

الشرح العملي التطبيقي لـ DES

اليوم تطبيق عملي للتشفير بـ DES

يعتمد شرحي على أنك على الأقل تفهمت الموضوع السابق

لنبدأ على بركة الله ...

المعطيات : يوجد معطيات أخرى على الرخصة للتسهيل

Plain text = P = [00000000]

P4 = [2431]

IP = [26314857] ; IP-1=[41357286]

E/P= [41232341]

P8 = [6 3 7 4 8 5 10 9]

S0=

	00	01	10	11
00	1	0	3	2
01	3	2	1	0
10	0	2	1	3
11	3	1	3	2

S1=

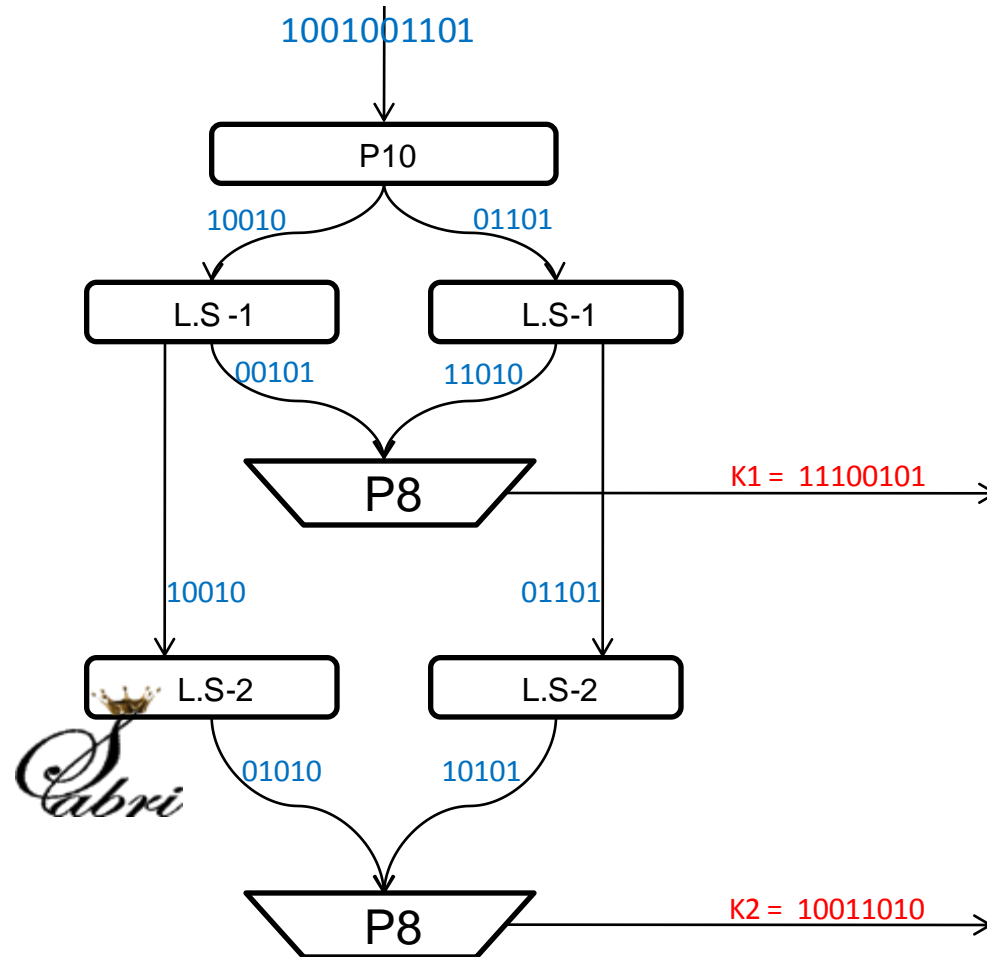
	00	01	10	11
00	0	1	2	3
01	2	0	1	3
10	3	0	1	0
11	2	1	0	3

المطلوب :

Give Key 1 & 2 ; Cipher text ...

