Encryption Algorithms & Protocols

Symmetric key Crypto
- Block cipher

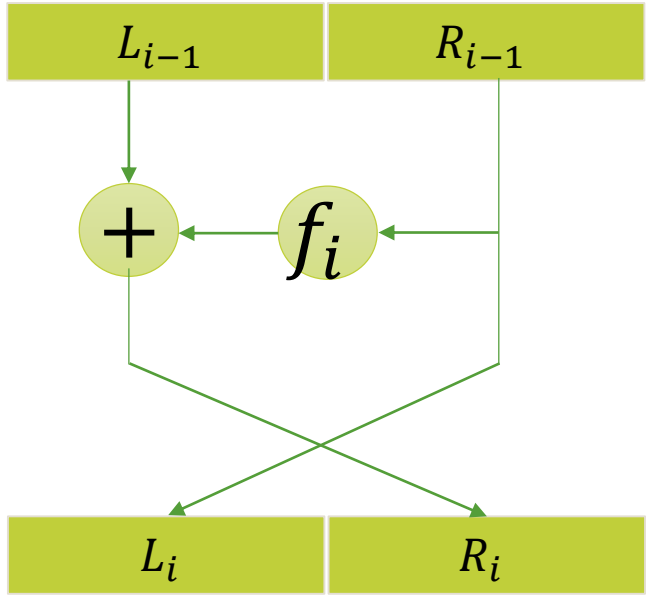
Dr. Omar Abusada
E-mail: abossada1@gmail.com

Block Cipher (Iterated)

- Plaintext and Ciphertext consist of fixed-sized blocks.
- Ciphertext obtained from plaintext by iterating a round function.
- Input to round function consists of key and output of previous round.
- Usually implemented in software.

Feistel Cipher: Encryption

- Feistel cipher is a type of block cipher, not a specific block cipher.
- Split plaintext block into left and right halves: $P = (L_0 , R_0)$
- For each round $i = 1,2,3, \ldots \ldots \ldots \ldots \ldots \ldots, n$ *compute*:
- $L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$, where F is round function and K_i is **subkey**
- Ciphertext: $C = (L_n , R_n)$.



Feistel Cipher: Decryption

- Start with Ciphertext: $C = (L_n , R_n)$.
- For each round $i = n, n-1, \ldots\ldots\ldots\ldots\ldots, 2,1 compute$:
- R_{i-1}=L_i
- $L_{i-1} = R_i \oplus F(R_{i-1}, K_i)$, where F is round function and K_i is **subkey**
- Plaintext: $P = (L_0 , R_0)$.
- Formula "works" for any function F
- But only secure for certain functions F

Feistel Cipher: Example

- Plain text [0 1 1 1 1 0 1 0 0 0 0 1].
- key = [1st to 2nd -- 2nd to 3rd -- 3rd to 1st]
- L_0 = [0 1 1 1 1 0], R_0 =[1 0 0 0 0 1],
- **1st iteration :**
- $L_1 = R_0$ = [1 0 0 0 0 1],
- $F(R_{i-1}, K_i)$= $F(R_0, K_1)$=[0 1 0 1 0 0] **[1st to 2nd -- 2nd to 3rd -- 3rd to 1st]**
- $R_1 = L_0 \oplus F(R_{i-1}, K_i)$ = [0 1 1 1 1 0]⊕[0 1 0 1 0 0]=[0 0 1 0 1 0]
- **Ciphertext= [1 0 0 0 0 10 0 1 0 1 0]**

