((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following Algorithms does not belong to symmetric encryption?
((OPTION_A)) THIS IS MANDATORY OPTION	3DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	RC5
((OPTION_D)) This is optional	IDEA
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Assymmetric Encryption: Why can a message encrypted with the Public Key only be decrypted with the receiver's appropriate Private Key?
((OPTION_A)) THIS IS MANDATORY OPTION	Not true, the message can also be decrypted with the Public Key.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	A so called "one way function with back door" is applyed for the encryption
((OPTION_C)) This is optional	The Public Key contains a special function which is used to encrypt the message and which can only be reversed by the appropriate Private Key.
((OPTION_D)) This is optional	The encrypted message contains the function for decryption which identifies the Private Key.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	An one-way function is a function which a computer can calculate quickly, but whose reversal would last months or years. An one-way function with back door can be reversed with the help of a couple of additional information (the back door), but scarcely

	without this information. The information for the back door is contained in the private Key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the largest disadvantage of the symmetric Encryption?
((OPTION_A)) THIS IS MANDATORY OPTION	More complex and therefore more time-consuming calculations.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Problem of the secure transmission of the Secret Key
((OPTION_C)) This is optional	Less secure encryption function.
((OPTION_D)) This is optional	Isn't used any more
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION	As there is only one key in the symmetrical encryption, this must

)) This is also optional	be known by both sender and recipient and this key is sufficent to decrypt the secret message. Therefore it must be exchanged between sender and receiver in such a manner that an unauthorized person can in no case take possesion of it.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which is the principle of the encryption using a key?
((OPTION_A)) THIS IS MANDATORY OPTION	The key indicates which funcion is used for encryption. Thereby it is more difficult to decrypt a intercepted message as the function is unknown.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	The key contains the secret function for encryption including parameters. Only a password can activate the key.
((OPTION_C)) This is optional	All functions are public, only the key is secret. It contains the parameters used for the encryption resp. decryption.
((OPTION_D)) This is optional	The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption.
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or	C

E	
((EXPLANATION)) This is also optional	The encoding of a message is calculated by an algorithm. If always the same algorithm would be used, it would be easy to crack intercepted messages. However, it isn't possible to invent a new algorithm whenever the old one was cracked, therefor the possibility to parameterize algorithms is needed and this is the assignment of the key. All algorithms must be public, only the keys are secret (principle of Kerckhoff, Dutch cryptographer during 19th century).

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	If the sender and receiver use different keys, the system is referred to as conventional cipher system
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Such a system is called asymmetric, two-key, or public-key cipher system

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Use Caesar's Cipher to decipher the following HQFUBSWHG WHAW
((OPTION_A)) THIS IS MANDATORY OPTION	ABANDONED LOCK
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ENCRYPTED TEXT
((OPTION_C)) This is optional	ABANDONED TEXT
((OPTION_D)) This is optional	ENCRYPTED LOCK
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Caesar Cipher uses C =(p+3) mod 26 to encrypt.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Caesar Cipher is an example of
((OPTION_A)) THIS IS MANDATORY OPTION	Poly-alphabetic Cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Mono-alphabetic Cipher
((OPTION_C)) This is optional	Multi-alphabetic Cipher
((OPTION_D)) This is optional	Bi-alphabetic Cipher
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Caesar Cipher is an example of Mono-alphabetic cipher, as single alphabets are encrypted or decrypted at a time.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Monoalphabetic ciphers are stronger than Polyalphabetic ciphers because frequency analysis is tougher on the former.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Monoalphabetic ciphers are easier to break because they reflect the frequency of the original alphabet.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis
((OPTION_A)) THIS IS MANDATORY OPTION	Random Polyalphabetic, Plaintext, Playfair
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Random Polyalphabetic, Playfair, Vignere
((OPTION_C)) This is optional	Random Polyalphabetic, Vignere, Playfair, Plaintext
((OPTION_D)) This is optional	Random Polyalphabetic, Plaintext, Beaufort, Playfair
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Random Polyalphabetic is the most resistant to frequency analysis, followed by Vignere, Playfair and then Plaintext.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	On Encrypting “thepepsiisintherefrigerator” using Vignere Cipher System using the keyword “HUMOR” we get cipher text-
((OPTION_A)) THIS IS MANDATORY OPTION	abqdnwewuwjphfvrrtrfznsdokvl
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	abqdvmwuwjphfvvyyrfznydokvl
((OPTION_C)) This is optional	tbqyrvmwuwjphfvvyyrfznydokvl
((OPTION_D)) This is optional	baiuvmwuwjphfoeiyrfznydokvl
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Cipher text:= Ci = Pi + ki mod m (mod 26).

