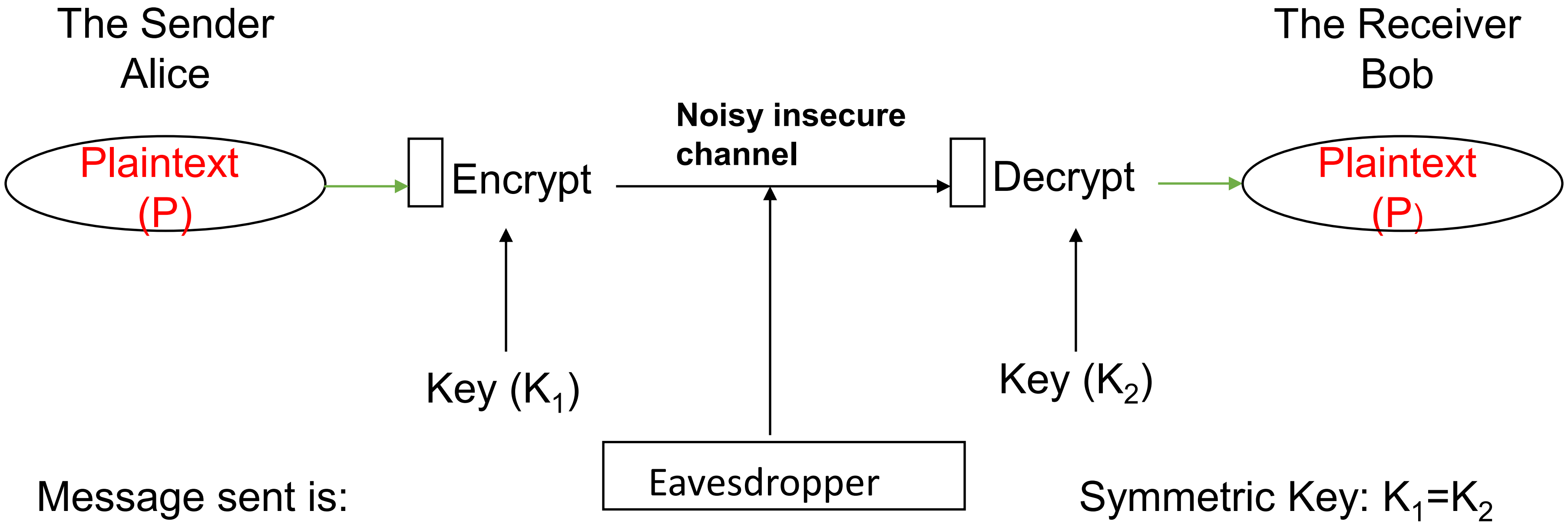
Block Ciphers and the Data Encryption Standard

ITC 3093 Principles of Computer Security

Based on Cryptography and Network Security by William Stallings and Lecture slides by Lawrie Brown

Cipher Needs



Message sent is:

$C= E_{K1}(P)$

Decrypted as:

$P=D_{K2}(C)$

P is called plaintext.

C is called ciphertext.

Symmetric Key: $K_1=K_2$

Public Key: $K_1{}^1K_2$

K_1 is publicly known

K_2 is Bob’s secret

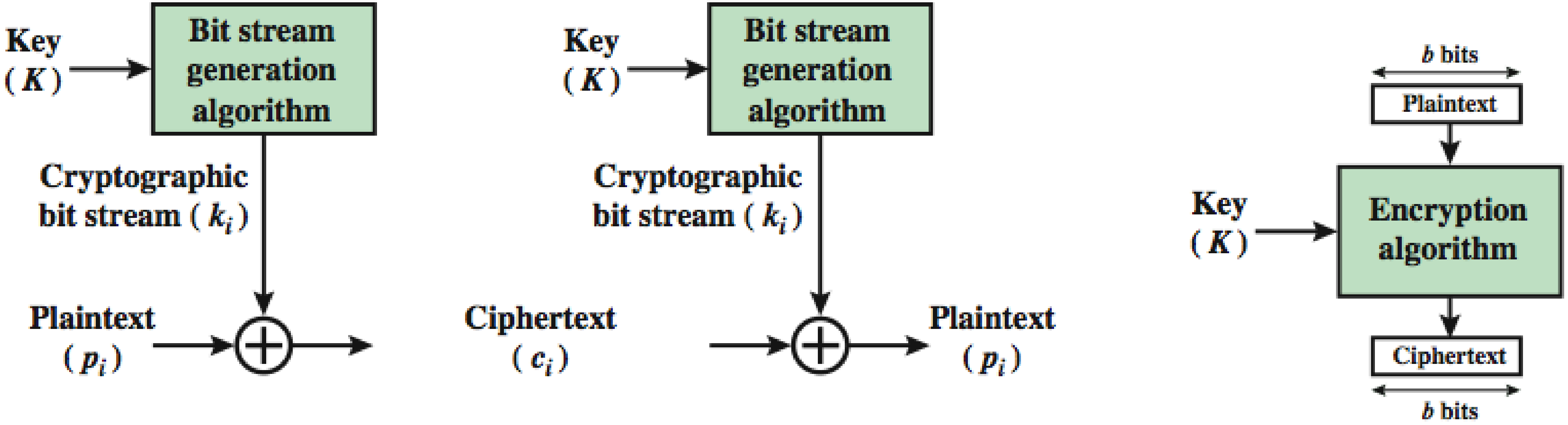
Cipher Requirements

- WW II
  - Universally available (simple, light instrumentation) – interoperability.
  - Compact, rugged: easy for people (soldiers) to use.
  - Kerckhoff's Principle: Security in key only, we assume that the attacker knows the complete details of the cryptographic algorithm and implementation
  - Adversary has access to some corresponding plain and cipher-text
- Now
  - Adversary has access to unlimited cipher-text and lots of chosen text.
  - Implementation in digital devices (power/speed) paramount.
  - Easy for computers to use.
  - Resistant to ridiculous amount of computing power.

