

The background is a solid dark blue. It features a decorative pattern of concentric circles and dashed lines. There are two main sets of concentric circles, one on the left and one on the right, each with a dashed line passing through its center. These dashed lines intersect to form an 'X' shape across the entire slide.

Simplified DES

CS-480b

Network Security

Dick Steflrik

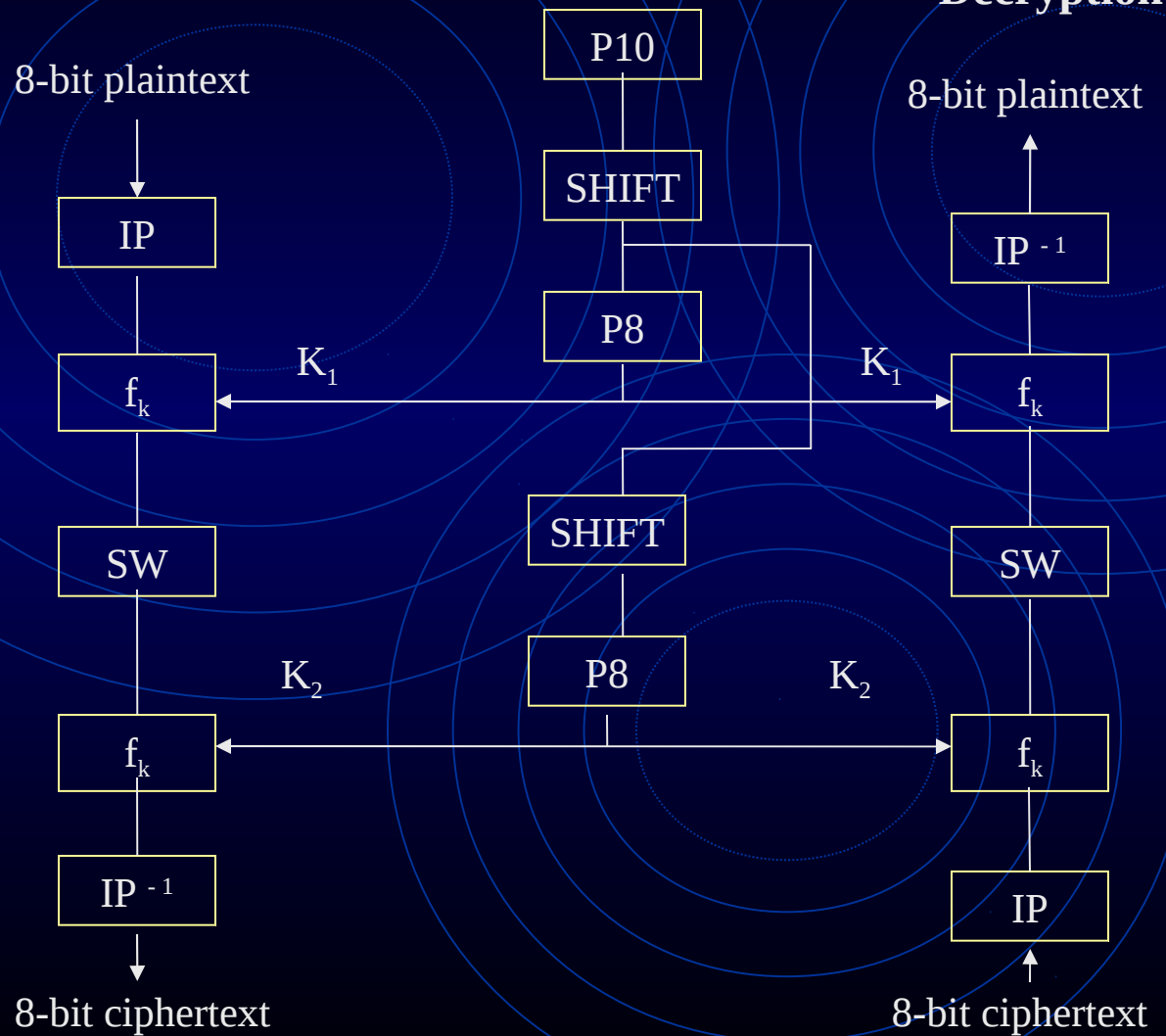
What is Simplified DES

- Developed 1996 as a teaching tool
 - Santa Clara University\ul> - 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

