

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In public key cryptosystem _____ keys are used for encryption and decryption.
((OPTION_A)) THIS IS MANDATORY OPTION	Same
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Different
((OPTION_C)) This is optional	Encryption Keys
((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_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION) This is also optional	In conventional cryptosystem, same keys are used for encryption and decryption where as in public key cryptosystem different keys are used.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In public key cryptosystem which is kept as public?
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption keys
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption keys
((OPTION_C)) This is optional	Encryption & Decryption keys
((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_CH OICE)) Either A or B or C or D or E	A
((EXPLANATION) This is also optional	In public key cryptosystem, the encryption keys are kept as public where as decryption keys are kept as secret.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Public key cryptosystem uses same key for both encryption and decryption.
((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_CH OICE)) 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	Which should be kept as a secret in public key cryptosystem?
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption key
((OPTION_C)) This is optional	Encryption & Decryption key
((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_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	In public key cryptosystem, Encryption is done using public key . decryption key needs to be kept as a secret.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Euler's totient function is determined by
((OPTION_A)) THIS IS MANDATORY OPTION	pq
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$(p-1)(q-1)$
((OPTION_C)) This is optional	$(p+1)(q+1)$
((OPTION_D)) This is optional	p/q
((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 Euler's totient function is determined by $(p-1)(q-1)$, where p and q are kept hidden.

((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 RSA algorithm, we select 2 random large values 'p' and 'q'. Which of the following is the property of 'p' and 'q'?
((OPTION_A)) THIS IS MANDATORY OPTION	p and q should be divisible by $\Phi(n)$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	p and q should be co-prime
((OPTION_C)) This is optional	p and q should be prime
((OPTION_D)) This is optional	p/q should give no remainder
((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 E	C
((EXPLANATION) This is also optional	'p' and 'q' should have large random values which are both prime numbers.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA, $\Phi(n)$ = _____ in terms of p and q.
((OPTION_A)) THIS IS MANDATORY OPTION	$(p)/(q)$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$(p)(q)$
((OPTION_C)) This is optional	$(p-1)(q-1)$
((OPTION_D)) This is optional	$(p+1)(q+1)$
((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 E	C
((EXPLANATION)) This is also optional	$\Phi(n) = (p-1)(q-1)$.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA, we select a value 'e' such that it lies between 0 and $\Phi(n)$ and it is relatively prime to $\Phi(n)$.
((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_CH OICE)) Either A or B or C or D or E	B
((EXPLANATION)) This is also optional	$\gcd(e, \Phi(n))=1$; and $1 < e < \Phi(n)$.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 19$ and choose $e=17$. Apply RSA algorithm where message=5 and find the cipher text
((OPTION_A)) THIS IS MANDATORY OPTION	$C=80$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$C=92$
((OPTION_C)) This is optional	$C=56$
((OPTION_D)) This is optional	$C=23$
((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 E	A
((EXPLANATION) This is also optional	$n = pq = 11 \times 19 = 209$.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For p = 11 and q = 19 and choose d=17. Apply RSA algorithm where Cipher message=80 and thus find the plain text.
((OPTION_A)) THIS IS MANDATORY OPTION	54
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	43
((OPTION_C)) This is optional	5
((OPTION_D)) This is optional	24
((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 E	C
((EXPLANATION) This is also optional	$n = pq = 11 \times 19 = 209$. $C = M^e \bmod n$; $C = 5^{17} \bmod 209$; $C = 80 \bmod 209$.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	$n = 35$; $e = 5$; $C = 10$. What is the plaintext (use RSA) ?
((OPTION_A)) THIS IS MANDATORY OPTION	3
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	7
((OPTION_C)) This is optional	8
((OPTION_D)) This is optional	5
((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 E	D
((EXPLANATION)) This is also optional	Use RSA system to decrypt and get $PT = 5$.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For $p = 11$ and $q = 17$ and choose $e=7$. Apply RSA algorithm where PT message=88 and thus find the CT.
((OPTION_A)) THIS IS MANDATORY OPTION	23
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	64
((OPTION_C)) This is optional	11
((OPTION_D)) This is optional	54
((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 E	C
((EXPLANATION) This is also optional	$n = pq = 11 \times 19 = 187$. $C = M^e \text{ mod } n$; $C = 88^7 \text{ mod } 187$; $C = 11 \text{ mod } 187$.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	For p = 11 and q = 17 and choose e=7. Apply RSA algorithm where Cipher message=11 and thus find the plain text.
((OPTION_A)) THIS IS MANDATORY OPTION	88
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	122
((OPTION_C)) This is optional	143
((OPTION_D)) This is optional	111
((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 E	A
((EXPLANATION) This is also optional	$n = pq = 11 \times 19 = 187$. $C = M^e \bmod n$; $C = 11^{23} \bmod 187$; $C = 88 \bmod 187$.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In an RSA system the public key of a given user is $e = 31$, $n = 3599$. What is the private key of this user?
((OPTION_A)) THIS IS MANDATORY OPTION	3031
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	2412
((OPTION_C)) This is optional	2432
((OPTION_D)) This is optional	1023
((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 E	A
((EXPLANATION) This is also optional	By trail and error, we determine that $p = 59$ and $q = 61$. Hence $f(n) = 58 \times 60 = 3480$. Then, using the extended Euclidean algorithm, we find that the multiplicative inverse of 31 modulo $f(n)$ is 3031