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	On Encrypting “cryptography” using Vignere Cipher System using the keyword “LUCKY” we get cipher text
((OPTION_A)) THIS IS MANDATORY OPTION	nlazeiibljji
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	nlazeiibljii
((OPTION_C)) This is optional	olaaeiibljki
((OPTION_D)) This is optional	mlaaeiibljki
((OPTION_E)) This is optional. If optional keep empty so that	

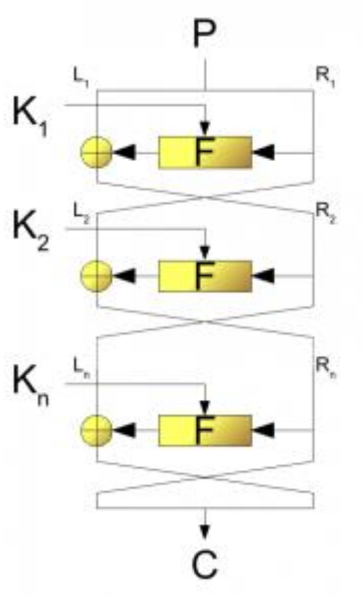
system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Cipher text:= Ci = Pi + ki mod m (mod 26).

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Confusion hides the relationship between the ciphertext and the plaintext.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Confusion hides the relationship between the ciphertext and the key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The S-Box is used to provide confusion, as it is dependent on the unknown key.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	false
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that	

system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The S-Box is used to provide confusion, as it is dependent on the unknown key. The P-Box is fixed, and there is no confusion due to it, but it provides diffusion.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	This is an example of  P L1 R1 K1 F L2 R2 K2 F Ln Rn Kn F C
((OPTION_A)) THIS IS MANDATORY OPTION	SP Networks
((OPTION_B)) THIS IS ALSO MANDATORY	Feistel Cipher

OPTION	
((OPTION_C)) This is optional	Hash Algorithm
((OPTION_D)) This is optional	Hill Cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following slows the cryptographic algorithm – 1) Increase in Number of rounds 2) Decrease in Block size 3) Decrease in Key Size 4) Increase in Sub key Generation
((OPTION_A)) THIS IS MANDATORY OPTION	1 and 3
((OPTION_B)) THIS IS ALSO MANDATORY	2 and 3

OPTION	
((OPTION_C)) This is optional	3 and 4
((OPTION_D)) This is optional	2 and 4
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Increase in any of the above 4 leads to slowing of the cipher algorithm i.e. more computational time will be required.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES follows
((OPTION_A)) THIS IS MANDATORY OPTION	Hash Algorithm
((OPTION_B)) THIS IS ALSO MANDATORY	Caesars Cipher

OPTION	
((OPTION_C)) This is optional	Feistel Cipher Structure
((OPTION_D)) This is optional	SP Network
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The DES Algorithm Cipher System consists of ____________rounds (iterations) each with a round key
((OPTION_A)) THIS IS MANDATORY OPTION	12
((OPTION_B)) THIS IS ALSO MANDATORY	18

OPTION	
((OPTION_C)) This is optional	9
((OPTION_D)) This is optional	16
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The DES Algorithm Cipher System consists of 16 rounds (iterations) each with a round key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The DES algorithm has a key length of
((OPTION_A)) THIS IS MANDATORY OPTION	128 Bits
((OPTION_B)) THIS IS ALSO MANDATORY	32 Bits

OPTION	
((OPTION_C)) This is optional	64 Bits
((OPTION_D)) This is optional	16 Bits
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm, although the key size is 64 bits only 48bits are used for the encryption procedure, the rest are parity bits.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY	FALSE

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	56 bits are used, the rest 8 bits are parity bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm the round key is ___________ bit and the Round Input is _____________bits.
((OPTION_A)) THIS IS MANDATORY OPTION	48, 32
((OPTION_B)) THIS IS ALSO MANDATORY	64,32

OPTION	
((OPTION_C)) This is optional	56, 24
((OPTION_D)) This is optional	32, 32
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The round key is 48 bits. The input is 32 bits

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via _____________
((OPTION_A)) THIS IS MANDATORY OPTION	Scaling of the existing bits
((OPTION_B)) THIS IS ALSO MANDATORY	Duplication of the existing bits

OPTION	
((OPTION_C)) This is optional	Addition of zeros
((OPTION_D)) This is optional	Addition of ones
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The round key is 48 bits. The input is 32 bits. This input is first expanded to 48 bits (permutation plus an expansion), that involves duplication of 16 of the bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The Initial Permutation table/matrix is of size
((OPTION_A)) THIS IS MANDATORY OPTION	16×8
((OPTION_B)) THIS IS ALSO MANDATORY	12×8

OPTION	
((OPTION_C)) This is optional	8×8
((OPTION_D)) This is optional	4×8
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	There are 64 bits to permute and this requires a 8×8 matrix.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The number of unique substitution boxes in DES after the 48 bit XOR operation are
((OPTION_A)) THIS IS MANDATORY OPTION	8
((OPTION_B)) THIS IS ALSO MANDATORY	4

