DATA ENCRYPTION STANDARD

BLOCK CIPHER DESIGN PRINCIPLES

- A Block Cipher works on a "block" of bits or bytes
- The algorithm is simple and fast, but applied for a number of "rounds"
- Several Principles determine the strength of a Block Cipher

1. Number of Rounds

The greater the number of rounds, the harder to cryptanalyze the ciphertext.

2. Block Size

Larger block sizes mean greater security but reduced encryption/ decryption speed

3. Key Size

Larger key size means greater security but reduces encryption/ decryption speed

BLOCK CIPHER DESIGN PRINCIPLES

4. Round Function

Greater complexity generally leads to greater resistance to cryptanalysis

5. Subkey generation algorithm

Greater complexity leads to greater difficulty of cryptanalysis

6. Fast software encryption and decryption

Encrypting can be embedded in applications or utility functions

BLOCK CIPHER DESIGN – NUMBER OF ROUNDS

- The greater the number of rounds, the harder to cryptanalyze the ciphertext
- Chosen so that known cryptanalytic efforts require greater effort than brute force key attack
- If DES had fewer rounds, then differential cryptanalysis would require less effort than a brute-force key search

BLOCK CIPHER DESIGN – CRITERIA FOR DESIGNING THE ROUND FUNCTION

- Strict Avalanche Criterion
  - An output bit j of an S-box should change with probability 0.5 when any single input bit i is inverted for all i, j
  - The algorithm should have good avalanche properties
- Bit Independence Criterion
  - Output bits j, k should change independently when any single input bit i is inverted for all i, j, k

BLOCK CIPHER DESIGN – DESIGN OF THE ROUND FUNCTION

- The Feistel block cipher uses a round function *f*, which uses Substitution Boxes
- It gets harder to cryptanalyze *f* as it increases in non-linearity
- Implementing the SAC and BIC criteria increases the strength of the confusion
- The key schedule should guarantee the SAC and BIC criterion for diffusion

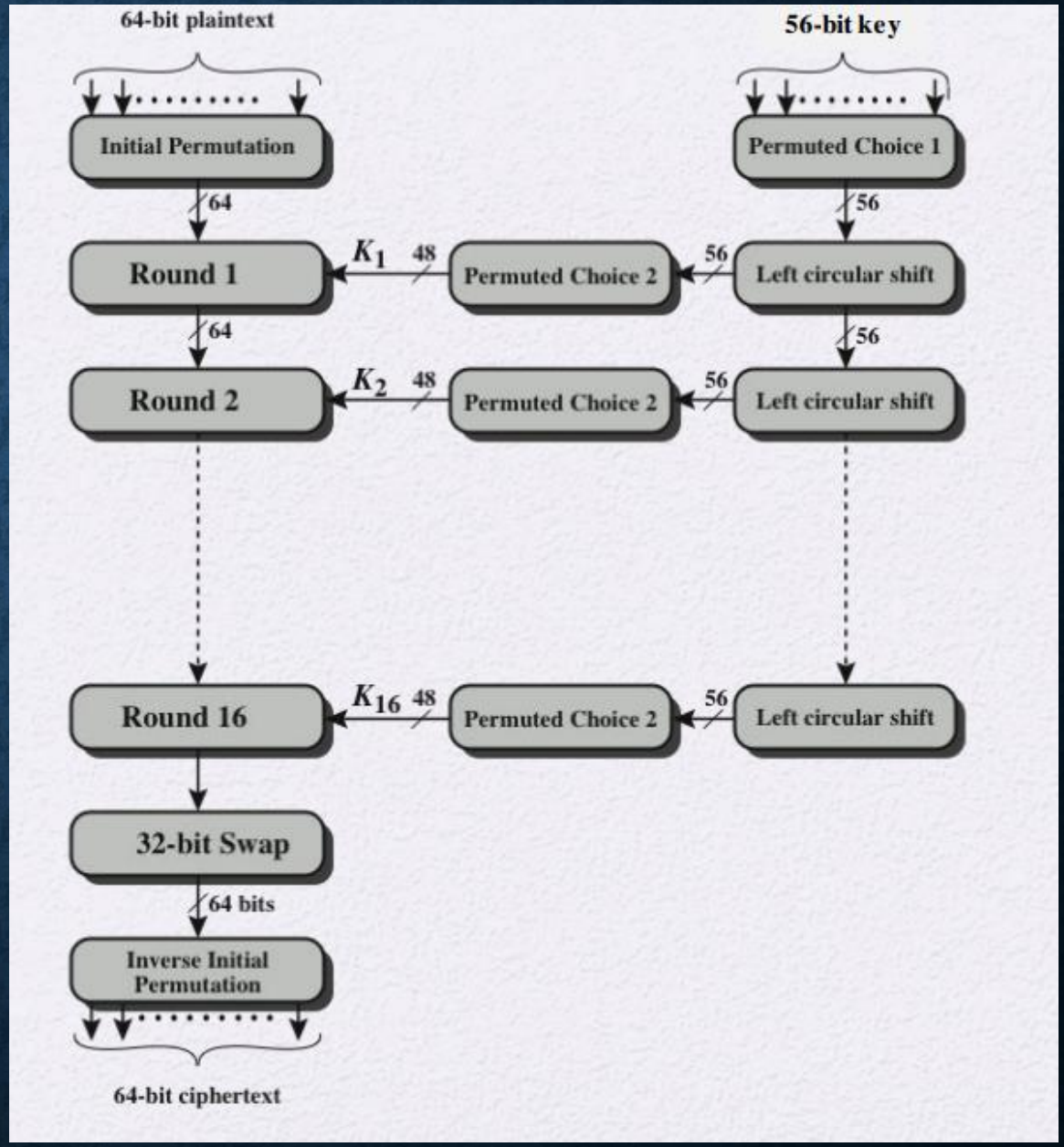
THE DATA ENCRYPTION STANDARD (DES)