Block vs Stream Ciphers

- block ciphers process messages in 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
  - better analysed
  - broader range of applications

Block vs Stream Ciphers



(a) Stream Cipher Using Algorithmic Bit Stream Generator

(b) Block Cipher

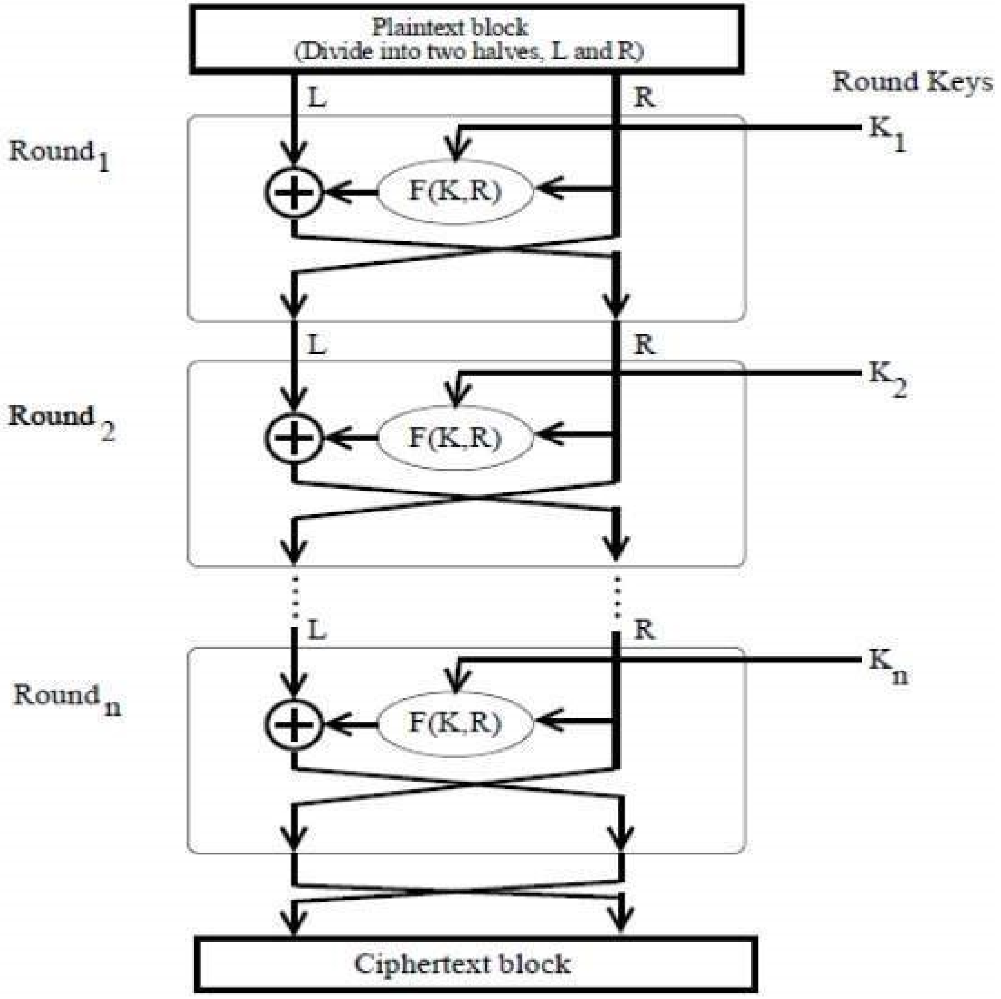
Modern Block Ciphers

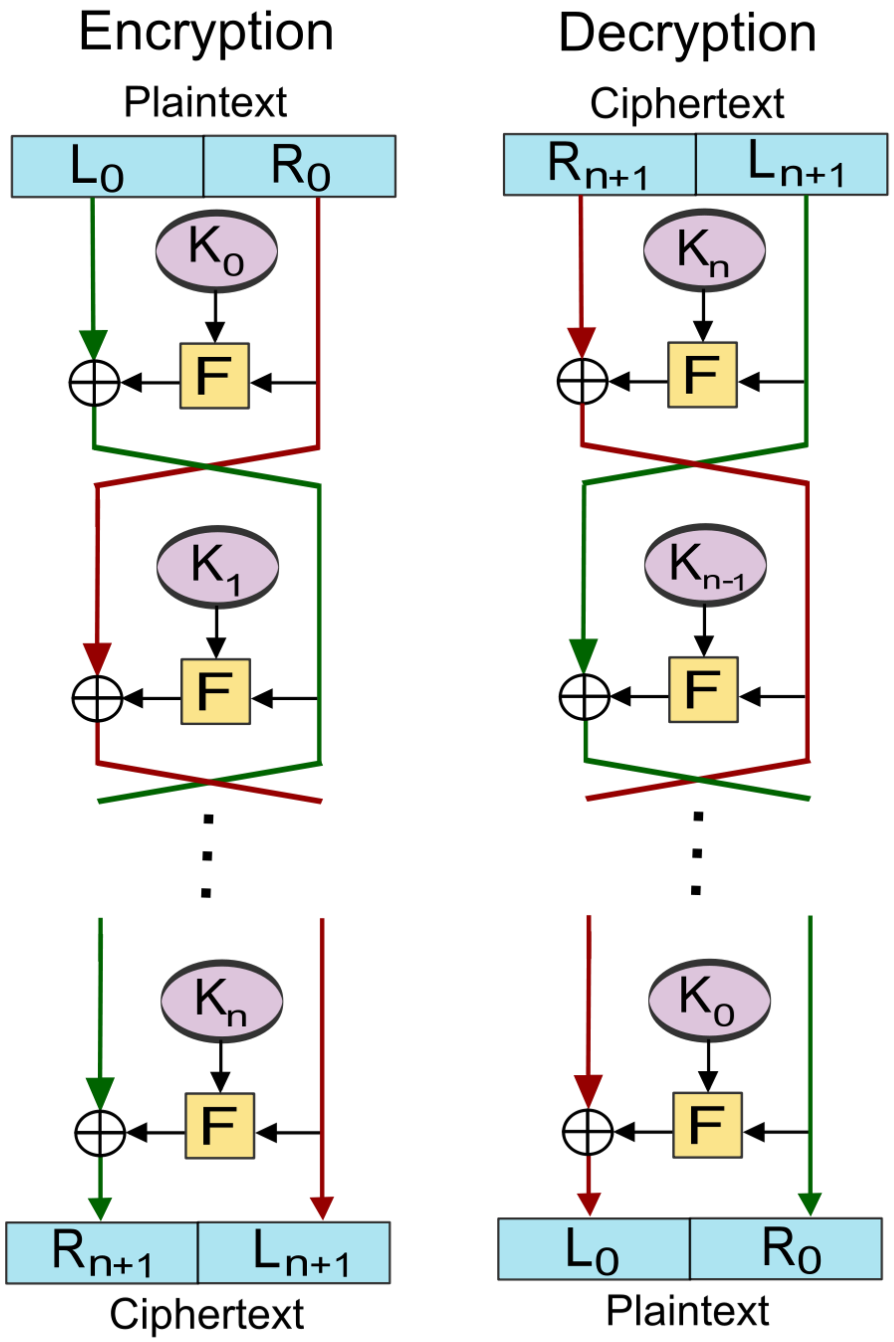
- one of the most widely used types of cryptographic algorithms
- provide secrecy /authentication services
- focus on DES (Data Encryption Standard)
- to illustrate block cipher design principles

