Simplified DES

CS-480b

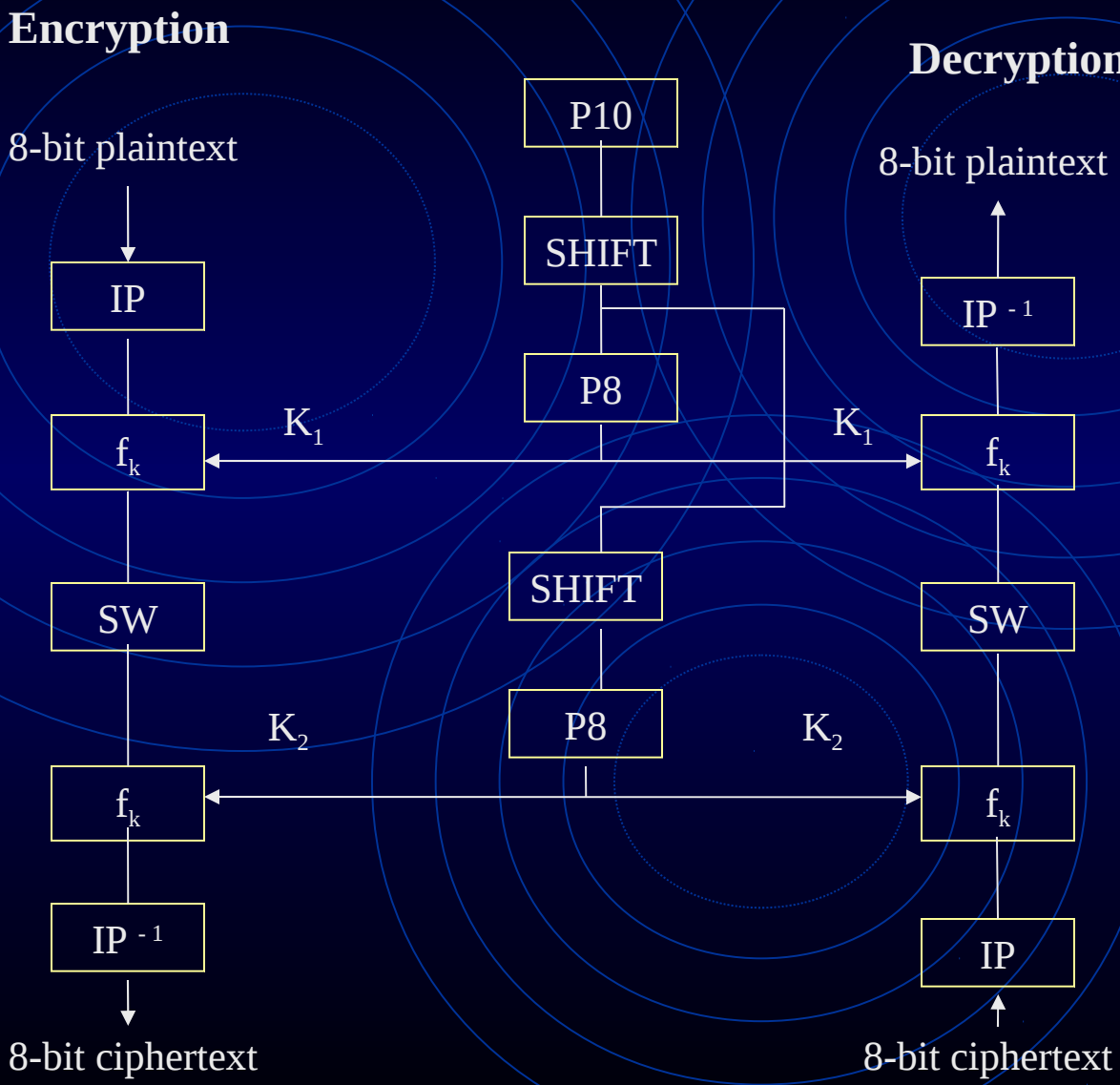
Network Security

Dick Steflik

What is Simplified DES

- Developed 1996 as a teaching tool
  - Santa Clara University\
    - Prof. Edward Schaefer
  - Takes an 8-bit block plaintext, a 10 –bit key and produces an 8-bit block of ciphertext
  - Decryption takes the 8-bit block of ciphertext, the same 10-bit key and produces the original 8-bit block of plaintext

