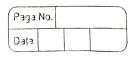
		Page No.		
		Date		
	Devanshu Surana			
· · ·	Pc-23, Panel C			
111	1032210755	F . 1		
		· · · · · · · ·	1	
+ 1, 1, 1.	ICS Lab A3 () ()		r ₀ .	
	The state of the s	: · a.		
	FAQIS			
	What is S-AES algorithm and how	it is	diff	esent
1.7-4	From AES algorithm?			
Ans.	Simplified AES (S-AES) is a reduced-	- roun	d vers	Sian
	of the AES algorithm. S-AES is design	ned f	or ed	luca.
6 6	-tional purposes and to help student	3 and	bea	innes
	understand the basic principles of	9 27A	n crust	hon
	without the complexity of the full 1	AES a	90 U.	
·	S-AES typically uses a smaller num!	ber o	f row	nds
	and a smaller key size compared t	to the	2 star	dara
	AES.	· 1		
. 7	in the second of the second agree of	. 1	= ",	
2.	Explain key generation in S-AES.	Ŧ		
Ans.	Key generation in S-AES:	7		
	1. Rey Selection: In 8-AES, we have t	o sele	ect st	ortest
	key often 8-bits in length. This	Key w	oill be	
1 ,	used for both encryption an	d de	eryptic	on.
	2. Key Expansion: Key expansion is a	critica	1 proc	less
() , () , () , () , () , ()	that generates round keys for	each	now)	d
	of encryption from the original	key.		
	of encryption from the original 3. Encryption key: The selected short k directly for the initial round of	ey is	used	
	directly for the initial round i	of encry	yption !	ìn
	S-HES.		J	
	4. Decryption key: We can use the same	short	Key &	br
	4. Decryption key: We can use the same decryption as well since the symmetric.	e algo	orithm	js
	symmetric.	V		
				ı



3. Explain Encryption in S-AES.

Ans. 1. Initial Round: The plaintext is combined with the first part of the key using simple bitwise XDR operation. 2. i) Substitution: Each byte of the data is substituted with a corresponding value from a fixed s-box. ii) Permutation: The bytes are rearranged: 3. In the last round, the remaining part of the key is combined with the data using another top operation. 4. Output: The result of the final round is the cipher text, which represents the encrypted data. 4. Explain Decryption in S-AES.

Ans. 1. Initial Round: The cipher text is combined with the last part of the key using a xor operation to reverse the final round of encryption.

2. The main rounds of decryption reverse the permutation -ion and substitution operations from the encryption process. 3. The decryption process concludes with the rethe key is xored with the key data to obtain the original plaintext. The result of the final round of decryption should -d be the original plaintext, which matches the input data before encryption.