Block Cipher Principles

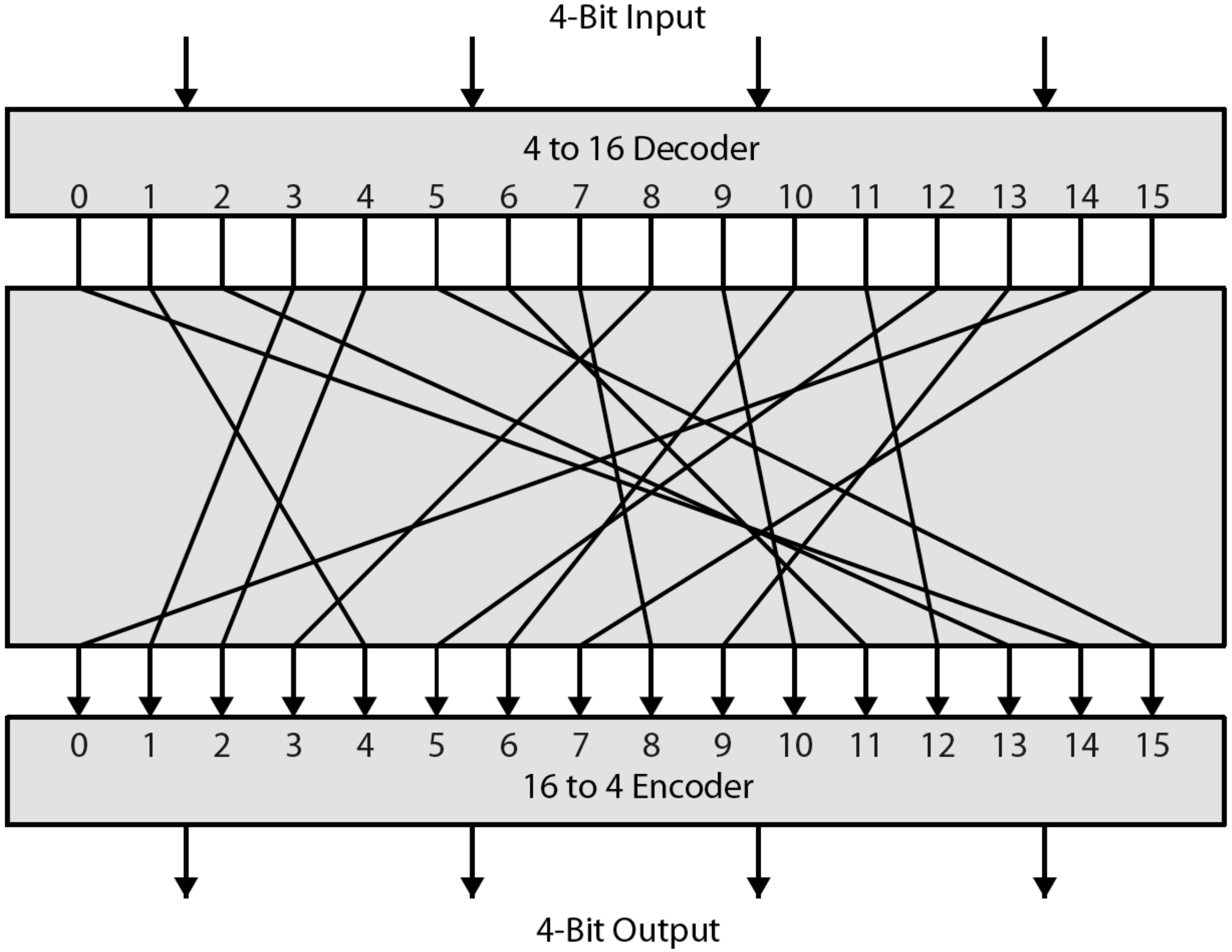
- most symmetric block ciphers are based on a **Feistel Cipher Structure**
- needed since must be able to **decrypt** ciphertext to recover messages efficiently
- block ciphers look like an extremely large substitution
- would need table of 2^{64} entries for a 64-bit block
- instead create from smaller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

Feistel Cipher Structure





Ideal Block Cipher



Based on Cryptography and Network Security by William Stallings and Lecture slides by Lawrie Brown

Substitution-Permutation Ciphers

- **Claude Shannon** introduced idea of substitution-permutation (S-P) networks in 1949 paper
- form basis of modern block ciphers
- S-P nets are based on the two primitive cryptographic operations seen before:
  - **substitution** (S-box)
  - **permutation** (P-box)
- provide confusion & diffusion of message & key

Confusion and Diffusion

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

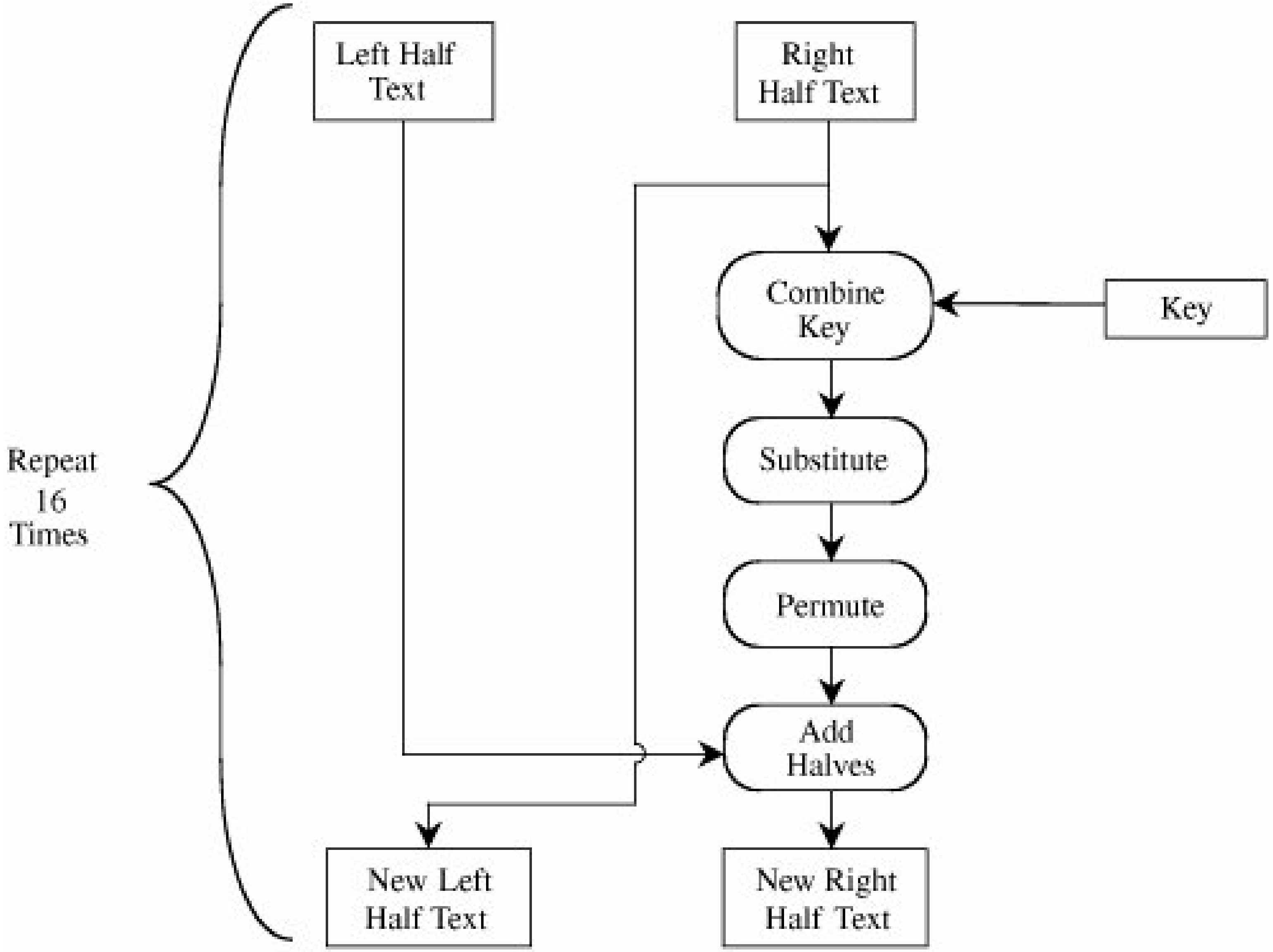
Data Encryption Standard (DES)