Same procedure can go to the 2nd , 3rd and so on iterations

https://www.youtube.com/watch?v=w8_rloQMQ08

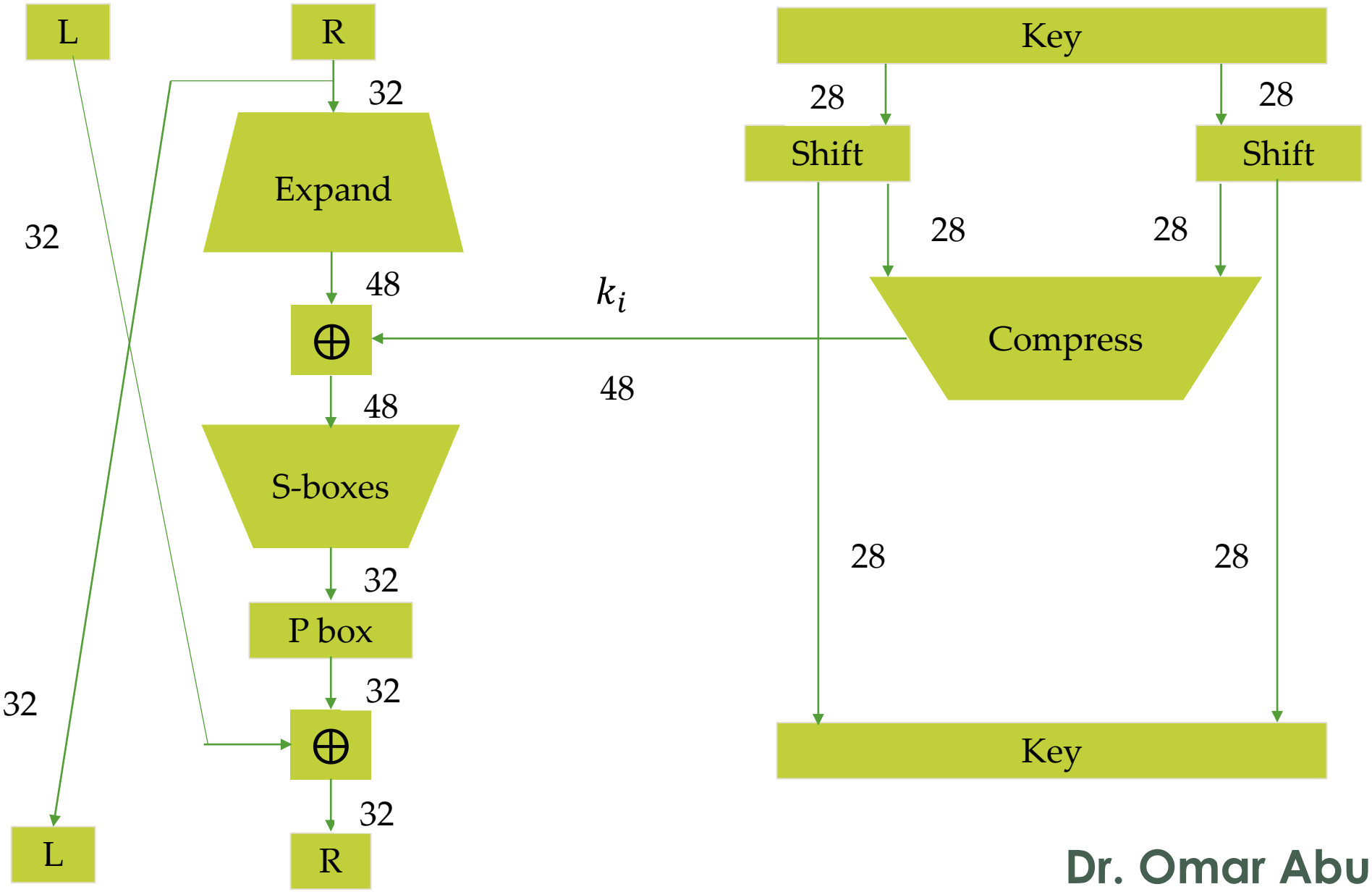
Data Encryption Standard

- DES developed in 1970's.
- Based on IBM's Lucifer cipher.
- DES was U.S. government standard.
- DES development was debateable.
  - NSA secretly involved.
  - Design process was secret.
  - Key length reduced from 128 to 56 bits.
  - Subtle changes to Lucifer algorithm.

DES Numerology

- DES is a Feistel cipher with…
  - 64 bit block length.
  - 56 bit key length.
  - 16 rounds.
  - 48 bits of key used each round (Subkey).
- Each round is simple (for a block cipher).
- Security depends heavily on “S-boxes”.
  - Each S-boxes maps 6 bits to 4 bits.

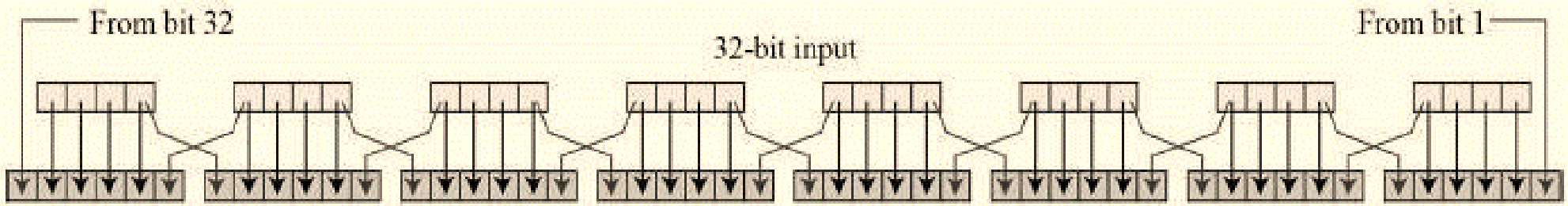
One Round of DES



DES Expansion Permutation

- Input 32 bits

0	1	2	3	4	5	6	7	8	9	10	11
12	13	14	15	16	17	18	19	20	21	22	23
24	25	26	27	28	29	30	31				