- Issued in 1977 by the National Bureau of Standards (now NIST) as Federal Information Processing Standard 46
- The most widely used encryption scheme until the introduction of the Advanced Encryption Standard (AES) in 2001
- Algorithm is referred to as the Data Encryption Algorithm (DEA)
  - Data is encrypted in 64-bit blocks using a 56-bit key
  - The algorithm transforms 64-bit input in a series of steps into a 64- bit output
  - The same steps, with the same key, are used to reverse the encryption

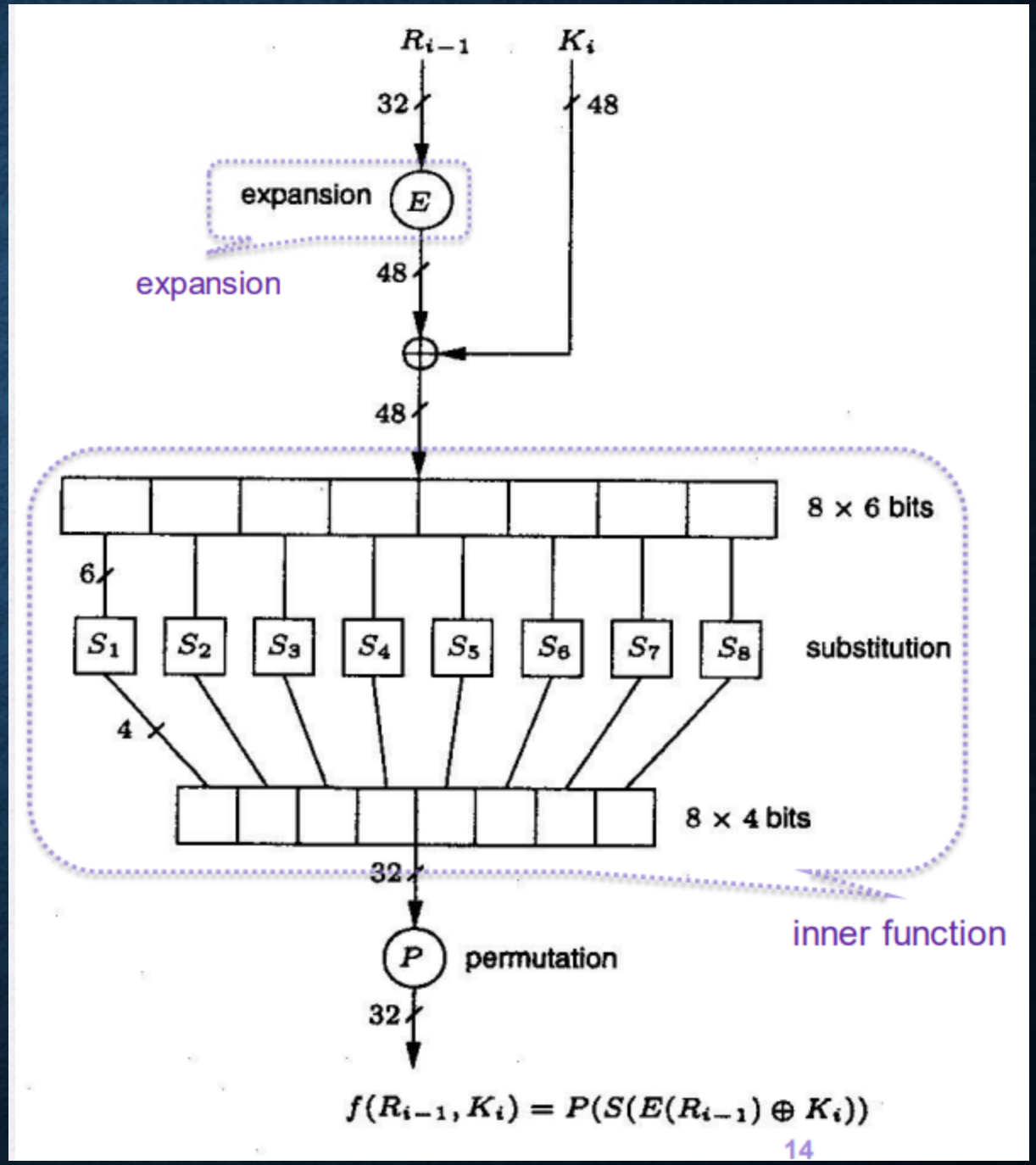
DES STRUCTURE

- The DES encryption/decyption process involves 16 rounds of operation
- For each round, a round-key of 48 bits is generated from the 56-bit key through 2 transformations – a left shift of either 1 or 2 bits (depending on the key schedule) and a Permute-Choice, that picks 48 of the 56 available bits.
- Before the 1st round, the 64 bit text is permuted (has its bits rearranged) through another Permute Choice Transformation.
- For each round
  - The previous right half is retained as the next round's left half.
  - The right half is sent throughthe Round Function and then XORED with the left half to produce the next round's right half.
- The Round function consists of
  - Expansion function applied on the right half
  - XOR with the round key
  - Substitution using an S-box
  - Permutation of the bits