OPTION	
((OPTION_C)) This is optional	6
((OPTION_D)) This is optional	12
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The substitution consists of a set of 8 S-boxes, each of which accepts 6 bits as input and produces 4 bits as output.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	During decryption, we use the Inverse Initial Permutation (IP-1) before the IP.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY	false

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	IP-1 is the first step and the last step is IP during decryption.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A preferable cryptographic algorithm should have a good avalanche effect.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY	false

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Thus statement is true as a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as the avalanche effect.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the size(in bits) of the key in the SDES algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	24
((OPTION_B)) THIS IS ALSO MANDATORY	16

OPTION	
((OPTION_C)) This is optional	20
((OPTION_D)) This is optional	10
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	The size of the key in the SDES algorithm is 10 bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	GCD(a,b) is the same as GCD(|a|,|b|).
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY	FALSE

OPTION	
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	This is true. gcd(60,24) = gcd(60,-24) = 12.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 1160718174 and 316258250 using Euclidean algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	882
((OPTION_B)) THIS IS ALSO MANDATORY	770

OPTION	
((OPTION_C)) This is optional	1078
((OPTION_D)) This is optional	1225
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	GCD(1160718174, 316258250) = 1078

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 102947526 and 239821932 using Euclidean algorithm
((OPTION_A)) THIS IS MANDATORY OPTION	11
((OPTION_B)) THIS IS ALSO MANDATORY	12

OPTION	
((OPTION_C)) This is optional	8
((OPTION_D)) This is optional	6
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	GCD(102947526, 239821932) = 6.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Calculate the GCD of 8376238 and 1921023 using Euclidean algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	13
((OPTION_B)) THIS IS ALSO MANDATORY	12

OPTION	
((OPTION_C)) This is optional	17
((OPTION_D)) This is optional	7
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	GCD(8376238, 1921023) = 13.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The multiplicative Inverse of 1234 mod 4321 is
((OPTION_A)) THIS IS MANDATORY OPTION	3239
((OPTION_B)) THIS IS ALSO MANDATORY	3213

OPTION	
((OPTION_C)) This is optional	3242
((OPTION_D)) This is optional	Does not exist
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The multiplicative Inverse of 1234 mod 4321 is 3239.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The multiplicative Inverse of 550 mod 1769 is
((OPTION_A)) THIS IS MANDATORY OPTION	434
((OPTION_B)) THIS IS ALSO MANDATORY	224

OPTION	
((OPTION_C)) This is optional	550
((OPTION_D)) This is optional	Does not exist
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The multiplicative Inverse of 550 mod 1769 is 550.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2

((QUESTION))
ENTER CONTENT. QTN CAN HAVE IMAGES ALSO
	You are supposed to use hill cipher for encryption technique. You are provided with the following matrix,
	`A = [ 4 2`
	`2 1 ]`
	Is the given matrix 'A', a valid key to be used for encryption?

((OPTION_A)) THIS IS MANDATORY OPTION	Yes
((OPTION_B))	No

THIS IS ALSO MANDATORY OPTION	
((OPTION_C)) This is optional	Can't be determined
((OPTION_D)) This is optional	Data insufficient
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	For choosing any square matrix as a key, it should be taken care that the matrix is invertible, i.e. its inverse must exist. Here, in this case, $\lvert A \rvert = 0$ Therefore, it means that 'A' is not an invertible matrix. Hence matrix 'A' cannot be chosen as a key matrix for encryption in the Hill cipher.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	The DES (Data Encryption Standard) cipher follows the fiestal structure. Which of the following properties are not shown by the fiestal structure?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	The input text is divided into two parts: one being left half and another one being right half.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Swapping of the left and right halves are performed after each round.
((OPTION_C)) This is optional	The plain text is converted into a matrix form first
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The fiestal structure does not require the conversion of the plain text into matrix form at any of its steps.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	Among the following given options, chose the strongest encryption technique

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	DES (Data Encryption Standard))
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Double DES
((OPTION_C)) This is optional	Triple DES
((OPTION_D)) This is optional	AES (Advance Encryption Standard
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	It has been proved that the AES performs much better than the all the other DES, whether it be single DES or series of DES.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	**Consider the following steps,** i. Substitution bytes ii. Shift Rows