- IBM developed Lucifer cipher
  - by team led by Feistel in late 60's
  - used 64-bit data blocks with 128-bit key
- revised Lucifer was adopted in 1977 by NBS (now NIST) as the national cipher standard, DES
- encrypts 64-bit data using 56-bit key
- has widespread use
- has been considerable controversy over its security

DES Design Controversy

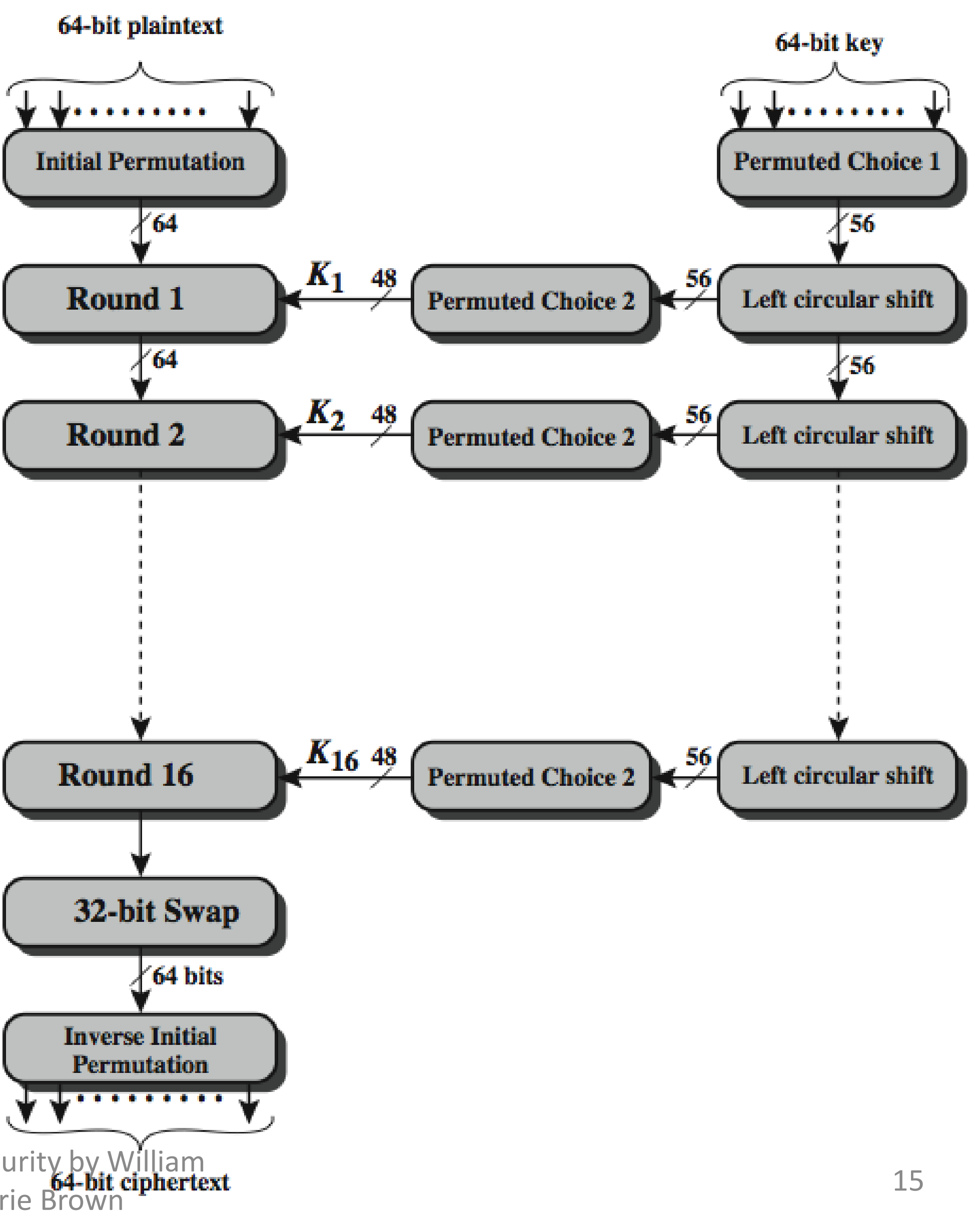
- although DES standard is public
- was considerable controversy over design
  - in choice of 56-bit key (vs Lucifer 128-bit)
  - and because design criteria were classified
- subsequent events and public analysis show in fact design was appropriate
- use of DES has flourished
  - especially in financial applications
  - still standardised for legacy application use