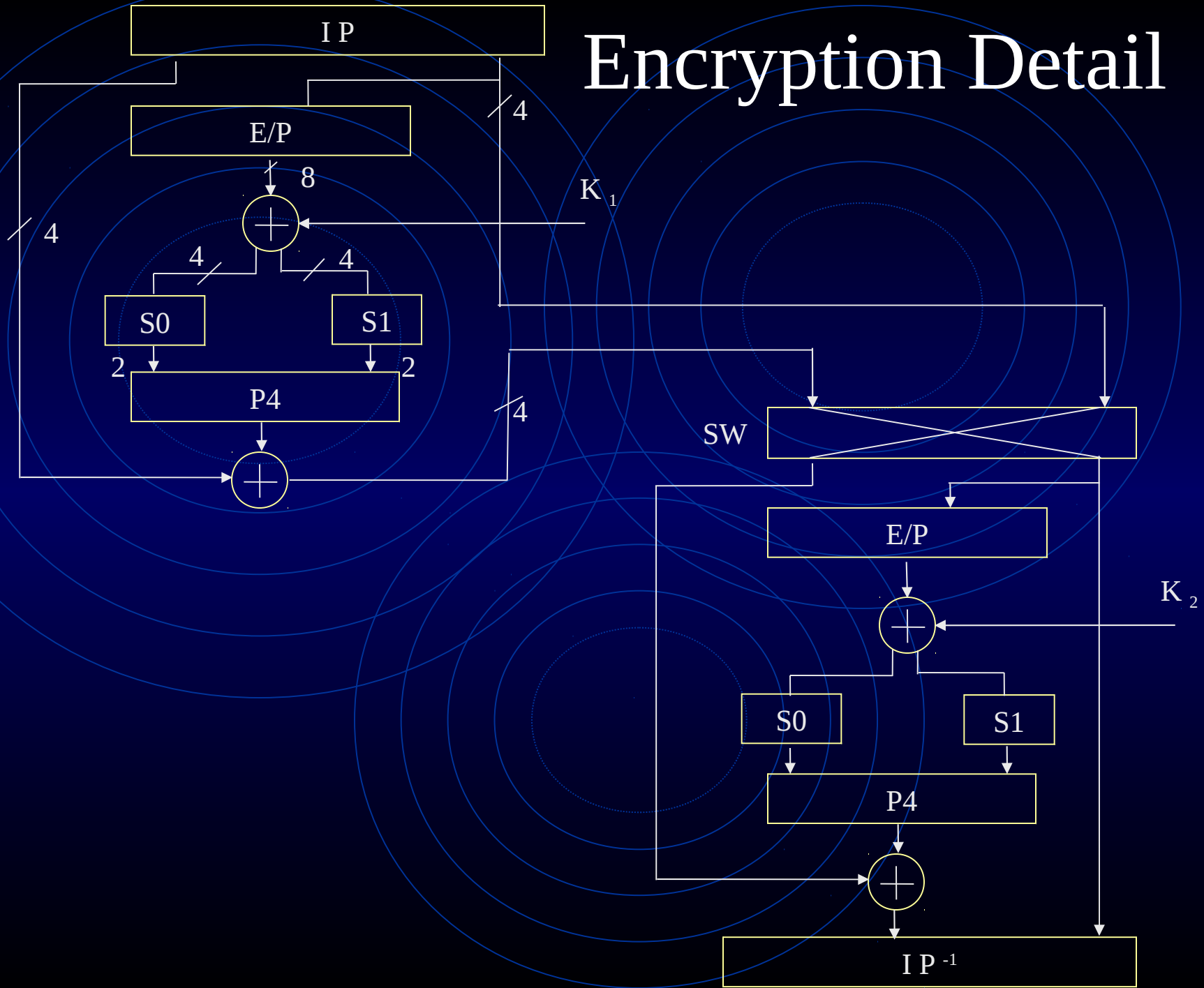
S-DES Scheme


Encryption
Decryption
P10
8-bit plaintext
8-bit plaintext
SHIFT
IP
IP - 1
P8
K1
K1
fk
fk
SW
SW
SHIFT
K2
P8
K2
fk
fk
IP - 1
IP
8-bit ciphertext
8-bit ciphertext