8-bit plaintext



Decryption

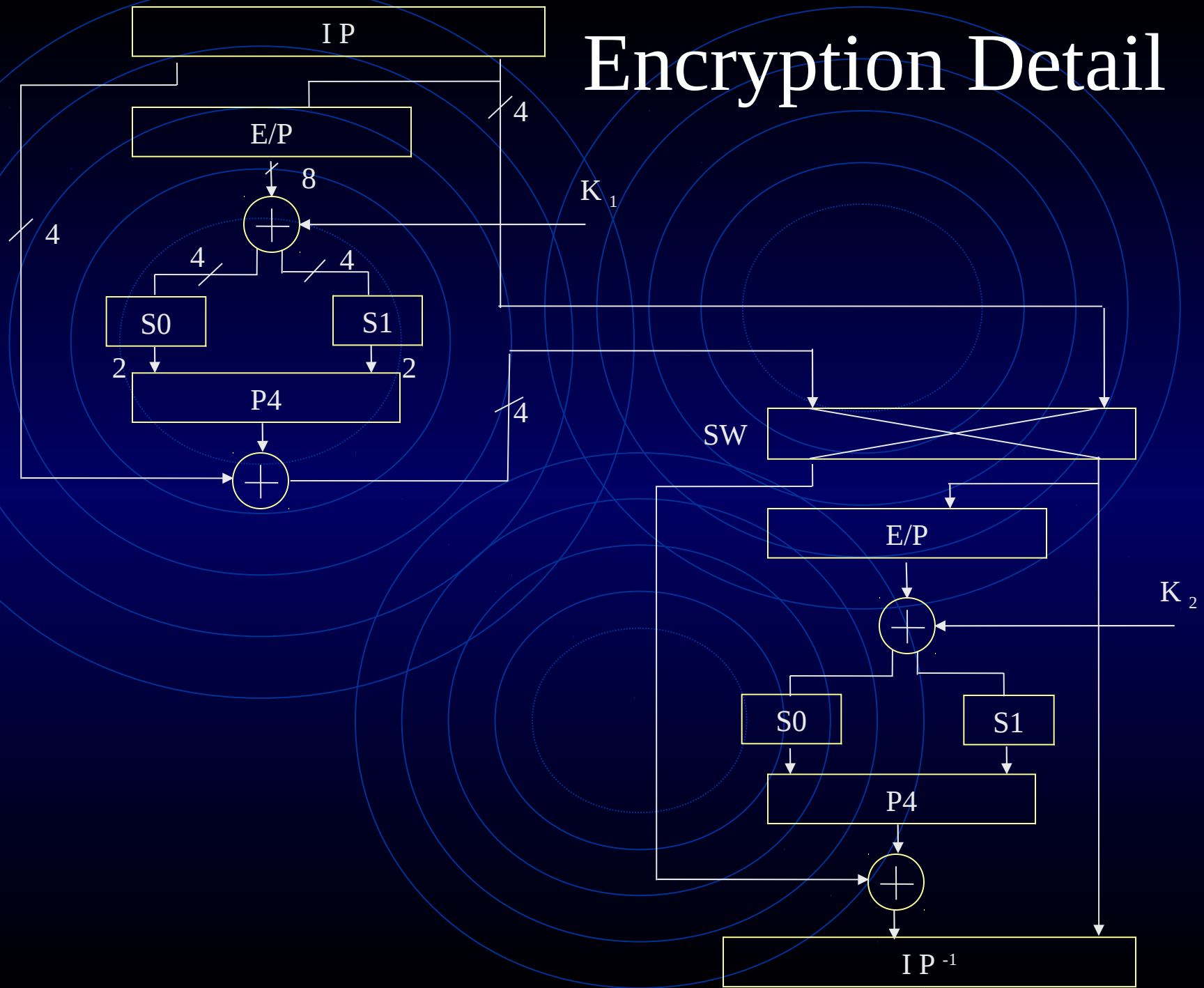
8-bit plaintext

8-bit ciphertext

Five Functions to Encrypt

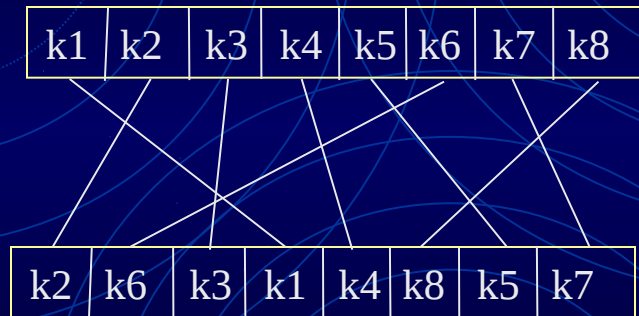
- IP – an initial permutation
- f_k - a complex, 2-input function
- SW – a simple permutation that swaps the two nybles