DES Encryption Overview



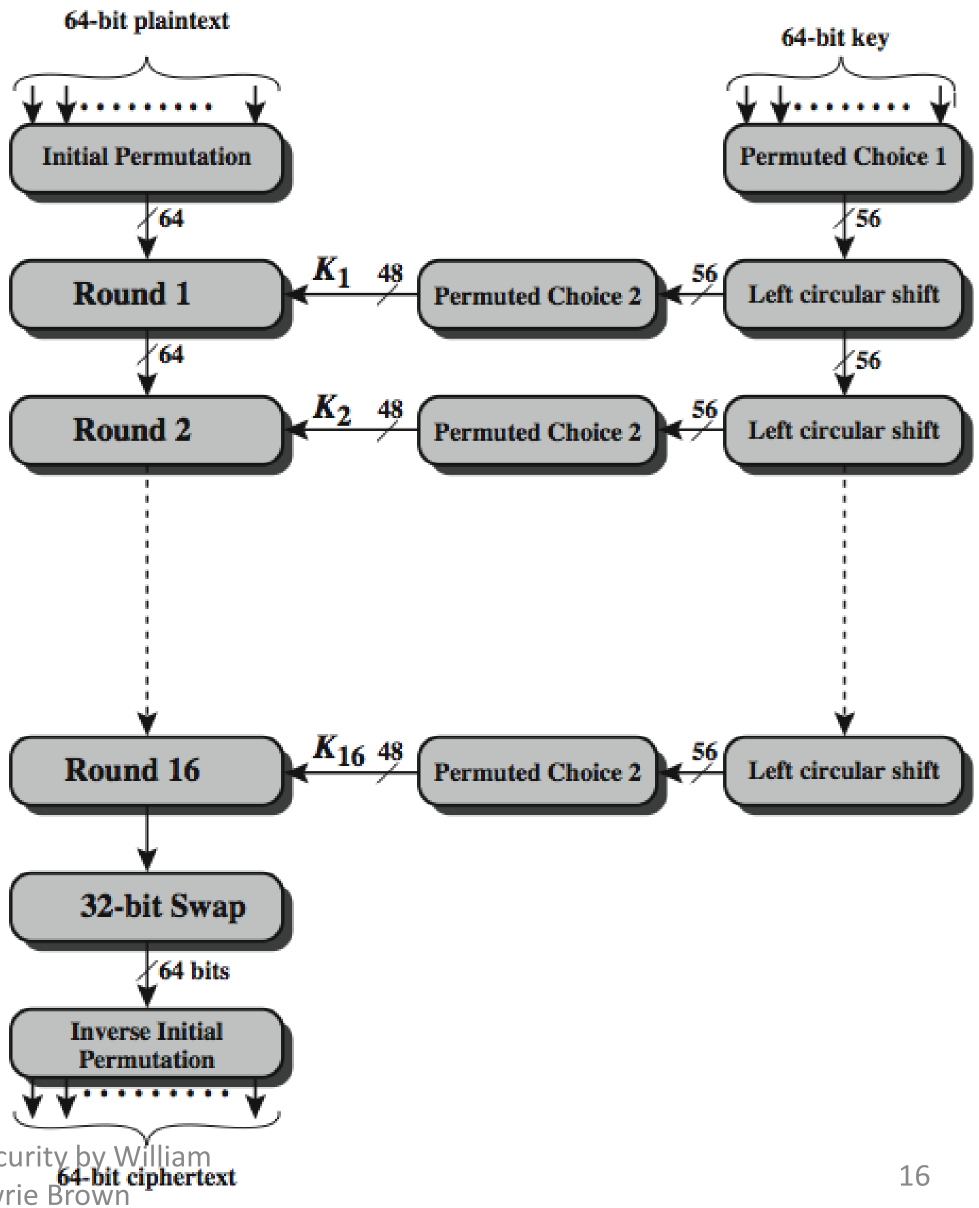
DES Encryption Overview

- The left side shows the basic process for enciphering a 64-bit data block which consists of:
  - an initial permutation (IP) which shuffles the 64-bit input block
  - 16 rounds of a complex key dependent round function involving substitutions & permutations
  - a final permutation, being the inverse of IP



DES Encryption Overview

- The right side shows the handling of the 56-bit key and consists of:
    - an initial permutation of the key (PC1) which selects 56-bits out of the 64-bits input, in two 28-bit halves
    - 16 stages to generate the 48-bit subkeys using a left circular shift and a permutation of the two 28-bit halves

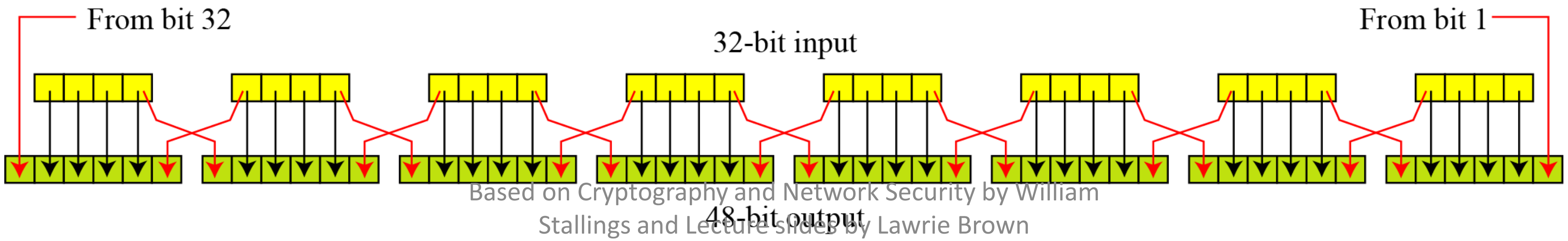


Based on Cryptography and Network Security by William Stallings and Lecture slides by Lawrie Brown

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)
- example:

```
IP(675a6967 5e5a6b5a) = (ffb2194d 004df6fb)
```