IMAGES ALSO	iii. Mix columns iv. Add round key **The above steps are performed in each round of which of the following ciphers?**
((OPTION_A)) THIS IS MANDATORY OPTION	Rail fence cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data Encryption Standard (DES)
((OPTION_C)) This is optional	Advance Encryption Standard (AES)
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_______ algorithm transforms ciphertext to plaintext.
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A _________ cipher replaces one character with another character.
((OPTION_A)) THIS IS MANDATORY OPTION	substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The ________ cipher reorders the plaintext characters to create a ciphertext.
((OPTION_A)) THIS IS MANDATORY OPTION	substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The _________ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.
((OPTION_A)) THIS IS MANDATORY OPTION	man-in-the-middle
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ciphertext attack
((OPTION_C)) This is optional	plaintext attack
((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an asymmetric-key cipher, the receiver uses the _______ key.
((OPTION_A)) THIS IS MANDATORY OPTION	private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	public
((OPTION_C)) This is optional	either a or b
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	DES is a(n) ________ method adopted by the U.S. government.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	either (a) or (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	ECB and CBC are _________ ciphers.
((OPTION_A)) THIS IS MANDATORY OPTION	block
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	stream
((OPTION_C)) This is optional	field
((OPTION_D)) This is optional	none of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In _________ cipher, the same key is used by both the sender and receiver.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	__________ ciphers can be categorized into two broad categories: monoalphabetic and polyalphabetic.
((OPTION_A)) THIS IS MANDATORY OPTION	Substitution
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an asymmetric-key cipher, the sender uses the__________ key.
((OPTION_A)) THIS IS MANDATORY OPTION	private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	public
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a(n) ________ cipher, a pair of keys is used.
((OPTION_A)) THIS IS MANDATORY OPTION	symmetric-key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	asymmetric-key
((OPTION_C)) This is optional	either (a) or (b)
((OPTION_D)) This is optional	neither (a) nor (b)
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	2

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	AES uses a _____________ bit block size and a key size of ___________ bits.
((OPTION_A)) THIS IS MANDATORY OPTION	128; 128 or 256
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	64; 128 or 192
((OPTION_C)) This is optional	256; 128, 192, or 256
((OPTION_D)) This is optional	128; 128, 192, or 256
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	It uses a 128-bit block size and a key size of 128, 192, or 256 bits.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2	1

OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Like DES, AES also uses Feistel Structure.
((OPTION_A)) THIS IS MANDATORY OPTION	True
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	False
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	AES does not use a Feistel structure. Instead, each full round consists of four separate functions: -byte substitution -Permutation -arithmetic operations over a finite field, and -XOR with a key.

((MARKS)) QUESTION IS OF	1

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The 4×4 byte matrices in the AES algorithm are called
((OPTION_A)) THIS IS MANDATORY OPTION	States
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Words
((OPTION_C)) This is optional	Transitions
((OPTION_D)) This is optional	Permutations
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF	1

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is a type of substitution cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	poly alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Transposition cipher
((OPTION_C)) This is optional	Columnar cipher
((OPTION_D)) This is optional	Rail fence cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In substitution cipher the plain text is replaced by cipher text according to a fixed rule. There are two types of substitution cipher- Mono alphabetic and Poly alphabetic cipher.

((MARKS)) QUESTION IS OF	1

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following correctly defines poly alphabetic cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	a substitution based cipher which uses multiple substitution at different positions
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a substitution based cipher which uses fixed substitution over entire message
((OPTION_C)) This is optional	a transposition based cipher which uses multiple substitution at different positions
((OPTION_D)) This is optional	A transposition based cipher which uses fixed substitution over entire message
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Poly alphabetic cipher is a type of substitution cipher. It uses multiple substitution at different positions in order to cipher the plain text.

((MARKS)) QUESTION IS OF	1

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following is not a type of poly alphabetic cipher?
((OPTION_A)) THIS IS MANDATORY OPTION	Rotor cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Hill cipher
((OPTION_C)) This is optional	One time pad cipher
((OPTION_D)) This is optional	Affine cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	In poly alphabetic cipher each symbol of plain text is replaced by a different cipher text regardless of its occurrence. Out of the given options, only affine cipher is not a poly alphabetic cipher.

((MARKS)) QUESTION IS OF	2

HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	We are provided the plain text “SUN”. You need to convert the given plain text into ciphertext under the Ceasar cipher encryption technique. Which of the following options is the correct ciphertext for the given text if the key is 2?
((OPTION_A)) THIS IS MANDATORY OPTION	UWP
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	NUS
((OPTION_C)) This is optional	WUP
((OPTION_D)) This is optional	QSL
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In the Caesar cipher technique, the encryption is performed as follows, E (P , K) = (P + K) mod 26 Therefore, E (S , 2) = (18 + 2) mod 26 = 20 = U E (U , 2) = (20 + 2) mod 26 = 22 = W E (N , 2) = (13 + 2) mod 26 = 15 = P Hence, the ciphertext is "UWP".