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Compute private key (d, p, q) given public key (e=23, n=233 ´ 241=56,153).
((OPTION_A)) THIS IS MANDATORY OPTION	35212
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	12543
((OPTION_C)) This is optional	19367
((OPTION_D)) This is optional	32432
((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	Since n=233 ´ 241=56,153, p=233 and q=241 f(n) = (p – 1)(q – 1) = 55,680 Using Extended Euclidean algorithm, we obtain d = 23–1 mod 55680 = 19,367.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In a RSA cryptosystem a particular A uses two prime numbers $p = 13$ and $q = 17$ to generate her public and private keys. If the public key of A is 35. Then the private key of A is _____.
((OPTION_A)) THIS IS MANDATORY OPTION	11
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	13
((OPTION_C)) This is optional	16
((OPTION_D)) This is optional	17
((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 an RSA cryptosystem, for public key: $\text{GCD}(\phi(n), e) = 1$ And, for private key:

	$(e * d) \bmod \phi(n) = 1$ Where, $\phi(n) = (p - 1) * (q - 1) = (13 - 1)(17 - 1) = 12 * 16 = 192$ Such that $1 < e, d < \phi(n)$ Therefore, the private key is: $(35 * d) \bmod \phi(n) = 1$ $d = 11$
--	---

((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 RSA public key cryptosystem, which one of the following numbers will always be largest?
((OPTION_A)) THIS IS MANDATORY OPTION	E
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	N
((OPTION_C)) This is optional	P
((OPTION_D)) This is optional	Q
((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 number n is generated as the product of the two large prime numbers p and q . Therefore, n must always be greater than both p and q . Furthermore, it is an algorithm constraint that e must be chosen such that e is smaller than n . Therefore, in RSA cryptography n is always the largest of the four variables shown in the options to this question.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	If Richard wants to send an encrypted message to Sue using a public key cryptosystem, which key does he use to encrypt the message?
((OPTION_A)) THIS IS MANDATORY OPTION	Richard's public key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Richard's private key
((OPTION_C)) This is optional	Sue's public key
((OPTION_D)) This is optional	Sue's 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	C
((EXPLANATION)) This is also optional	Richard must encrypt the message using Sue's public key so that Sue can decrypt it using her private key. If he encrypted the message with his own public key, the recipient would need to know Richard's private key to decrypt the message. If he encrypted it with his own private key, any user could decrypt the message using Richard's freely available public key. Richard could not encrypt the message using Sue's private key because he does not have access to it. If he did, any user could decrypt it using Sue's freely available public key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Acme Widgets currently uses a 1,024-bit RSA encryption standard companywide. The company plans to convert from RSA to an elliptic curve cryptosystem. If it wishes to maintain the same cryptographic strength, what ECC key length should it use?
((OPTION_A)) THIS IS MANDATORY OPTION	160 bits
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	512 bits
((OPTION_C)) This is optional	1,024 bits
((OPTION_D)) This is optional	2,048 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	A
((EXPLANATION)) This is also optional	The elliptic curve cryptosystem requires significantly shorter keys to achieve encryption that would be the same strength as encryption achieved with the RSA encryption algorithm. A 1,024-bit RSA key is cryptographically equivalent to a 160-bit elliptic curve cryptosystem key.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Richard received an encrypted message sent to him from Sue. Which key should he use to decrypt the message?
((OPTION_A)) THIS IS MANDATORY OPTION	Richard's public key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Richard's private key
((OPTION_C)) This is optional	Sue's public key
((OPTION_D)) This is optional	Sue's 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	Sue would have encrypted the message using Richard's public key. Therefore, Richard needs to use the complementary key in the key pair, his private key, to decrypt the message.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	One commonly used public-key cryptography method is the _____ algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	RSS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RAS
((OPTION_C)) This is optional	RSA
((OPTION_D)) This is optional	RAA