DES ENCRYPTION ALGORITHM

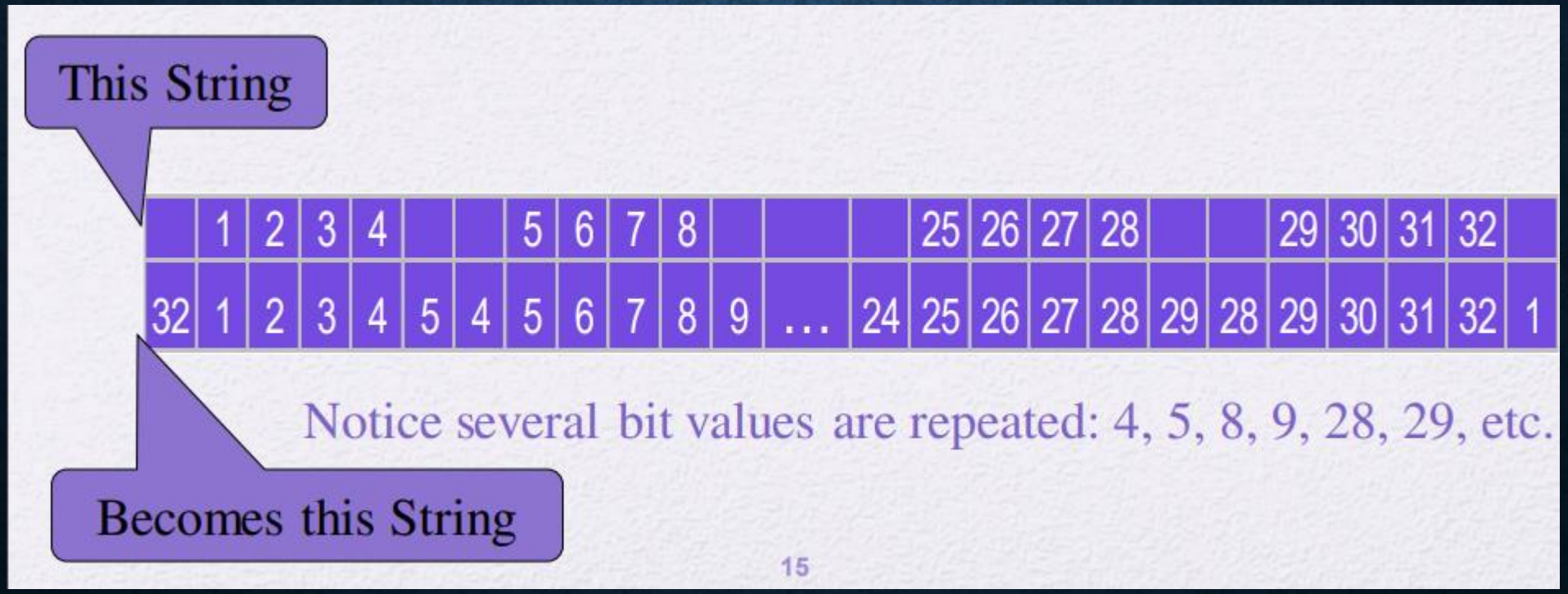


THE DES ROUND FUNCTION



THE EXPANSION FUNCTION

- Expand 32 bit input to 48 bits by adding a bit to the front and end of each 4 bit segment
- The missing bits are copies of the adjacent bits



S-BOXES

- A substitution box is a table (usually pre-computed), where the current bit-chunk is used to calculate an *i* and a *j* value.
- We index into row i and column j of the S-box, and replace the current bi-chunk with the value in the table at that index.
- For DES, the 48-bit intermediate value is divided into 6 8-bit chunks. The S-box is used to then build 8 4-bit chunks, forming the 32-bit output
- The outer 2 bits of each 6-bit chunk determine which row is used
- The inner 4 bits determine which column is used
- There are 8 different S-boxes, one for each 6-bit chunk

S-BOX EXAMPLE

Use bits 1 & 6 to select the row

Bits 2-5 to select the substitution

	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

KEY SCHEDULE

- INPUT: 56-bit key $K = k_1 , k_2 , \dots , k_{56}$
- OUTPUT: sixteen 48-bit keys: $K_1 , K_2 , \dots , K_{16}$
- The algorithm used for generating the key schedule combines and selects bits of K to generate the round keys.
- The 56-bit key is divided into two 28-bit halves, and in each successive round both halves are rotated by 1 or 2 bits and then 48-bits are selected by using a permuted choice-- for details see this page:

DES EXAMPLE

Round	*Ki*	*Li*	*Ri*
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

STRENGTH OF DES

- Attacks faster than Brute force
  - Differential cryptanalysis (requires ~ 2^{47} chosen plaintexts)
  - Linear cryptanalysis (requires ~2^{47} known plaintexts)
  - Timing attacks: encryption or decryption take slightly different amounts of time for different inputs
- It appears unlikely that any of these attacks will ever be successful against more powerful versions of DES such as triple DES