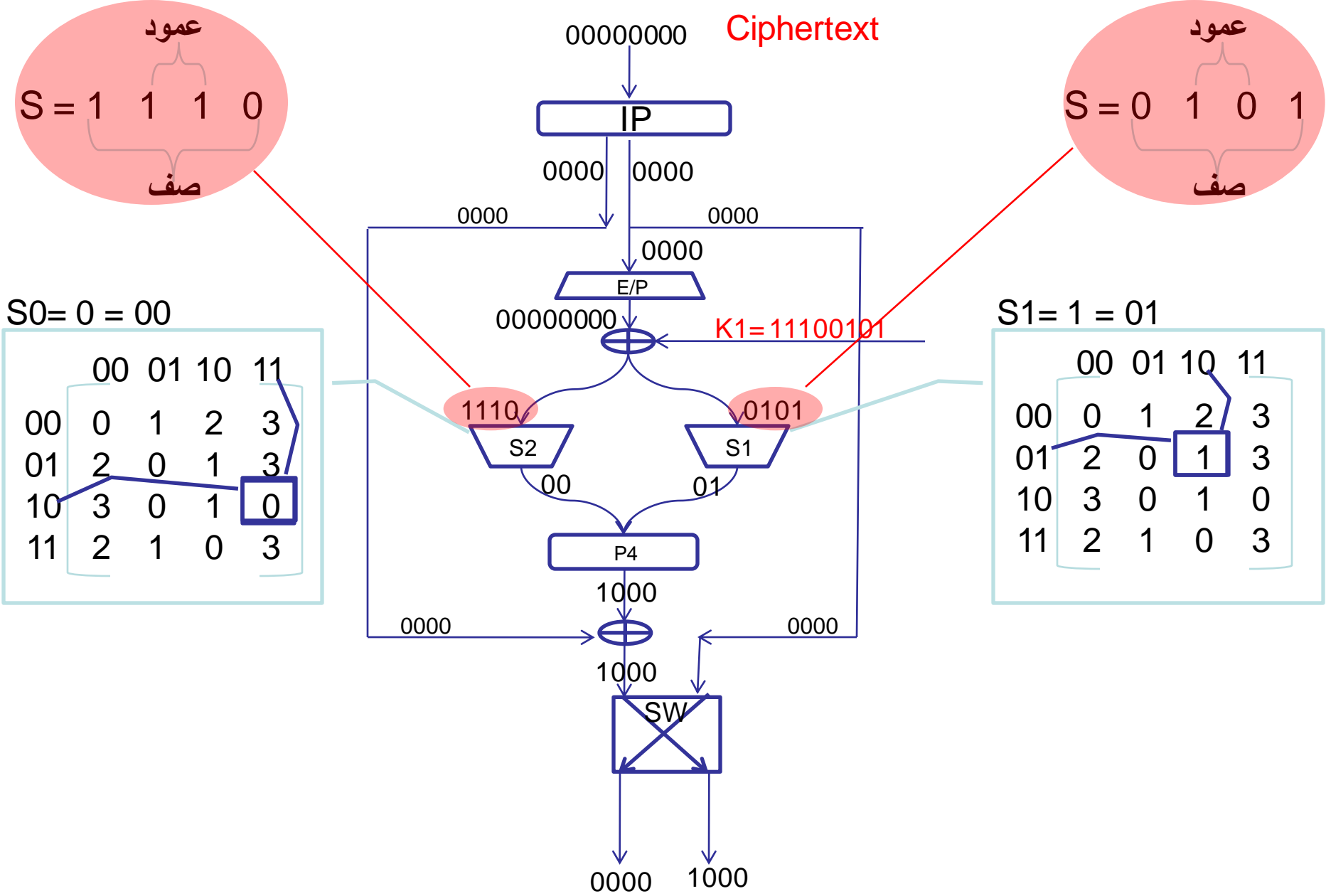
To Find (Generate) The keys

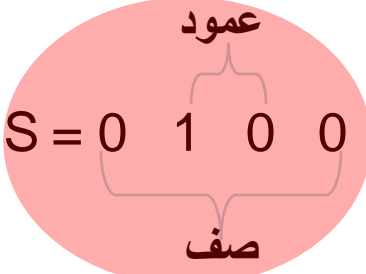
Key Generation



$K1 = 11100101$

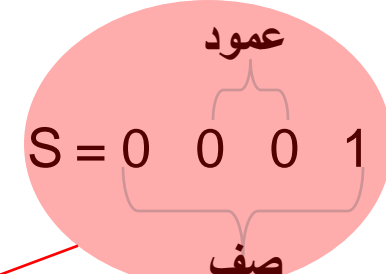
$K2 = 10011010$





