BEACH

CECS 378: Intro to Computer Security Principles

Lecture 4

Louis Uuh

Week 5

DES Key Details

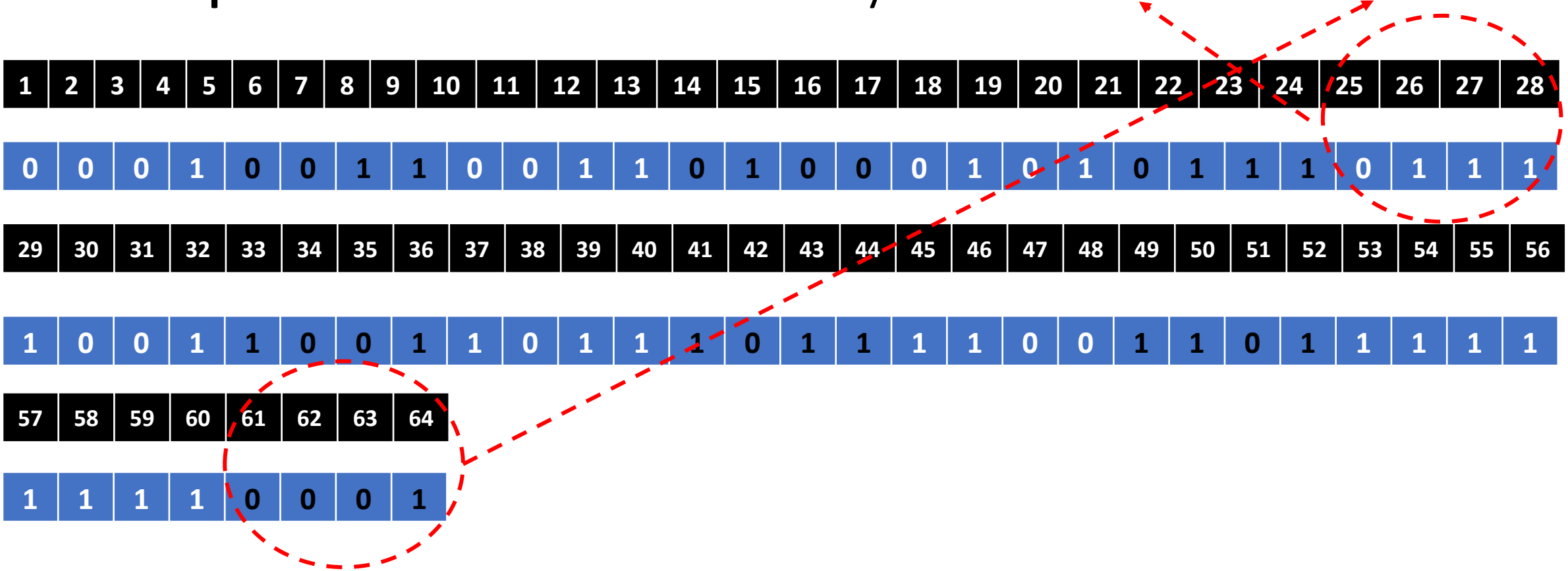
BEACH

- DES operates on the 64-bit blocks using *key* sizes of 56- bits
- Keys are actually stored as being 64 bits long
  - Every 8 bit is not used (E.g. bit 8, 16, 24, 32, 40, 48, 56 and 64)
- Number every bit from left to right (1 to 64)
- The 8 bits mentioned above will get eliminated when we create the subkeys

DES Key Example

BEACH

- **Example:** Let **K** be the hexadecimal key **K** = 133457799BBCDFF1



DES Key Permuted

BEACH

- 64 – bit key is permuted according to the following table
- First entry in the table is "57", this means that the 57th bit of the original key **K** becomes the first bit of the permuted key **K+**

PC–1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

DES Key Permuted

BEACH

- Bit 49 (Original key) → Becomes 2nd bit of the permuted key
- Bit 41 (Original key) → Becomes 3rd bit of the permuted key
- Bit 4 (Original key) → Becomes last bit of the permuted key

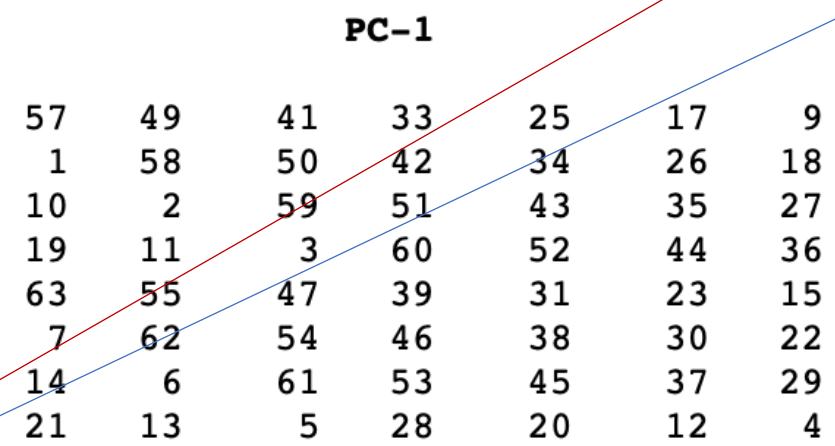
PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

DES Key Permuted

BEACH

- From the original 64-bit key
- **K** = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001



- We get the 56-bit permutation
- **K+** = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

DES Key Steps

BEACH

- Split the key into left and right halves, C_0 and D_0 each half containing 28 bits
- $\boldsymbol{C_0}$ = 1111000 0110011 0010101 0101111
  $\boldsymbol{D_0}$ = 0101010 1011001 1001111 0001111
- Create sixteen blocks $\boldsymbol{C_n}$ and $\boldsymbol{D_n}$, 1<=$\boldsymbol{n}$<=16
- Each pair of blocks $\boldsymbol{C_n}$ and $\boldsymbol{D_n}$ is formed from the previous pair $\boldsymbol{C_{n-1}}$ and $\boldsymbol{D_{n-1}}$
- Do a left shift based on this schedule, by moving each bit one place to the left, except for the first bit which is recycled to the end of the block

Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits

DES Key Shifting

BEACH

- C_0 = 1111000 0110011 0010101 0101111

  D_0 = 0101010 1011001 1001111 0001111

- C_1 = 1110000 1100110 0101010 1011111

  D_1 = 1010101 0110011 0011110 0011110

Shifting

Rounds	Shift
1, 2, 9, 16	one bit
Others	two bits

DES Key 2nd Permutation

BEACH

- Now form the keys Kn, for 1<=n<=16
- Apply the permutation based on the second table

PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

DES Key 2nd Permutation

BEACH

- C_1D_1 = 1110000 1100110 0101010 1011111 1010101 0110011 0011110 0011110
- K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

PC–2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32