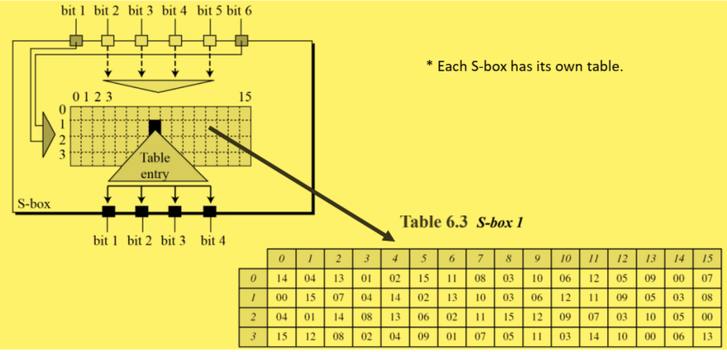
Q1

Illustrate how DES and AES implement substitution operation.



* Each S-box has its own table.

Table 6.3 *S-box 1*

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

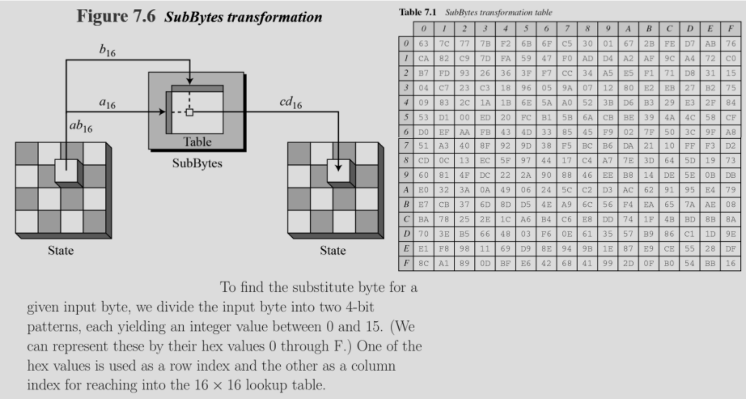


Figure 7.6 ***SubBytes transformation***

Table 7.1 *SubBytes transformation table*

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	CB	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

To find the substitute byte for a given input byte, we divide the input byte into two 4-bit patterns, each yielding an integer value between 0 and 15. (We can represent these by their hex values 0 through F.) One of the hex values is used as a row index and the other as a column index for reaching into the 16 × 16 lookup table.

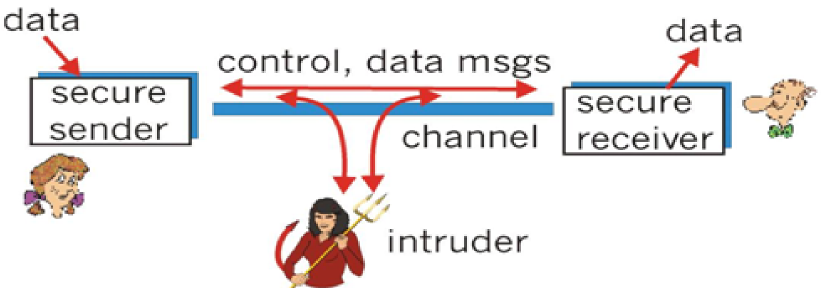
Define confusion and diffusion. How they are implemented in DES? (No diagram necessary).

Confusion ensures that even a small change in the input (plaintext or key) results in a significant change in the output (ciphertext). Diffusion ensures that changes in the plaintext or key affect a large portion of the ciphertext.

Confusion is implemented using S-Boxes in DES and Diffusion is accomplished through multiple rounds of permutation, substitution, and bitwise operations (XOR) applied to mix the input bits thoroughly.

Q2

Illustrate a security scenario using Bob, Alice and Trudy to show the need for encryption with authentication.



The intruder (attacker) can modify encrypt transmitted data in such a way that its meaning at the receiving end will change giving some kind of advantage to the intruder (attacker). This means that encrypted data need to be authenticated which not only avoid any changes in data but ensure that the transmitted data is actually from the sender.

a) Explain a scenario where encryption is not required but integrity and authentication is critical.

Release of some patch from any software vendor or any public announce through digital media. This does not need encryption but requires that the contents should remain the same and comes from the actual sender.

b) Illustration how a 128bit data is transformed in this case.

Labelled diagram required. This is a textual description instead. A 128 bit message digest is created using SHA-128 thus creating a unique hash for 128 bit data. Padding is not needed in this case as the data size exactly matches with the hash function size. This hash is encrypted with private key of the sender (to ensure authentication and nonrepudiation) and send along with the message.