- f_k - a complex, 2-input function; again
- IP – inverse permutation of the initial permutation

Encryption Detail



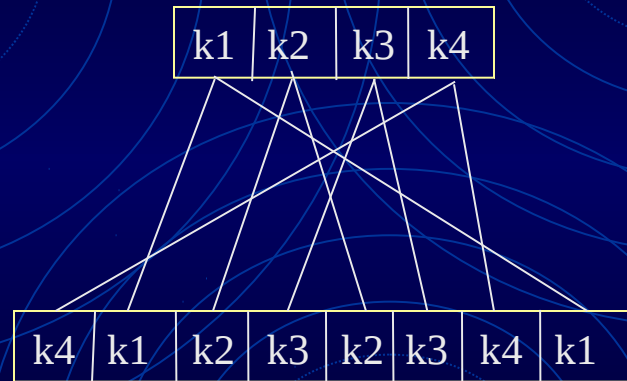
Initial Permutation (IP)

Move the bits of the original character around a little...

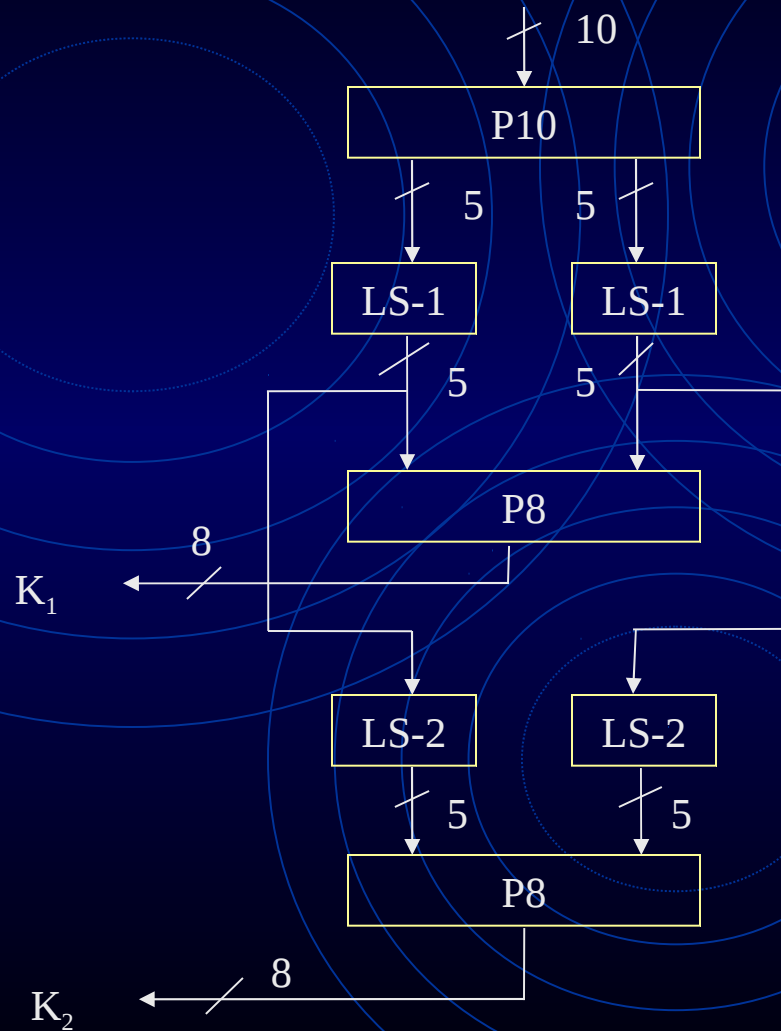


Expansion/Permutation (E/P)