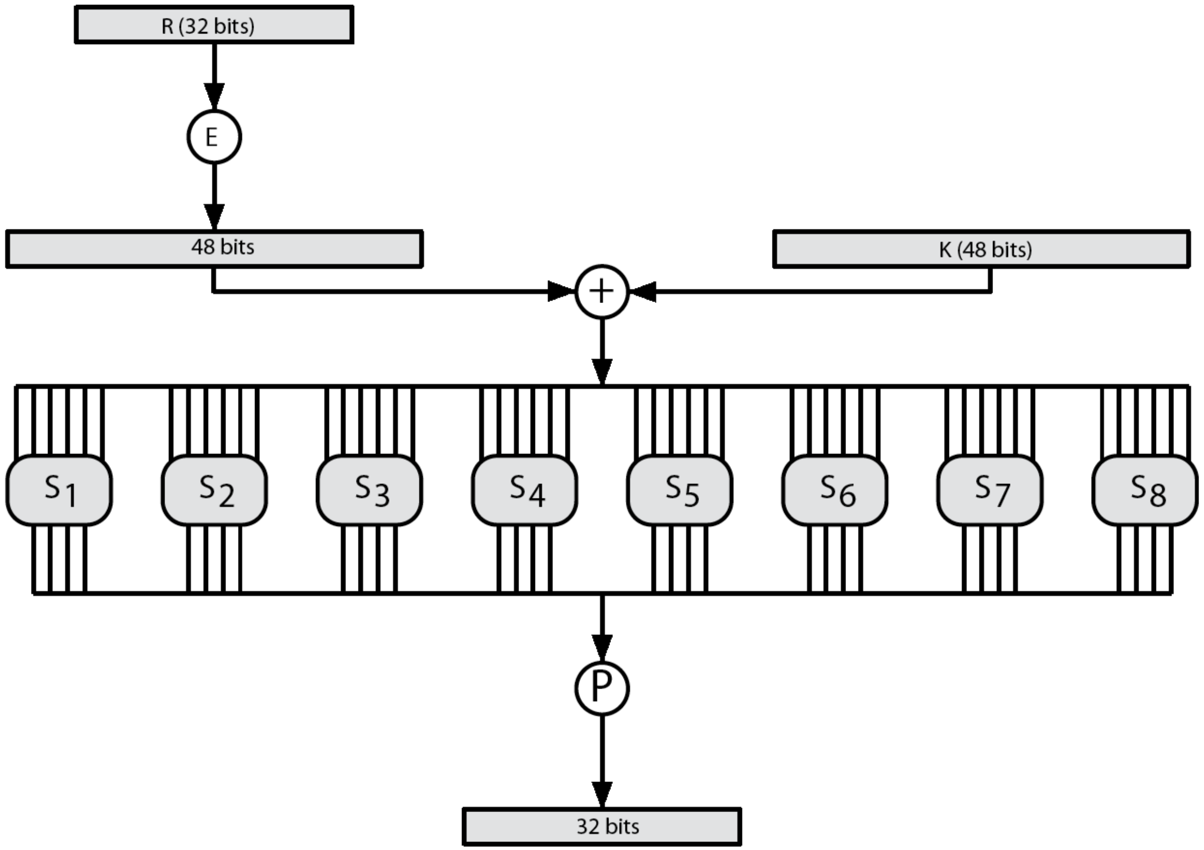


DES Round Structure

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

  $L_i = R_{i-1}$

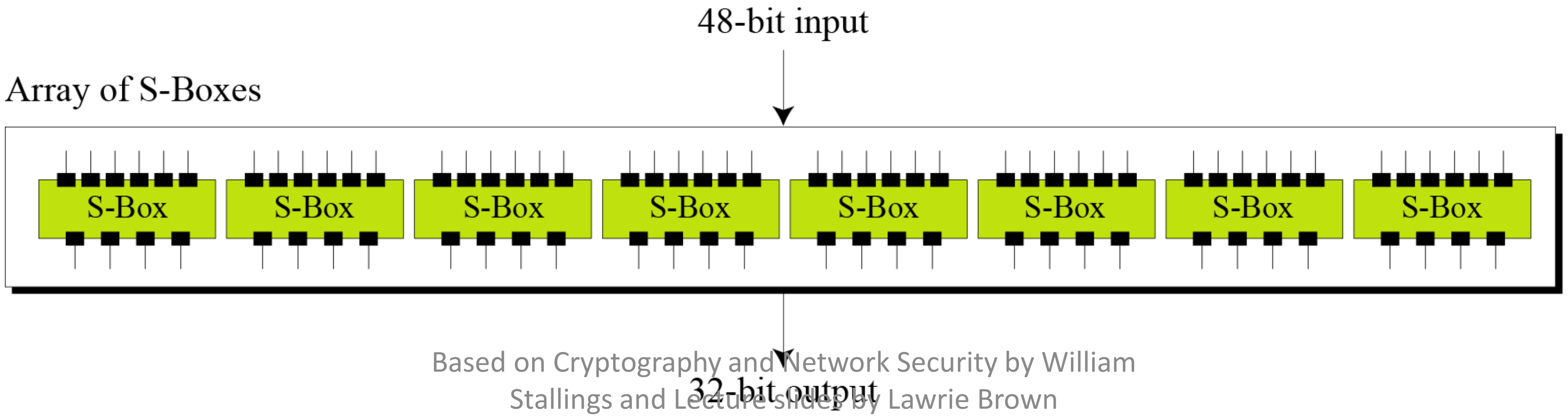
  $R_i = L_{i-1} \oplus \mathrm{F}(R_{i-1}, K_i)$
- F takes 32-bit R half and 48-bit subkey:
  - expands R to 48-bits using perm E
  - adds to subkey using XOR
  - passes through 8 S-boxes to get 32-bit result
  - finally permutes using 32-bit perm P



Based on Cryptography and Network Security by William Stallings and Lecture slides by Lawrie Brown

Substitution Boxes (S)

- The S-boxes do the real mixing (confusion).
- DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.
- Row selection depends on both data & key
  - feature known as autoclaving (autokeying)
- Example: `S(18 09 12 3d 11 17 38 39) = 5fd25e03`

