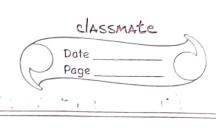
Test-1 CNS Roll nor 214101031. gs. Avalanche effect & effect in DES. It states that a single small change in the plain test or message. should have a cascading effect on. entire cipher test generation, So that the end cipher teset is totally different from the first cipher teset. This is a desirable trait in a. encryption algo, thus keys uniquely identify the plain test & authenticity can be verified just using ciple text. So a small change is iput leads to In DES ue have 16 sounds & 2 permutations

	classmate
	DatePage
(2)	214101031
7	To each and the in all hits are used
	to look we be the subsite of the
	In each sound, the input bits are used to look up for the output according to function.
	Janey or.
0 .	The a small change is subsequent
	This a small change in subsequent sounds lead to a totally different end cipher fesct.
	end eigher teset.
	1
	Thus having an avalanche effect-
	x x x x
	-, -, -, -, -, -, -, -, -, -, -, -, -, -
0.3,	Yes, a block cipher can be
	constoucted using a hash function
٠,	
	The feistal stoueture refers to
	the same cer se said above.
	one half
	The drey is used with a
1	The appear is used with a hush function on first part of teset block.
	of fesct block.
	S .



3	214101	03
	11	

Thes than is XORed with the
This than is XORed with the remaining half.
Since it heads the same direction
for function both for encumption
le de cruption. There & son 3.
for function both for en crupption & de cryption. There It was \$5.
Thus the hash function can
Thus the hash function can be used in block cipher as
explained.
x x x
A-DBMZ-MBNA @
B-> A MIZZMI @NB 6

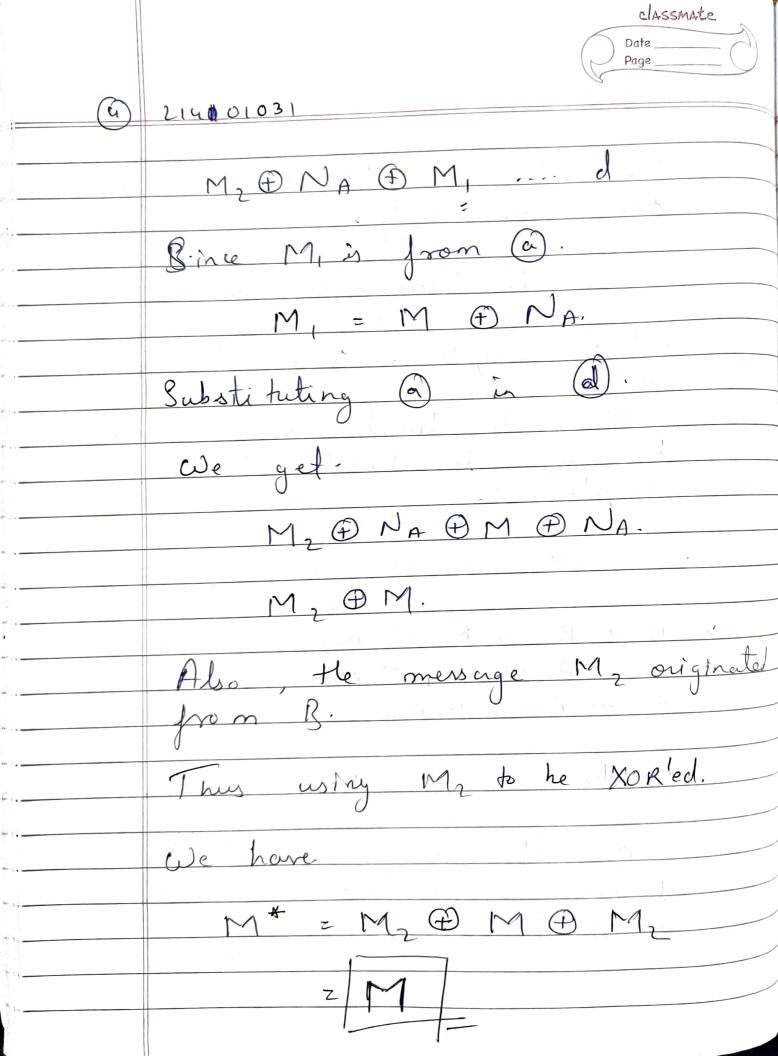
GY A-> BM_=M & NA --- (a)

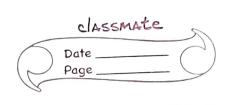
B-> A M_Z M_ & NB --- 6

A-> BMZ & NA C

a) Recovery for B=>.

Buill have to sats XOR tee Later received message with original message.





3	21410	1031

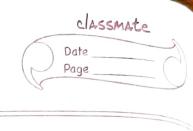
Thus Bis uble to retoire the mersage. M. He given way.

g. E. D.

b). No, this system is not secure as any one intercepting the messages has access to M, & And.

using these the original fest can be deciphered as shown.

Thus is system is not



9.2. Advantages & Dis advantage cif S-block is DES.

-> It offeres security as it

S. block is just no-linear purt which is XOR operations of ley plaintexed & cipler text