((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 _____ 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 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	What is the objective of Diffie-Hellman key exchange?
((OPTION_A)) THIS IS MANDATORY OPTION	To protect encrypted data from man-in-the-middle attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	To perform mutual authentication on both sides
((OPTION_C)) This is optional	To prove to another party that one holds a secret key without revealing it
((OPTION_D)) This is optional	To establish a shared secret key on both sides

((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	The security of RSA encryption relies on which assumption?
((OPTION_A)) THIS IS MANDATORY OPTION	It is computationally infeasible to compute a GCD of two large numbers.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	It is computationally infeasible to factor a large number.
((OPTION_C)) This is optional	It is computationally infeasible to test whether a large number is prime.
((OPTION_D)) This is optional	It is computationally infeasible to compute a square modulo n.

((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	All of the above
((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	Which of the below is asymmetric cryptography?
((OPTION_A)) THIS IS MANDATORY OPTION	ECC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	Both ECC and RSA
((OPTION_D)) This is optional	None of these

((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 requires less hardware capacity because of less key size
((OPTION_A)) THIS IS MANDATORY OPTION	ECC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSA
((OPTION_C)) This is optional	DES
((OPTION_D)) This is optional	AES

((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	Diffie Hellman is ____
((OPTION_A)) THIS IS MANDATORY OPTION	Encryption algorithm
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Decryption algorithm
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these

((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	D-H is key exchange algorithm

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Timing attack on RSA can be avoided by __
((OPTION_A)) THIS IS MANDATORY OPTION	Padding extra bits in message
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Adding delays
((OPTION_C)) This is optional	Both
((OPTION_D)) This is optional	None of these

((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 algorithm is used in cryptocurrency?
((OPTION_A)) THIS IS MANDATORY OPTION	RSA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	AES
((OPTION_C)) This is optional	ECC
((OPTION_D)) This is optional	None of these

((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	When a hash function is used to provide message authentication, the hash function value is called to as:
((OPTION_A)) THIS IS MANDATORY OPTION	Message Field
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Message Digest
((OPTION_C)) This is optional	Message Score
((OPTION_D)) This is optional	Message Leap

((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	We know that the hash function providing message authentication is referred to as message digest in cryptography.

((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 are used to create a message digest a. RSA b. SHA-1 c. DES d. MD5
((OPTION_A)) THIS IS MANDATORY OPTION	A&B
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	B&C
((OPTION_C)) This is optional	A&C

((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	B
((EXPLANATION)) This is also optional	They are Message digest algorithm

((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 output of a cryptographic hash function?
((OPTION_A)) THIS IS MANDATORY OPTION	A variable set of bits
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	A fixed set of bits, derived from one-way mathematical operations
((OPTION_C)) This is optional	An output which may be easily discovered by an adversary

((OPTION_D)) This is optional	Outputs of such functions are of no importance
((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	Message digest algorithms are primarily used to provide _____
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Authentication
((OPTION_C)) This is optional	Integrity

((OPTION_D)) This is optional	authorization
((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 a message digest algorithm.
((OPTION_A)) THIS IS MANDATORY OPTION	DES
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	IDEA
((OPTION_C)) This is optional	MD5