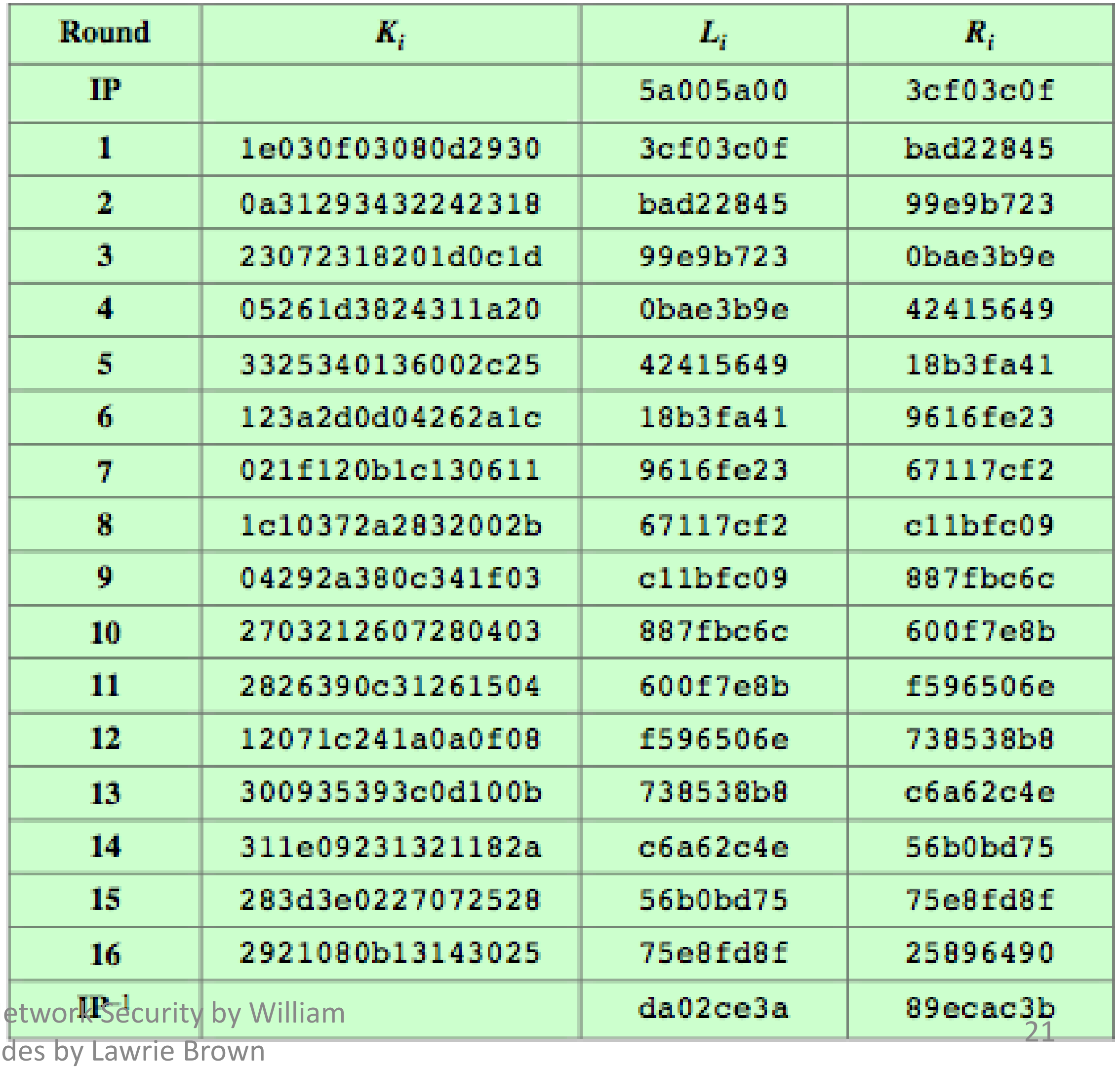


DES Decryption

- decrypt must unwind steps of data computation
- with Feistel design, do encryption steps again using subkeys in reverse order (SK16 … SK1)
    - IP undoes final FP step of encryption
    - 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

DES Example

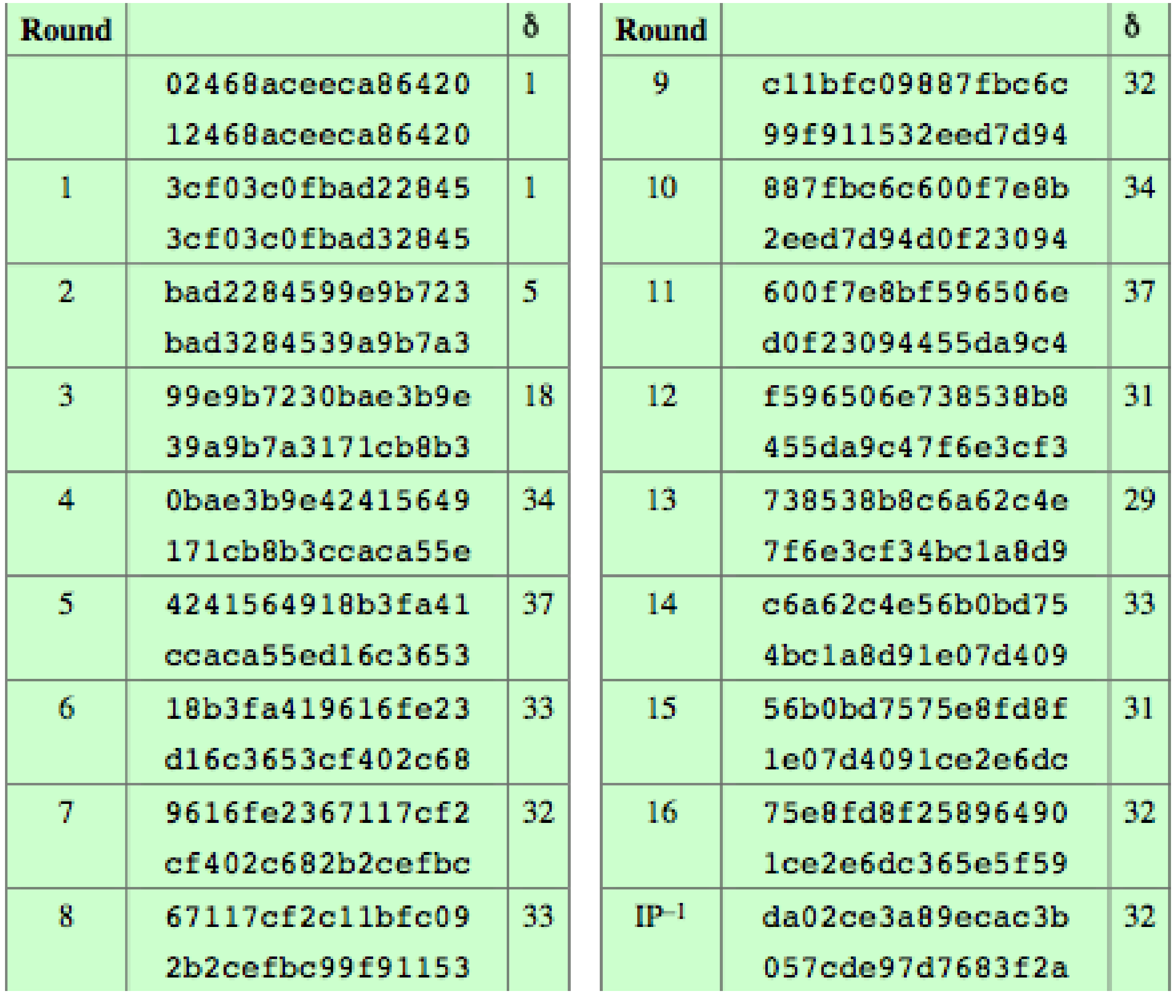
- Plaintext: 02468aceeca86420
- Key: 0f1571c947d9e859
- Ciphertext: da02ce3a89ecac3b
- The first row shows the 32-bit values of the left and right halves of data after the initial permutation.
- The next 16 rows show the results after each round.