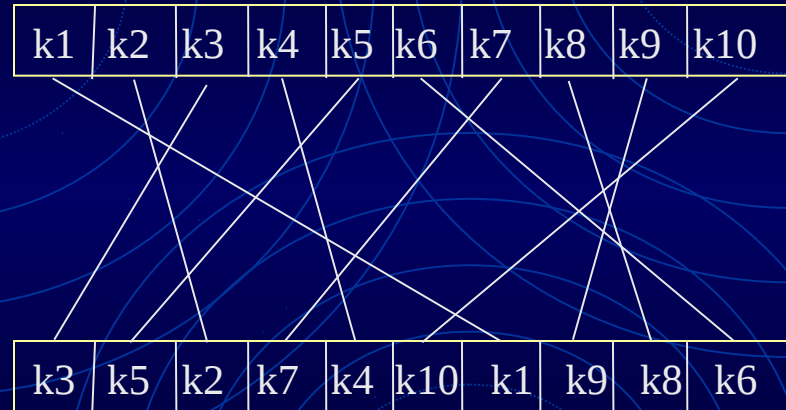
Expand 4 bits into 8 and permute them...



Key Generation

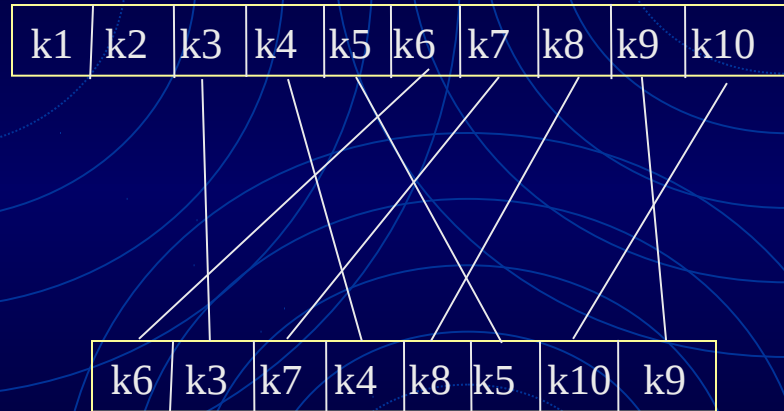


P10 Permutation



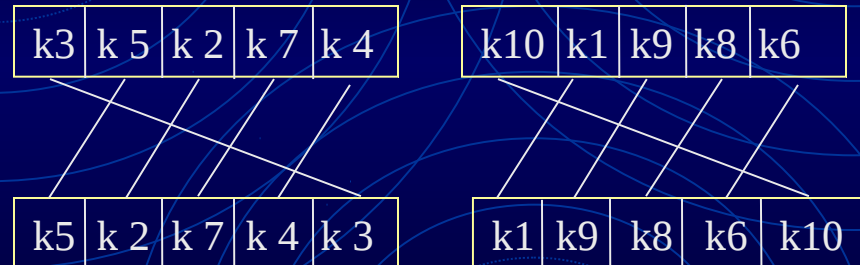
P8 Permutation

Permute 10 into 8



LS-1

Left circular shift 1 each 5 bit group



LS-2

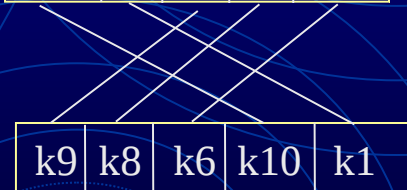
Left circular shift 2 each 5 bit group

k3	k5	k2	k7	k4
----	----	----	----	----

k10	k1	k9	k8	k6
-----	----	----	----	----

k2	k7	k4	k3	k5
----	----	----	----	----

k9	k8	k6	k10	k1
----	----	----	-----	----



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