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following cipher techniques include the involvement of matrix operations in their algorithms of encryption and decryption?
((OPTION_A)) THIS IS MANDATORY OPTION	Hill Cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Playfair cipher
((OPTION_C)) This is optional	Both a and b
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also	The hill cipher includes a square matrix as the key, and in Playfair cipher, we create a 5X5 matrix using the given key string. Hence,

optional	both these ciphers include the use of matrices.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Playfair cipher is an example of __________
((OPTION_A)) THIS IS MANDATORY OPTION	mono-alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	poly-alphabetic cipher
((OPTION_C)) This is optional	transposition cipher
((OPTION_D)) This is optional	additive cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	Playfair cipher is a substitution cipher. It falls under the category of poly alphabetic cipher as it uses multiple substitution at different positions in order to cipher the plain text.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Encryption in Playfair cipher is done using _
((OPTION_A)) THIS IS MANDATORY OPTION	a 5×5 table
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a 13×2 table
((OPTION_C)) This is optional	vigenere table
((OPTION_D)) This is optional	a 6×6 table
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A

((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the plain text corresponding to cipher text “BPKYFS” if playfair cipher is used with keyword as “SECRET” (assuming j is combined with i)?
((OPTION_A)) THIS IS MANDATORY OPTION	INDIAN
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	WORLD
((OPTION_C)) This is optional	DOLLAR
((OPTION_D)) This is optional	HELLO
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C

((EXPLANATION)) This is also optional	To decrypt the message we follow the reverse procedure. The table is formed in the same manner. Applying this we get the plain text to be “DOLLAR”.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair are identical?
((OPTION_A)) THIS IS MANDATORY OPTION	then that pair is neglected
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	a null(or x) is added in between the letters
((OPTION_C)) This is optional	one of the identical letter is replaced by some other letter
((OPTION_D)) This is optional	then both of the letters are replaced by the letter appearing just next in the row
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	In playfair cipher if the letters in a pair are identical then a null is added in between the letters. Any letter can be used as a null as long as that letter is not the one being repeated.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair appear in same row?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letter at the corner of the row
((OPTION_D)) This is optional	that pair is neglected
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B

((EXPLANATION)) This is also optional	If the letters in a pair appear in same row then they are replaced by the letters appearing immediately right to them respectively. If the element to be replaced appears at the corner of the row then we wrap around to the left side of that row.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the ciphered text if the string “SANFOUNDRY” is given as input to the code of playfair cipher with keyword as “SECRET” (assuming j is combined with i)?
((OPTION_A)) THIS IS MANDATORY OPTION	ZHQAPNPAFR
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	AHQAPNPAFR
((OPTION_C)) This is optional	HAQAPNPAFR
((OPTION_D)) This is optional	QHAAPNPAFR
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CH OICE)) Either A or B or C or D or	B

E	
((EXPLANATION)) This is also optional	For encrypting the plain text using playfair cipher we use a 5×5 table that is constructed by using keyword. Then we apply rules for encryption in order to get the ciphered text. Table is given as under- S E C R T A B D F G H I K L M N O P Q U V W X Y Z

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair appear in same column?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letters at the corner of the row
((OPTION_D))	that pair is neglected

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	If the letters in a pair appear in the same column then they are replaced by the letters appearing immediately below them respectively. If the element to be replaced appears at the corner of the column then we wrap around to the top side of that column.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the rule for encryption in playfair cipher if the letters in a pair does not appear in same row or column?
((OPTION_A)) THIS IS MANDATORY OPTION	they are replaced by the letter appearing immediately below them respectively
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	they are replaced by the letter appearing immediately right to them respectively
((OPTION_C)) This is optional	they are replaced by the letter of the same row at the corner of the rectangle defined by the original pair respectively

((OPTION_D)) This is optional	that pair is neglected
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	If the letters in a pair does not appear in same row or column then they are replaced by the letters of the same row at the corner of the rectangle defined by the original pair respectively. The order of letters should be maintained.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Columnar cipher falls under the category of?
((OPTION_A)) THIS IS MANDATORY OPTION	mono-alphabetic cipher
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	poly-alphabetic cipher
((OPTION_C))	additive cipher

This is optional	
((OPTION_D)) This is optional	Transposition cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Columnar cipher is a transposition cipher. It falls under the category of transposition cipher as it encrypts the plain text by rearranging its letters.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following ciphered text would have NOT used transposition cipher for encryption of the plain text “CIPHER”?
((OPTION_A)) THIS IS MANDATORY OPTION	EPIHRC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	EHIPCR
((OPTION_C))	DTIPRC

This is optional	
((OPTION_D)) This is optional	HRIPEC
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	We know that transposition cipher encrypts the plain text by shuffling the letters of the plain text. So out of the given options, only “DTIPRC” does not have the same set of letters as “CIPHER”.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	How many columns do we need to have in the table, that is used for encryption in columnar transposition cipher when a given keyword is “SECRET” and plain text is “SANFOUNDRY”?
((OPTION_A)) THIS IS MANDATORY OPTION	4
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	5
((OPTION_C))	6

