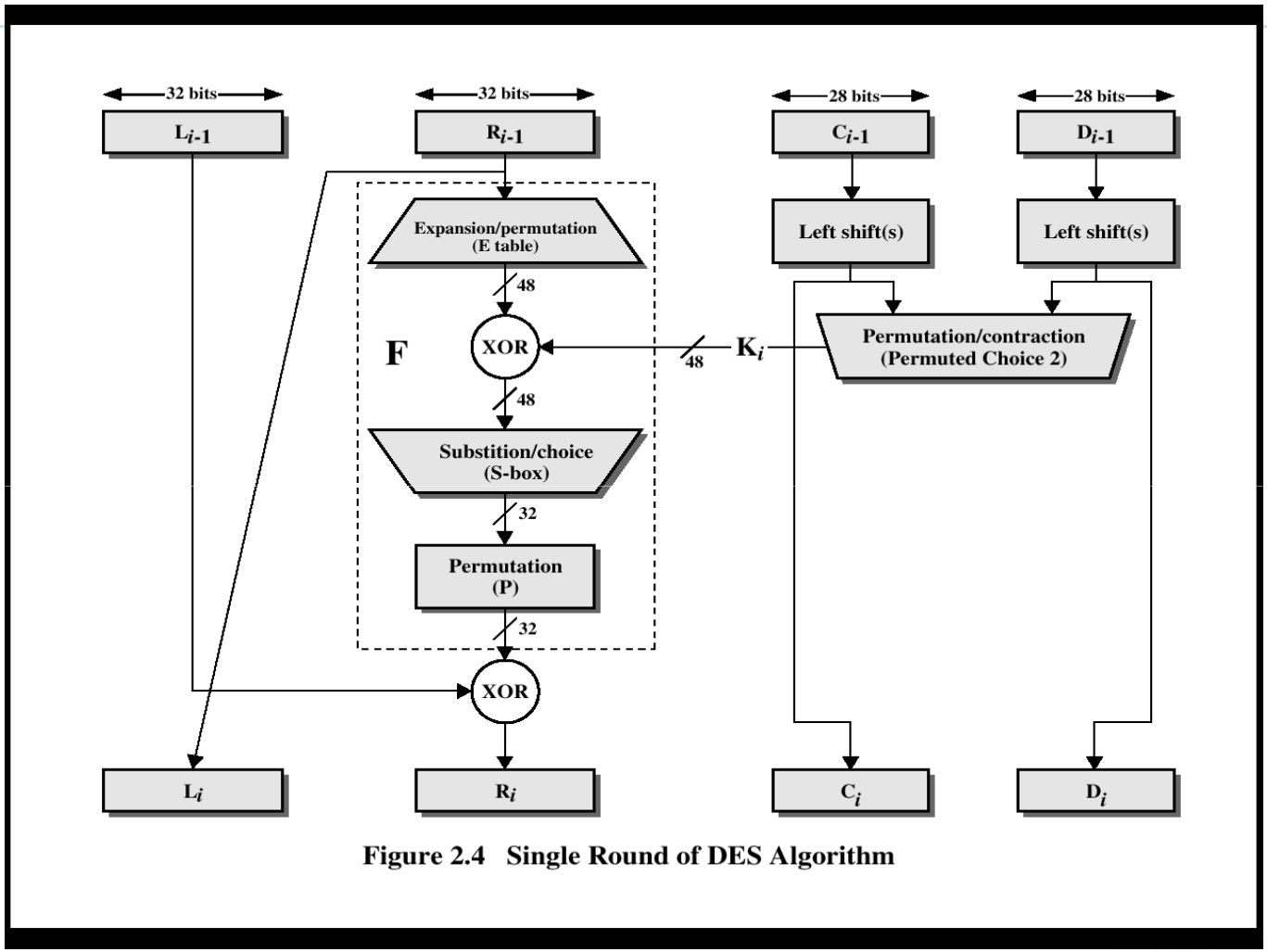


Figure 2.4 Single Round of DES Algorithm

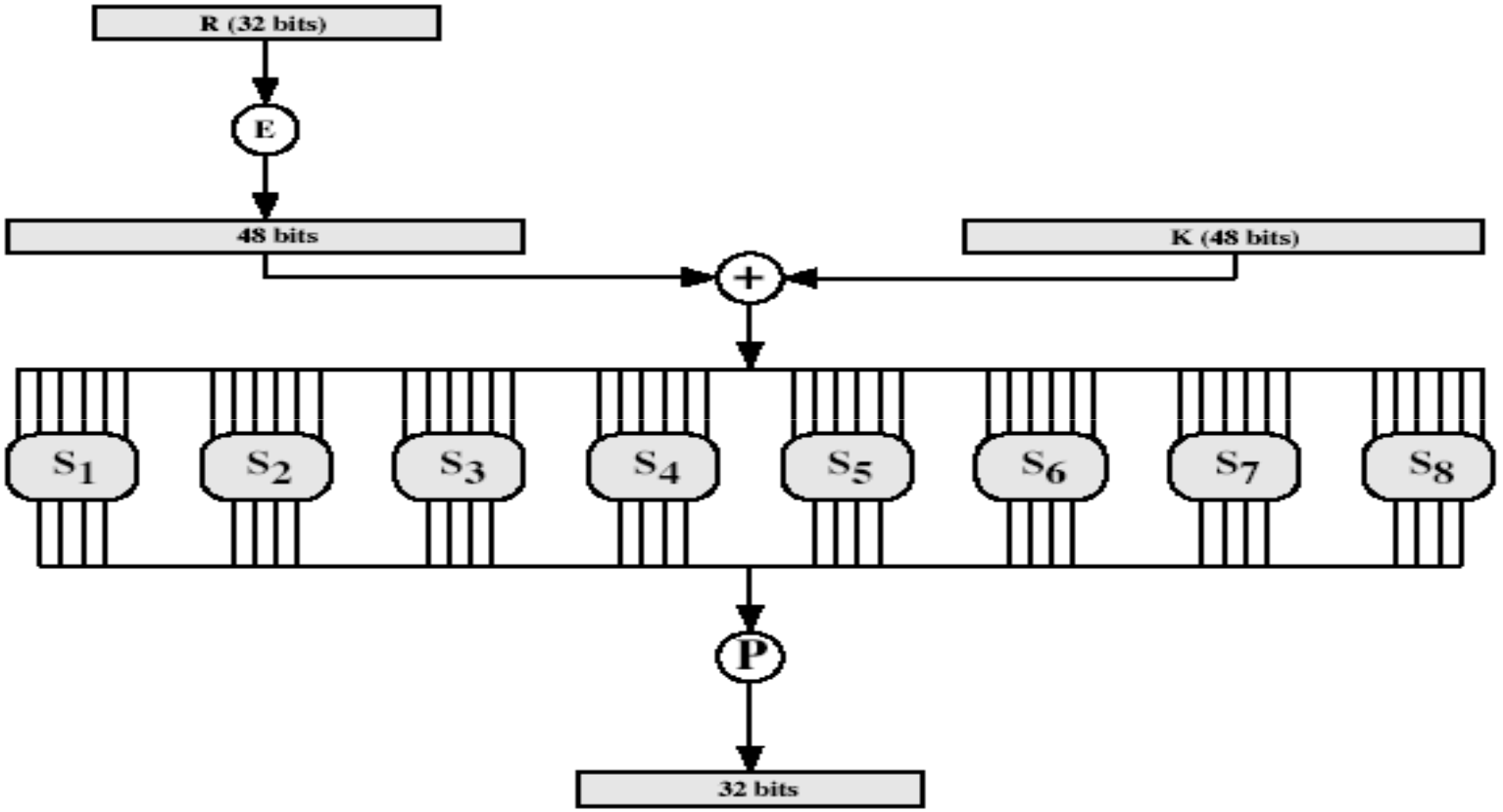
DES Round Structure

- uses two 32-bit L & R halves
- as for any Feistel cipher can describe as:

  $L_i = R_{i-1}$

  $R_i = L_{i-1}$ xor F(R_{i-1}, K_i)
- takes 32-bit R half and 48-bit subkey and:
  - expands R to 48-bits using perm E
  - adds to subkey
  - passes through 8 S-boxes to get 32-bit result
  - finally permutes this using 32-bit perm P

DES Round Structure



Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

Substitution Boxes S

- have eight S-boxes which map 6 to 4 bits
- each S-box is actually 4 little 4 bit boxes
  - outer bits 1 & 6 (**row** bits) select one rows
  - inner bits 2-5 (**col** bits) are substituted
  - result is 8 lots of 32 bits
- row selection depends on both data & key

Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

DES Key Schedule

- forms subkeys used in each round
- consists of:
  - initial permutation of the key (PC1) which selects 56-bits in two 28-bit halves
  - 16 stages consisting of:
    - selecting 24-bits from each half
    - permuting them by PC2 for use in function f,
    - rotating **each half** separately either 1 or 2 places depending on the **key rotation schedule** K

Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

DES Decryption

- decrypt must unwind steps of data computation
- with Feistel design, do encryption steps again
- using subkeys in reverse order (SK16 … SK1)
- 1st round with SK16 undoes 16th encrypt round
- 16th round with SK1 undoes 1st encrypt round
- then final FP undoes initial encryption IP
- thus recovering original data value

Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

Avalanche Effect

- key desirable property of encryption alg
- where a change of **one** input or key bit results in changing approx **half** output bits
- making attempts to "home-in" by guessing keys impossible
- DES exhibits strong avalanche

Agenda

- Introduction
- Block Vs stream cipher