Five Functions to Encrypt

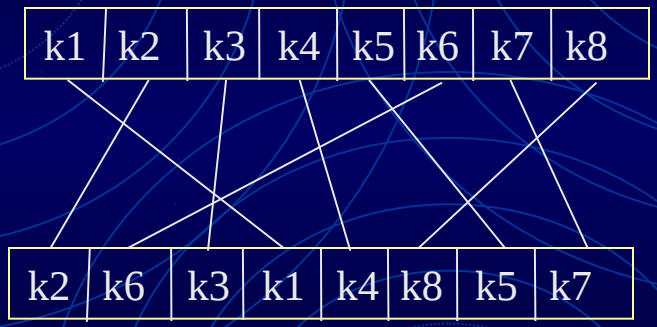
- IP – an initial permutation
- f_k - a complex, 2-input function
- SW – a simple permutation that swaps the two nybles
- f_k - a complex, 2-input function; again
- IP – inverse permutation of the initial permutation

Encryption Detail



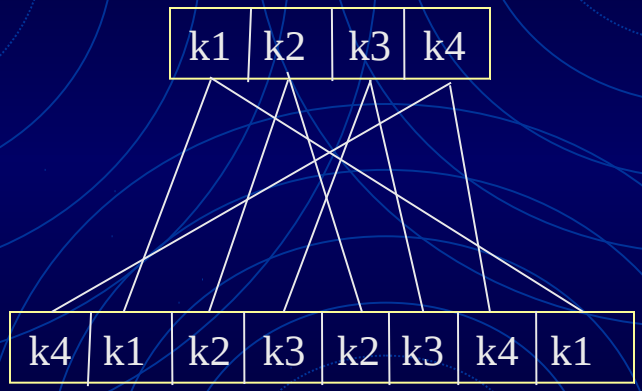
Initial Permutation (IP)

Move the bits of the original character around a little…

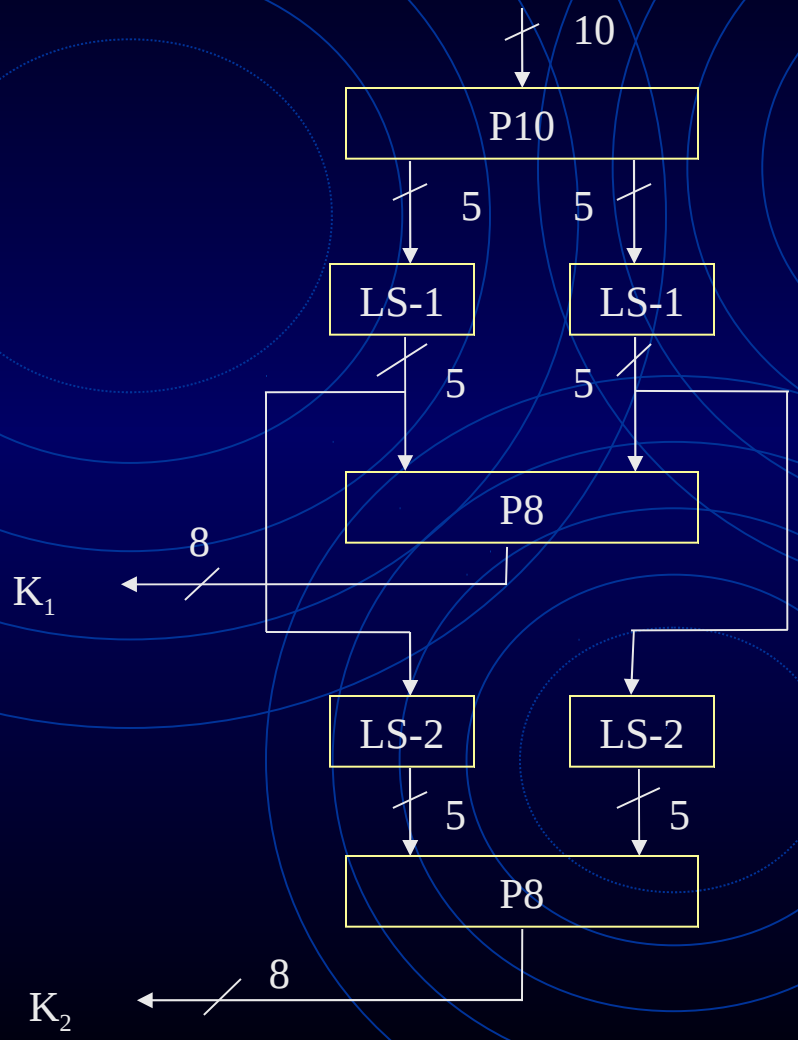


Expansion/Permutation (E/P)