- **Input 32 bits**
- **Output 48bits**

- Output 48 bits

31	0	1	2	3	4	3	4	5	6	7	8
7	8	9	10	11	12	11	12	13	14	15	16
15	16	17	18	19	20	19	20	21	22	23	24
23	24	25	26	27	28	27	28	29	30	31	0

DES P-box

- Input 32 bits

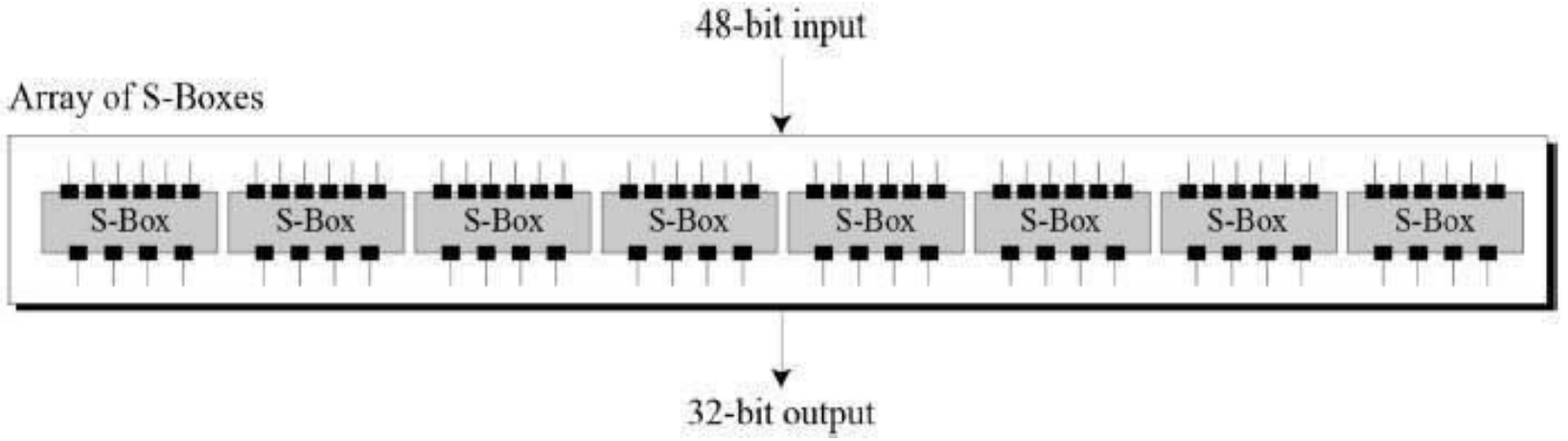
0	1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20	21
22	23	24	25	26	27	28	29	30	31	

- Output 32 bits

15	6	19	20	28	11	27	16	0	14	22	25	4	17	30	9
1	7	23	13	31	26	2	8	18	12	29	5	21	10	3	24

DES S-box

- 8 “substitution boxes” or S-boxes
- Each S-box maps 6 bits to 4 bits
- S-box number 1



Input bits (0,5)

Input bits (1,2,3,4,)

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

DES Subkey

56 bit DES key, numbered 0,1,2,…,55

- Left half key bits, LK

49	42	35	28	21	14	7
0	50	43	36	29	22	15
8	1	51	44	37	30	23
16	9	2	52	45	38	31

- Right half key bits, RK

55	48	41	34	27	20	13
6	54	47	40	33	26	19
12	5	53	46	39	32	25
18	11	4	24	17	10	3

DES Subkey

For rounds i=1,2,...,16

- Let LK = (LKcircular shift left by r_i)
- Let RK = (RKcircular shift left by r_i)
- **Left half of subkey k_i is of LK bits**

13	**16**	**10**	**23**	**0**	**4**	**2**	**27**	**14**	**5**	**20**	**9**
22	**18**	**11**	**3**	**25**	**7**	**15**	**6**	**26**	**19**	**12**	**1**

- **Right half of subkey k_i is RK bits**

12	**23**	**2**	**8**	**18**	**26**	**1**	**11**	**22**	**16**	**4**	**19**
15	**20**	**10**	**27**	**5**	**24**	**17**	**13**	**21**	**7**	**0**	**3**

DES Subkey

- For rounds 1, 2, 9 and 16 the shift r_i is 1, and in all other rounds r_i is 2.
- Bits 8,17,21,24 of LK omitted each round.
- Bits 6,9,14,25 of RK omitted each round.
- Compression permutation yields 48 bit Subkey $\boldsymbol{k_i}$ from 56 bits of LK and RK.
- **Key schedule** generates subkey.

https://www.youtube.com/watch?v=cVhlCzmb-v0

DES Last Word (Almost)

- An initial permutation before round 1.
- Halves are swapped after last round.
- A final permutation (inverse of initial perm) applied to $(\boldsymbol{R_{16}}, \boldsymbol{L_{16}})$.
- None of this serves security purpose.