This is optional	
((OPTION_D)) This is optional	7
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The number of columns in the table used for the purpose encryption in columnar transposition cipher will always be equal to the number of letters in the keyword. So in this case it will be equal to 6.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What will be the encrypted text corresponding to plain text “CLASSIFIED” using columnar transposition cipher with a keyword as “GAMES”?
((OPTION_A)) THIS IS MANDATORY OPTION	LFDSIASECI
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SECIAISDFL
((OPTION_C))	CILFAISESD

This is optional	
((OPTION_D)) This is optional	IFSECIAISD
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	For encrypting using columnar cipher we have to arrange the letters of the plain text in a table which has the same number of columns as the letters of the keyword. Then the letters of the keyword are arranged in alphabetical order and we read along each column. 3 1 4 2 5 G A M E S C L A S S I F I E D So the ciphered text will be "IFSECIAISD".

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	How many rows will the letters of the plain text occupy in the table, that is used for encryption in columnar transposition cipher when a given keyword is "SECRET" and plain text is "SANFOUNDRY"?
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B))	2

THIS IS ALSO MANDATORY OPTION	
((OPTION_C)) This is optional	3
((OPTION_D)) This is optional	4
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Explanation: The number of columns in the table used for the purpose encryption in columnar transposition cipher will always be equal to the number of letters in the keyword.So when we will write the letters of the plain text row wise then there will be 2 rows of plain text in this case. The table is shown below :- S E C R E T 1 S A N F O U 2 N D R Y

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following statement is not true regarding columnar transposition cipher?
((OPTION_A)) THIS IS	probability of error is high while deciphering

MANDATORY OPTION	
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	it cannot be combined with other ciphers
((OPTION_C)) This is optional	it is a traditional symmetric cipher
((OPTION_D)) This is optional	it is a weak cipher
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Although columnar transposition cipher is a weak cipher in itself. But it can be combined with other substitution ciphers so as to improve its security. The probability of error remains high while decoding columnar cipher as it is a lengthy process

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is another data hiding technique which can be used in conjunction with cryptography for the extra-secure method of protecting data.
((OPTION_A))	Cryptography

THIS IS MANDATORY OPTION	
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Steganography
((OPTION_C)) This is optional	Tomography
((OPTION_D)) This is optional	Chorography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	Steganography is the technique of hiding data in another raw data. Steganography is another data hiding technique which can be used in conjunction with cryptography for an extra-secure method of protecting data.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	is hiding of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

((OPTION_A)) THIS IS MANDATORY OPTION	Cryptography
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C)) This is optional	Steganography
((OPTION_D)) This is optional	Chorography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	Steganography helps in hiding any form of data within data, where we can hide images, text, and other messages within images, videos, music or recording files.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A ________________ tool permits security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.

((OPTION_A)) THIS IS MANDATORY OPTION	Cryptography
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C)) This is optional	Chorography
((OPTION_D)) This is optional	Steganography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	A steganography tool is a software tool that permits a security professional or a hacker to embed hidden data within a carrier file like an image or video which can later be extracted from them.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The main motive for using steganography is that hackers or other users can hide a secret message behind a _______________

((OPTION_A)) THIS IS MANDATORY OPTION	special file
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ordinary file
((OPTION_C)) This is optional	program file
((OPTION_D)) This is optional	encrypted file
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	The main motive for using steganography is that hackers or other users can hide a secret message behind ordinary files. Some steganography tools are SSuite Picsel, rSteg etc.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	People will normally think it as a normal/regular file and your secret message will pass on without any _______________

((OPTION_A)) THIS IS MANDATORY OPTION	Suspicion
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	decryption
((OPTION_C)) This is optional	encryption
((OPTION_D)) This is optional	cracking
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	Steganography techniques help hackers or other users to conceal covert message behind regular files. People will normally think it as a normal/regular file and your secret message will pass on without any suspicion.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	By using _______________ you can diminish the chance of data leakage

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	Cryptography
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tomography
((OPTION_C)) This is optional	Chorography
((OPTION_D)) This is optional	Steganography
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	Hackers or other cyber criminals target ordinary files to hide different data or information within another data file. By using steganography, you can diminish the chance of data leakage.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	Which of the following is a mode of operation for the Block ciphers in cryptography?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	Electronic Code Book (ECB)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Cipher Block Chaining (CBC)
((OPTION_C)) This is optional	Counter (CTR) mode
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE	For which of the following should EBC (Electronic Code Book) process not be used for encryption?

IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	For large block sizes
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	For fixed block sizes
((OPTION_C)) This is optional	For small block sizes
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	It is preferred that the block size in the EBC technique must be greater than 64 bits. If not, the text is padded to make it of the required length. This is due to some particular words and phrases that may be reused again often so that the same repetitive part of ciphertext can emerge as mixed.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION))	Which of the following is the main disadvantage of the ECB (Electronic Code Book)?

ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	
((OPTION_A)) THIS IS MANDATORY OPTION	It requires large block size
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Padding is done to make the plain text divisible into blocks of fixed size
((OPTION_C)) This is optional	It is prone to cryptanalysis since there is a direct relationship between plain text and cipher text.
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	In ECB, there lies a direct relation between the plain text and the ciphertext. Therefore, it is easy for an outsider to break the encryption logic and steal the data.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following options is not correct according to the definition of the Cipher Block Chaining (CBC)?
((OPTION_A)) THIS IS MANDATORY OPTION	CBC is a mode of operation for stream ciphers.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Initialization vector (IV) is used in CBC in the initial phase.
((OPTION_C)) This is optional	It has better resistive nature towards cryptanalysis than ECB
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	CBC which stands for Cipher Block chaining is a mode of operation for block ciphers and not for stream ciphers.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following modes of operations can be followed for both stream ciphers as well as block ciphers?
((OPTION_A)) THIS IS MANDATORY OPTION	CBC (Cipher Block Chaining)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ECB (Electronic Code Book)
((OPTION_C)) This is optional	CFB (Cipher text Feed Back)
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	CFB is primarily a mode to derive some characteristics of a stream cipher from a block cipher on the cryptography in cryptoanalysis.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1

((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	All the below-stated processes are performed in the AES (Advanced Encryption Standard) Algorithm. Which of the following process(s) are not performed in the final round of the AES? i. Substitution bytes ii. Shift rows iii. Mix columns iv. Add round key
((OPTION_A)) THIS IS MANDATORY OPTION	i
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	iii
((OPTION_C)) This is optional	All of the mentioned
((OPTION_D)) This is optional	None of the mentioned
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	In the AES algorithm, the MIX COLUMN operation is performed in all the rounds except the final round of the algorithm.

((MARKS))	1

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	"The number of rounds in the AES algorithm depends upon the key size being used." Which among the following shows a correct relation between the size of the key used and the number of rounds performed in the AES algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	128 key size: 10 rounds
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	192 key size: 12 rounds
((OPTION_C)) This is optional	256 key size: 14 rounds
((OPTION_D)) This is optional	All of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS))	2

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following properties are the characteristic properties of a block cipher technique which differs from stream cipher**?**
((OPTION_A)) THIS IS MANDATORY OPTION	Avalanche effect
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Completeness
((OPTION_C)) This is optional	Both a. and b
((OPTION_D)) This is optional	None of the above
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS))	2

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For the AES-128 algorithm there are ___________ similar rounds and __________ round is different.
((OPTION_A)) THIS IS MANDATORY OPTION	2 pair of 5 similar rounds ; every alternate
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	9 ; the last
((OPTION_C)) This is optional	8 ; the first and last
((OPTION_D)) This is optional	10 ; no
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS))	1

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the 4 operations are false for each round in the AES algorithm? i) Substitute Bytes ii) Shift Columns iii) Mix Rows iv) XOR Key
((OPTION_A)) THIS IS MANDATORY OPTION	i) only
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	ii) iii) and iv)
((OPTION_C)) This is optional	ii) and iii)
((OPTION_D)) This is optional	only iv
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	AES rounds involve substitute bytes, shift rows, mix columns and addition of round key.

((MARKS))	1

QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	There is an addition of round key before the start of the AES round algorithms.
((OPTION_A)) THIS IS MANDATORY OPTION	TRUE
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	FALSE
((OPTION_C)) This is optional	
((OPTION_D)) This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	In AES the final round contains only three transformations, and there is an initial single transformation (Add Round Key) before the first round which can be considered Round 0. Each transformation takes 4×4 matrixes as input and produces a 4×4 matrix as output.