Round	K_i	L_i	R_i
IP		5a005a00	3cf03c0f
1	1e030f03080d2930	3cf03c0f	bad22845
2	0a31293432242318	bad22845	99e9b723
3	23072318201d0c1d	99e9b723	0bae3b9e
4	05261d3824311a20	0bae3b9e	42415649
5	3325340136002c25	42415649	18b3fa41
6	123a2d0d04262a1c	18b3fa41	9616fe23
7	021f120b1c130611	9616fe23	67117cf2
8	1c10372a2832002b	67117cf2	c11bfc09
9	04292a380c341f03	c11bfc09	887fbc6c
10	2703212607280403	887fbc6c	600f7e8b
11	2826390c31261504	600f7e8b	f596506e
12	12071c241a0a0f08	f596506e	738538b8
13	300935393c0d100b	738538b8	c6a62c4e
14	311e09231321182a	c6a62c4e	56b0bd75
15	283d3e0227072528	56b0bd75	75e8fd8f
16	2921080b13143025	75e8fd8f	25896490
IP^{-1}		da02ce3a	89ecac3b

Avalanche in DES

- a small change in either the plaintext or the key should produce a significant change in the ciphertext – **avalanche**
- key desirable property of encryption algorithm
- making attempts to “home-in” by guessing keys impossible
- DES exhibits strong avalanche



Round		δ	Round		δ
	02468aceeca86420 12468aceeca86420	1	9	c11bfc09887fbc6c 99f911532eed7d94	32
1	3cf03c0fbad22845 3cf03c0fbad32845	1	10	887fbc6c600f7e8b 2eed7d94d0f23094	34
2	bad2284599e9b723 bad3284539a9b7a3	5	11	600f7e8bf596506e d0f23094455da9c4	37
3	99e9b7230bae3b9e 39a9b7a3171cb8b3	18	12	f596506e738538b8 455da9c47f6e3cf3	31
4	0bae3b9e42415649 171cb8b3ccaca55e	34	13	738538b8c6a62c4e 7f6e3cf34bc1a8d9	29
5	4241564918b3fa41 ccaca55ed16c3653	37	14	c6a62c4e56b0bd75 4bc1a8d91e07d409	33
6	18b3fa419616fe23 d16c3653cf402c68	33	15	56b0bd7575e8fd8f 1e07d4091ce2e6dc	31
7	9616fe2367117cf2 cf402c682b2cefbc	32	16	75e8fd8f25896490 1ce2e6dc365e5f59	32
8	67117cf2c11bfc09 2b2cefbc99f91153	33	IP^{-1}	da02ce3a89ecac3b 057cde97d7683f2a	32

Based on Cryptography and Network Security by William Stallings and Lecture slides by Lawrie Brown

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
- must now consider alternatives to DES

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
    - differential cryptanalysis
    - linear cryptanalysis
    - related key attacks

Strength of DES – Timing Attacks

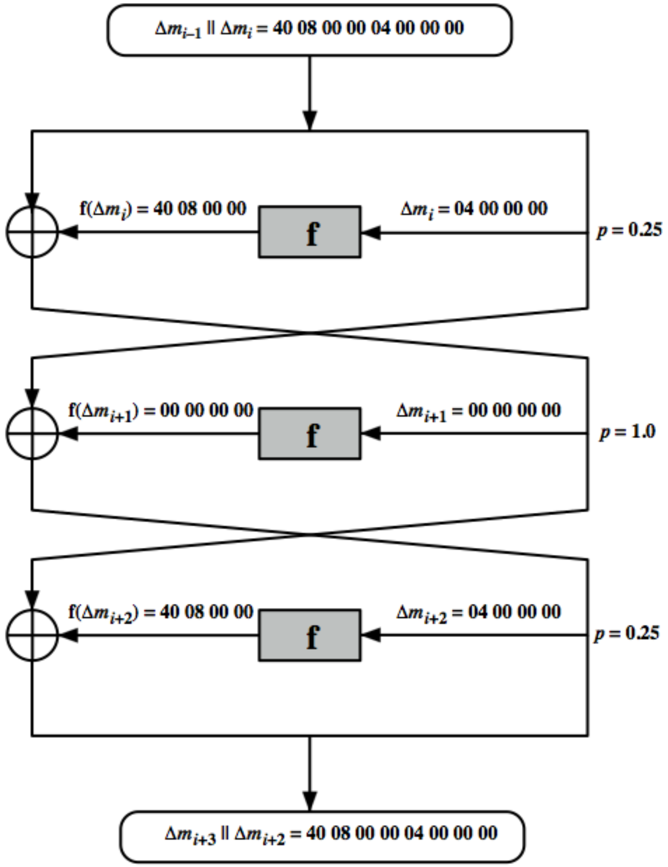
- attacks actual implementation of cipher
- use knowledge of consequences of implementation to derive information about some/all subkey bits
- specifically use fact that calculations can take varying times depending on the value of the inputs to it
- particularly problematic on smartcards

Differential Cryptanalysis

- one of the most significant recent (public) advances in cryptanalysis
- known by NSA in 70's cf DES design
- Murphy, Biham & Shamir published in 90’s
- powerful method to analyse block ciphers
- used to analyse most current block ciphers with varying degrees of success
- DES reasonably resistant to it, cf Lucifer

Differential Cryptanalysis

- have some input difference giving some output difference with probability p
- if find instances of some higher probability input / output difference pairs occurring
- can infer subkey that was used in round
- then must iterate process over many rounds (with decreasing probabilities)


$\Delta m_{i-1} \| \Delta m_i$ = 40 08 00 00 04 00 00 00
$f(\Delta m_i)$ = 40 08 00 00
f
Δm_i = 04 00 00 00
$p = 0.25$
$f(\Delta m_{i+1})$ = 00 00 00 00
f
Δm_{i+1} = 00 00 00 00
$p = 1.0$
$f(\Delta m_{i+2})$ = 40 08 00 00
f
Δm_{i+2} = 04 00 00 00
$p = 0.25$
$\Delta m_{i+3} \| \Delta m_{i+2}$ = 40 08 00 00 04 00 00 00

Linear Cryptanalysis

- another recent development
- also a statistical method
- must be iterated over rounds, with decreasing probabilities
- developed by Matsui et al in early 90's
- based on finding linear approximations
- can attack DES with 2^{43} known plaintexts, easier but still in practise infeasible

DES Design Criteria

- as reported by Coppersmith in [COPP94]
- 7 criteria for S-boxes provide for
  - non-linearity
  - resistance to differential cryptanalysis
  - good confusion
- 3 criteria for permutation P provide for
  - increased diffusion

Based on Cryptography and Network Security by William Stallings and Lecture slides by Lawrie Brown

Block Cipher Design

- basic principles still like Feistel’s in 1970’s
- number of rounds
  - more is better, exhaustive search best attack
- function f:
  - provides “confusion”, is nonlinear, avalanche
  - have issues of how S-boxes are selected
- key schedule
  - complex subkey creation, key avalanche

Summary

- block vs stream ciphers
- Feistel cipher design & structure
- DES
  - details
  - strength
- Differential & Linear Cryptanalysis
- block cipher design principles