((OPTION_D)) This is optional	RSA
((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	Message_____ means that the data must arrive at the receiver exactly as sent.
((OPTION_A)) THIS IS MANDATORY OPTION	confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	integrity
((OPTION_C)) This is optional	authentication

((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	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	Message _____ means that the receiver is ensured that the message is coming from the intended sender, not an imposter.
((OPTION_A)) THIS IS MANDATORY OPTION	confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	integrity
((OPTION_C)) This is optional	authentication

((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 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A(n) _____function creates a message digest out of a message
((OPTION_A)) THIS IS MANDATORY OPTION	encryption
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	decryption
((OPTION_C)) This is optional	hash

((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 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A(n) _____ is a trusted third party that assigns a symmetric key to two parties.
((OPTION_A)) THIS IS MANDATORY OPTION	Public directory
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Certificate authority
((OPTION_C)) This is optional	Both

((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 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature provides _____.
((OPTION_A)) THIS IS MANDATORY OPTION	authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	nonrepudiation
((OPTION_C)) This is optional	both (a) and (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	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 digital signature needs a(n)_____ system
((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 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	A(n) _____ is a federal or state organization that binds a public key to an entity and issues a certificate.
((OPTION_A)) THIS IS MANDATORY OPTION	KDC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Kerberos
((OPTION_C)) This is optional	CA

((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 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ means that a sender must not be able to deny sending a message that he sent.
((OPTION_A)) THIS IS MANDATORY OPTION	Confidentiality
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C)) This is optional	Authentication

((OPTION_D)) This is optional	Nonrepudiation
((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	_____ is a popular session key creator protocol that requires an authentication server and a ticket-granting server.
((OPTION_A)) THIS IS MANDATORY OPTION	KDC
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Kerberos
((OPTION_C)) This is optional	CA

((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	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	The MD5 is a message digest algorithm developed by
((OPTION_A)) THIS IS MANDATORY OPTION	Ron Rivest.
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	WhiteField Diffie.
((OPTION_C)) This is optional	Martin Hellman.

((OPTION_D)) This is optional	Diffie-Hellman.
((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	MD5 is quite fast and produces _____ message digests
((OPTION_A)) THIS IS MANDATORY OPTION	512 bits
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	1024 bits
((OPTION_C)) This is optional	128 bits

((OPTION_D)) This is optional	64 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)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The first step of MD5 is
((OPTION_A)) THIS IS MANDATORY OPTION	add padding bits to original message
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	adding append length bits
((OPTION_C)) This is optional	divide the input into 512 bit blocks

((OPTION_D)) This is optional	compression
((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	In MD5, the process block divides the 512 bits into _____ sub blocks.
((OPTION_A)) THIS IS MANDATORY OPTION	16
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	24
((OPTION_C)) This is optional	32

((OPTION_D)) This is optional	84
((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	Which financial institutions have a relationship with merchants for processing payment card authorizations and payments?
((OPTION_A)) THIS IS MANDATORY OPTION	Issuer
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Acquirer
((OPTION_C)) This is optional	Merchant

((OPTION_D)) This is optional	Dealer
((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	Which of the following contains the order information such as which items are being purchased?
((OPTION_A)) THIS IS MANDATORY OPTION	PI
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	OI
((OPTION_C)) This is optional	MD

((OPTION_D)) This is optional	DS
((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	Payment information can be encrypted by using _____.
((OPTION_A)) THIS IS MANDATORY OPTION	customer's private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	merchant public key
((OPTION_C)) This is optional	one-time session key.

((OPTION_D)) This is optional	customer's public 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	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	Digital signature envelope is decrypted by using _____.
((OPTION_A)) THIS IS MANDATORY OPTION	merchant private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	payment's private key
((OPTION_C)) This is optional	payment public key

((OPTION_D)) This is optional	merchant's public 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	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ will ensure the merchant and their payment information
((OPTION_A)) THIS IS MANDATORY OPTION	Digital certificate
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Merchant
((OPTION_C)) This is optional	Dual signature

((OPTION_D)) This is optional	Certificate authority
((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	SET provides an authentication with the help of _____
((OPTION_A)) THIS IS MANDATORY OPTION	dual signature
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	digital certificate
((OPTION_C)) This is optional	payment's public key