<table>
<tr><td>((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)</td><td>1</td></tr>
<tr><td>((QUESTION))
ENTER CONTENT. QTN CAN HAVE IMAGES ALSO</td><td>What is the Shifted Row transformation for the matrix bellow?<table>
<tr><td>FE</td><td>72</td><td>2B</td><td>D7</td></tr>
<tr><td>6B</td><td>77</td><td>A4</td><td>6B</td></tr>
<tr><td>AD</td><td>01</td><td>F0</td><td>63</td></tr>
<tr><td>30</td><td>D7</td><td>AF</td><td>FE</td></tr>
</table></td></tr>
<tr><td>((OPTION_A))
THIS IS MANDATORY OPTION</td><td><table>
<tr><td>FE</td><td>72</td><td>2B</td><td>D7</td></tr>
<tr><td>6B</td><td>77</td><td>A4</td><td>6B</td></tr>
<tr><td>AD</td><td>01</td><td>F0</td><td>63</td></tr>
<tr><td>30</td><td>D7</td><td>AF</td><td>FE</td></tr>
</table></td></tr>
<tr><td>((OPTION_B))
THIS IS ALSO MANDATORY OPTION</td><td><table>
<tr><td>72</td><td>2B</td><td>D7</td><td>FE</td></tr>
<tr><td>A4</td><td>6B</td><td>6B</td><td>77</td></tr>
<tr><td>63</td><td>AD</td><td>01</td><td>F0</td></tr>
<tr><td>30</td><td>D7</td><td>AF</td><td>FE</td></tr>
</table></td></tr>
<tr><td>((OPTION_C))
This is optional</td><td><table>
<tr><td>FE</td><td>72</td><td>2B</td><td>D7</td></tr>
<tr><td>77</td><td>A4</td><td>6B</td><td>6B</td></tr>
<tr><td>F0</td><td>63</td><td>AD</td><td>01</td></tr>
<tr><td>FE</td><td>30</td><td>D7</td><td>AF</td></tr>
</table></td></tr>
<tr><td>((OPTION_D))
This is optional</td><td><table>
<tr><td>D7</td><td>FE</td><td>72</td><td>2B</td></tr>
<tr><td>A4</td><td>6B</td><td>6B</td><td>77</td></tr>
<tr><td>01</td><td>AD</td><td>63</td><td>F0</td></tr>
<tr><td>30</td><td>D7</td><td>AF</td><td>FE</td></tr>
</table></td></tr>
</table>

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	The Shift Rows transformation consists of: -Not shifting the first row of the state array at all. -Circularly shifting the second row by one byte to the left. -Circularly shifting the third row by two bytes to the left, and -Circularly shifting the last row by three bytes to the left.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not weak key in DES
((OPTION_A)) THIS IS MANDATORY OPTION	0x0101010101010101
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	0xFEFABFEFEFEFEFEFE
((OPTION_C)) This is optional	0x1F1F1F1F0E0E0E0E
((OPTION_D))	0xFFFFFFFFFFFFFFFF

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Triple-DES has _______ keys.
((OPTION_A)) THIS IS MANDATORY OPTION	1
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	2
((OPTION_C)) This is optional	5
((OPTION_D))	4

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_______ is a encryption technique which uses two instance of DES on same plain text.
((OPTION_A)) THIS IS MANDATORY OPTION	Double DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Tripple DES
((OPTION_C)) This is optional	Both
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	__________ attack which can be used to break through double DES.
((OPTION_A)) THIS IS MANDATORY OPTION	Brute force
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	meet-in-the middle
((OPTION_C)) This is optional	Timing
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Triple DES involve __
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption, Decryption, Decryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption ,Encryption, Encryption
((OPTION_C)) This is optional	Decryption ,Encryption, Decryption
((OPTION_D))	Encryption, Decryption, Encryption

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	D
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_______ involves feeding the successive output blocks from the underlying block cipher back to it
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	OFB
((OPTION_D))	CFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ is counter-based version of CFB mode without the feedback
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	counter
((OPTION_D))	OFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below mode is independent of previous output
((OPTION_A)) THIS IS MANDATORY OPTION	ECB
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC
((OPTION_C)) This is optional	CFB
((OPTION_D))	OFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Errors get propagated in all modes except __and ____
((OPTION_A)) THIS IS MANDATORY OPTION	ECB,COUNTER
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CBC,COUNTER
((OPTION_C)) This is optional	CFB,COUNTER
((OPTION_D))	OFB,CFB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Patterns are not preserved in ___ mode
((OPTION_A)) THIS IS MANDATORY OPTION	CBC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	CFB
((OPTION_C)) This is optional	Both CBC and CFB
((OPTION_D))	ECB

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A small change in plaintext results in the very great change in the cipher text indicates which characteristic
((OPTION_A)) THIS IS MANDATORY OPTION	completeness
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Strong key
((OPTION_C)) This is optional	Avalanche effect
((OPTION_D))	All of the above

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	C
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In ______ ciphers, the plaintext is processed one bit at a time i.e. one bit of plaintext is taken, and a series of operations is performed on it to generate one bit of cipher text.
((OPTION_A)) THIS IS MANDATORY OPTION	Block
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Stream
((OPTION_C)) This is optional	Both
((OPTION_D))	None of these

This is optional	
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	More number of _____ provide more secure system in fiestel cipher.
((OPTION_A)) THIS IS MANDATORY OPTION	rounds
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	keys
((OPTION_C)) This is optional	encryption
((OPTION_D)) This is optional	Function
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	
((CORRECT_CHOICE)) Either A or B or C or D or E	A
((EXPLANATION)) This is also optional	The number of rounds used in a Feistel Cipher depends on desired security from the system. More number of rounds provide more secure system. But at the same time, more rounds mean the inefficient slow encryption and decryption processes..