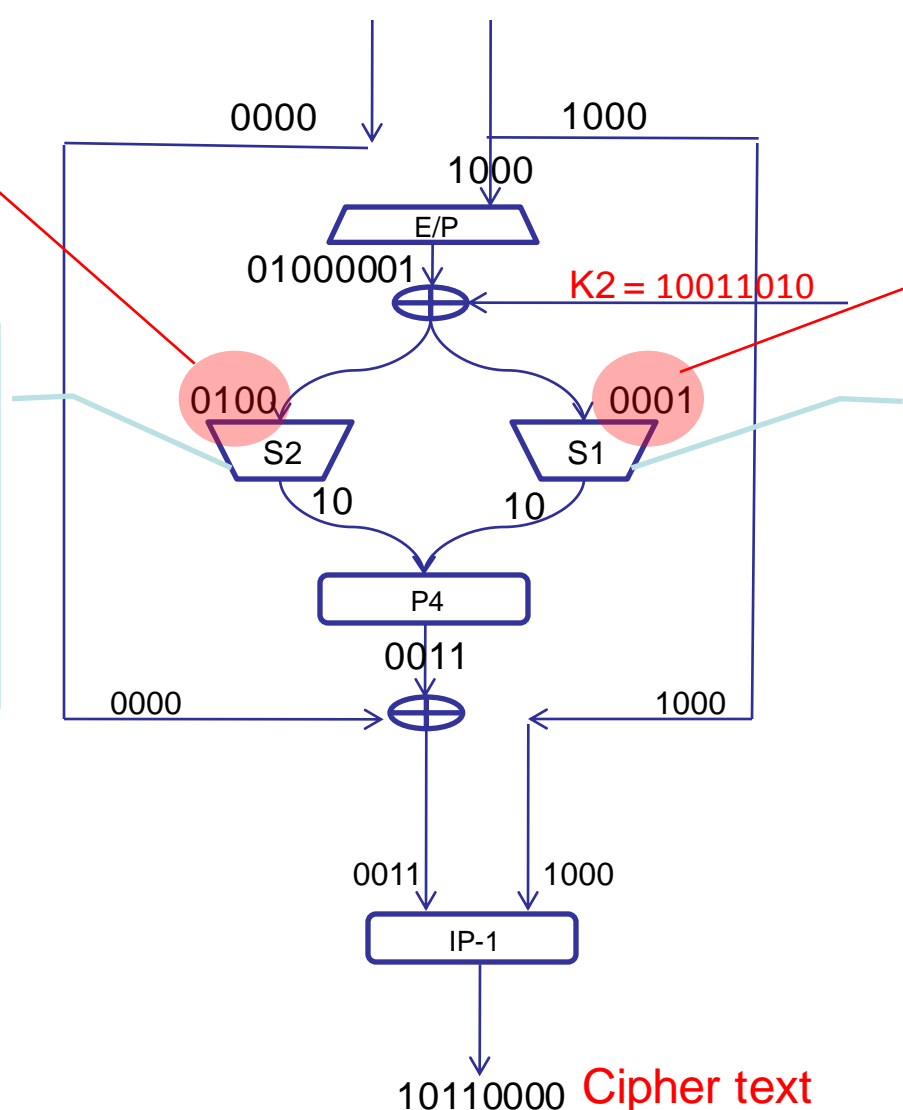
S0 = 2 = 10

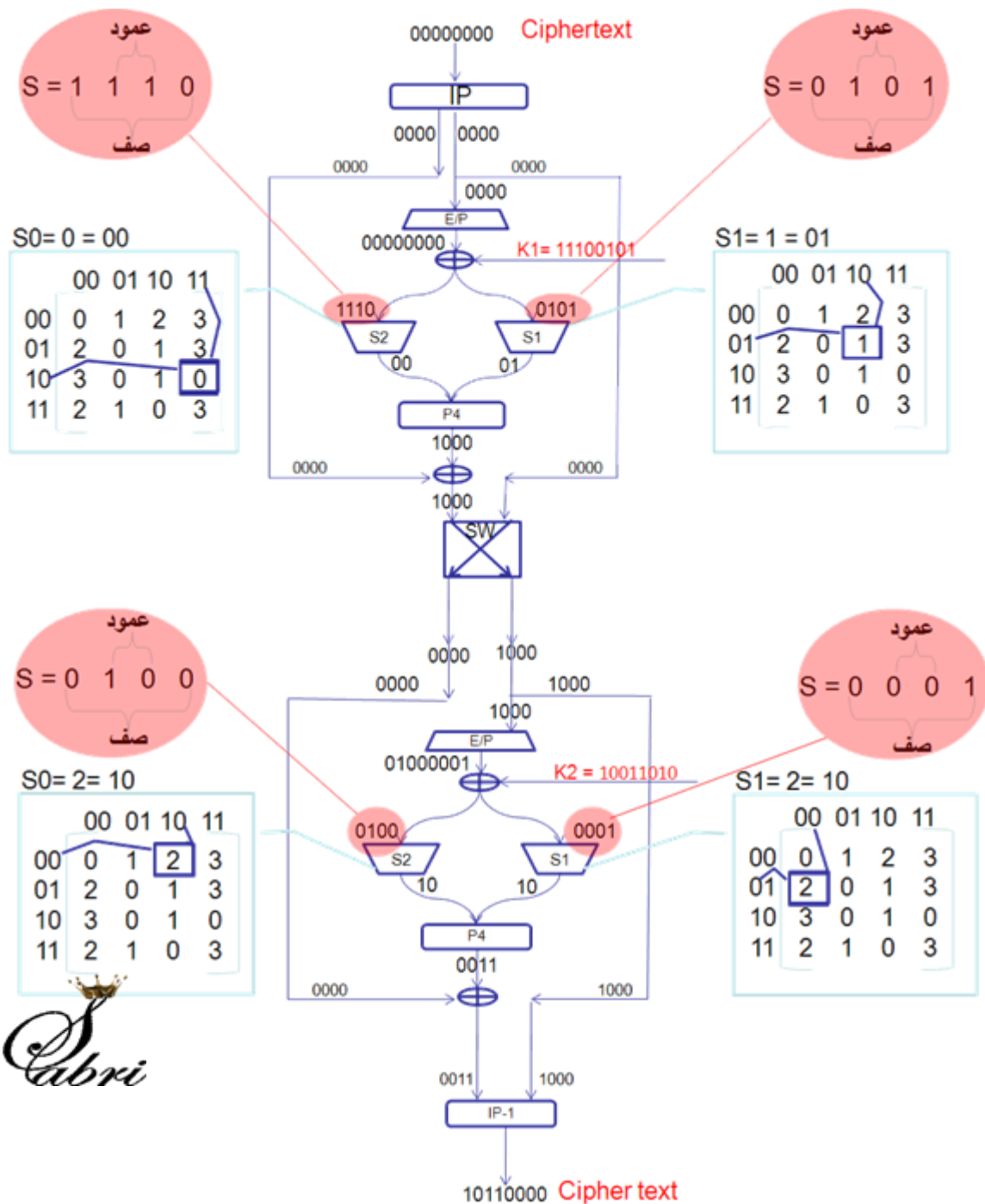
	00	01	10	11
00	0	1	2	3
01	2	0	1	3
10	3	0	1	0
11	2	1	0	3



S1 = 2 = 10

	00	01	10	11
00	0	1	2	3
01	2	0	1	3
10	3	0	1	0
11	2	1	0	3





المراجع :

• حبيب قلبي [William Stallings](#) و كتابه الأشهر بين نظرائه Cryptography and Network Security الإصدار الرابع

• www.king-sabri.net

للمراسلة : king-sabrii@hotmail.com

أسألكم الدعاء لي ولوالدي ...