  - Block cipher principles
- Feistel cipher structure
  - Feistel cipher design principles
- DES
  - Encryption
  - Initial permutation
  - Round structure
  - Substitution boxes
  - Key schedule
  - Decryption
  - Avalanche effect
  - Strength of DES

Strength of DES – Key Size

- 56-bit keys have $2^{56} = 7.2 \times 10^{16}$ values
- brute force search looks hard
- recent advances have shown is possible

– in 1997 on Internet in a few months

– in 1998 on dedicated h/w (EFF) in a few days

– in 1999 above combined in 22hrs!

- still must be able to recognize plaintext
- now considering alternatives to DES

Strength of DES – Timing Attacks

- DES finally and definitively proved insecure in July 1998, when the Electronic Frontier Foundation (EFF) announced that it had broken a DES encryption using a special-purpose "DES cracker" machine that was built for less than $250,000. The attack took less than three days.

Strength of DES – Analytic Attacks

- now have several analytic attacks on DES
- these utilise some deep structure of the cipher
  - by gathering information about encryptions
  - can eventually recover some/all of the sub-key bits
  - if necessary then exhaustively search for the rest
- generally these are statistical attacks
- include
  - differential cryptanalysis
  - linear cryptanalysis
  - related key attacks

Summary

- Understand the distinction between stream ciphers and block ciphers
- Present an overview of the Feistel cipher and explain how decryption is the inverse of encryption
- Present an overview of DES
- Explain the concept of avalanche effect
- Discuss the strength of DES

Test your understanding

1. Define avalanche effect.
2. Which parameters and design choices determine the actual algorithm of a Feistel cipher?
3. Explain DES algorithm.

References

1. William Stallings, Cryptography and Network Security, 6th Edition, Pearson Education, March 2013.
2. Charlie Kaufman, Radia Perlman and Mike Speciner, “Network Security”, Prentice Hall of India, 2002.