Security of DES

- Security depends heavily on S-boxes.
  - Everything else in DES is linear.
- Thirty years of intense analysis has revealed no “back door”.
- Attacks, essentially exhaustive key search.
- Inescapable conclusions
  - Designers of DES knew what they were doing
  - Designers of DES were way ahead of their time

Block Cipher Notation

- $\boldsymbol{P}$ = plaintext block
- $\boldsymbol{C}$ =ciphertext block
- Encrypt $\boldsymbol{P}$ with key $\boldsymbol{K}$ to get ciphertext $\mathbf{C}$
  - $\mathbf{C} = \boldsymbol{E}(\boldsymbol{P}, \boldsymbol{K})$
  - Decrypt $\boldsymbol{C}$ with key $\boldsymbol{K}$ to get plaintext $\boldsymbol{P}$
  - $\boldsymbol{P} = \boldsymbol{D}(\boldsymbol{C}, \boldsymbol{K})$
- Note: $\boldsymbol{P} = \boldsymbol{D}(\boldsymbol{E}(\boldsymbol{P}, \boldsymbol{K}), \boldsymbol{K})$
  - But $\boldsymbol{P} \neq \boldsymbol{D}(\boldsymbol{E}(\mathbf{P}, \boldsymbol{K_1}), \boldsymbol{K_2})$ and $\boldsymbol{C} \neq \boldsymbol{E}(\boldsymbol{D}(\mathbf{C}, \boldsymbol{K_1}), \boldsymbol{K_2})$ when $\boldsymbol{K_1} \neq \boldsymbol{K_2}$

Triple DES

- Today, 56 bit DES key is too small.
  - Exhaustive key search is possible.
- But DES is everywhere, so what to do?
- Triple DES or 3DES (112 bit key).
  - $\boldsymbol{C = E(D(E(P, K_1), K_2), K_1)}$.
  - $\boldsymbol{P = D(E(D(C, K_1), K_2), K_1)}$.
- Encrypt-Decrypt-Encrypt with 2 keys

Advanced Encryption Standard AES

- Replacement for DES was needed.
- AES competition (late 97)
  - o NSA openly involved
  - o Transparent process
  - o 15 strong algorithms proposed
  - o But 5 only shortlisted.
  - o In Oct. 2000 Rijndael Algorithm ultimately selected
- (pronounced like “Rain Doll”)
- Iterated block cipher (like DES)
- Not a Feistel cipher (unlike DES)

Advanced Encryption Standard AES

- The AES algorithm, also known as (Rijndael Algorithm) is a symmetric block cipher algorithm that takes:

  - **block size of 128 bits**.

  - **Key size of 128, 192 or 256 bits** (independent of block size)

- AES performs on byte data, instead of bit data.
- Number of rounds depends on Key length
  - 128 bit Key length_____ uses _____ 10 rounds
  - 192 bit Key length_____ uses _____ 12 rounds
  - 256 bit Key length_____ uses _____ 14 rounds

DES vs AES

DES

- Key length 56 bits
- Block size 64 bits
- Fixed number of rounds (16)
- Implemented slower

AES

- Key length 128/192/256 bits
- Block size 128 bits
- Number of rounds dependent on key length
- Implemented faster

A Few Other Block Ciphers

- **International Data Encryption Algorithm (IDEA)**
- Invented by James Massey
- One of the giants of modern crypto
- IDEA has 64-bit block, 128-bit key
- IDEA uses mixed-mode arithmetic
- Combine different math operations
  - IDEA the first to use this approach
  - Frequently used today

Blowfish

- Blowfish encrypts 64-bit blocks
- Key is variable length, up to 448 bits
- Invented by Bruce Schneier
- Almost a Feistel cipher
- $Ri = Li\text{-}1 \oplus Ki$
- $Li = Ri\text{-}1 \oplus F(Li\text{-}1 \oplus Ki)$
- The round function F uses 4 S-boxes
  - Each S-box maps 8 bits to 32 bits
- Key-dependent S-boxes
  - S-boxes determined by the key

… Thank you …