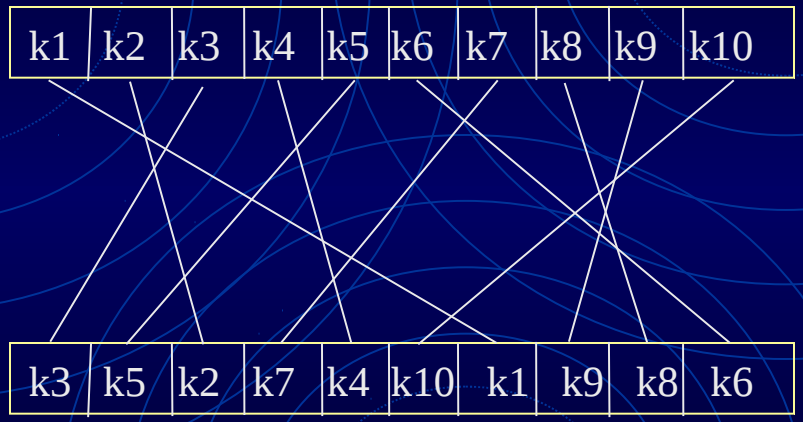
Expand 4 bits into 8 and permutate them…



Key Generation

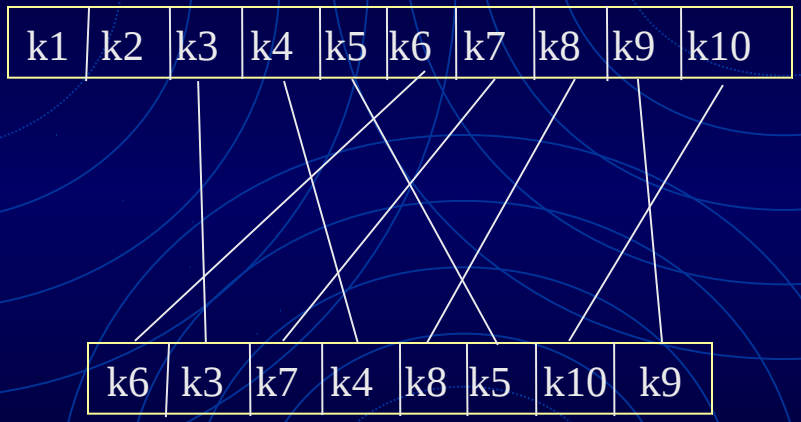


P10 Permutation



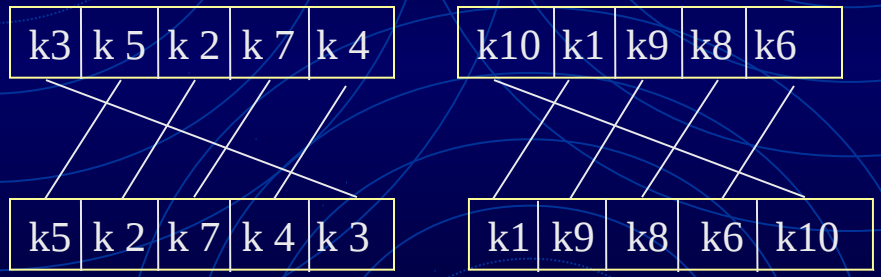
P8 Permutation

Permutate 10 into 8



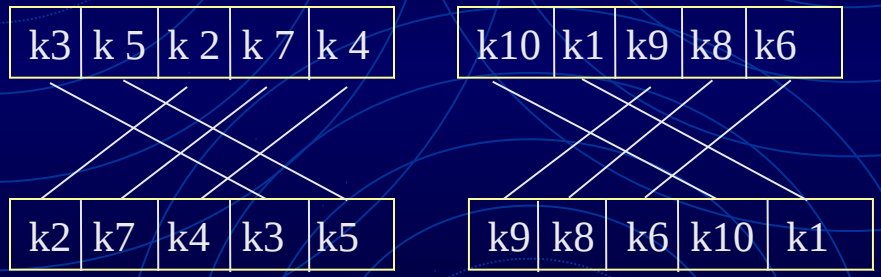
LS-1

Left circular shift 1 each 5 bit group



LS-2

Left circular shift 2 each 5 bit group



Substitution Boxes

S0

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

S1

0	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3