((OPTION_D)) This is optional	payment's 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	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____are very crucial for success of RSA algorithm
((OPTION_A)) THIS IS MANDATORY OPTION	Integers
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Prime numbers
((OPTION_C)) This is optional	Negative number

((OPTION_D)) This is optional	Fraction
((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	The _____ acts as financial institutions who provides a payment card to a card holder
((OPTION_A)) THIS IS MANDATORY OPTION	payment gateway
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	card holder
((OPTION_C)) This is optional	acquirer

((OPTION_D)) This is optional	issuer
((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	ISSUER means Bank

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Who will be responsible for processing the payment from the customer's account to the merchant account?
((OPTION_A)) THIS IS MANDATORY OPTION	Acquirer
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Merchant
((OPTION_C)) This is optional	Issuer

((OPTION_D)) This is optional	Payment gateway
((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	The cardholder combines the PIMD and OIMD and hashes them together to form
((OPTION_A)) THIS IS MANDATORY OPTION	OPMD
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	POMD
((OPTION_C)) This is optional	MD

((OPTION_D)) This is optional	DS
((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	Which process will ensure that the issues of the credit card is an approved transactions?
((OPTION_A)) THIS IS MANDATORY OPTION	Payment capture
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Payment authorization
((OPTION_C)) This is optional	Purchase request

((OPTION_D)) This is optional	Purchase reply
((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 used for hiding the payment information from the merchant.
((OPTION_A)) THIS IS MANDATORY OPTION	SET
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	SSL
((OPTION_C)) This is optional	SHTTP

((OPTION_D)) This is optional	TSP
((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	A __word buffer is used to compute the message digest in MD5
((OPTION_A)) THIS IS MANDATORY OPTION	3
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	4
((OPTION_C)) This is optional	5

((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	B
((EXPLANATION)) This is also optional	4 WORD A,B,C,D

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In MD5, the message is padding so that its length is divisible by ____
((OPTION_A)) THIS IS MANDATORY OPTION	32
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	128
((OPTION_C)) This is optional	512

((OPTION_D)) This is optional	1024
((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	MD5 should meet requirements:
((OPTION_A)) THIS IS MANDATORY OPTION	It is impossible to generate two inputs that cannot produce the same hash function
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	It is impossible to generate a message having the same hash value
((OPTION_C)) This is optional	Both of the above

((OPTION_D)) This is optional	None of these
((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	MD5 takes an input of ____ size and produces an output if a 128-bit hash value
((OPTION_A)) THIS IS MANDATORY OPTION	Any
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Multiple of 512
((OPTION_C)) This is optional	Multiple of 128

((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 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the following best describes sniffing?
((OPTION_A)) THIS IS MANDATORY OPTION	Gathering packets to locate IP addresses, in order to initiate a session hijacking attack
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Analyzing packets in order to locate the sequence number to start a session hijack
((OPTION_C)) This is optional	Monitoring TCP sessions in order to initiate a session-hijacking attack

((OPTION_D)) This is optional	Locating a host susceptible to a session-hijack attack
((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	Sniffing is usually used to locate the sequence number, which is necessary for a session hijack.

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The secret key between members needs to be created as a _____ key when two members contact Kerberos system
((OPTION_A)) THIS IS MANDATORY OPTION	Public
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Session
((OPTION_C))	complimentary

This is optional	
((OPTION_D)) This is optional	None of these
((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	The main components of Kerberos are:
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication server
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Ticket granting server
((OPTION_C))	database

This is optional	
((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)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The_____ performs the initial authentication and ticket for Ticket Granting Service
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication server
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Ticket granting server
((OPTION_C))	Database

This is optional	
((OPTION_D)) This is optional	Kerberos
((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	The Authentication Server verifies access right of users in ____
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication server
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TG server
((OPTION_C))	Database

This is optional	
((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 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	_____ issues the ticket for the Server
((OPTION_A)) THIS IS MANDATORY OPTION	AS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TGS
((OPTION_C))	DB

This is optional	
((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	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	Kerberos is primarily used for _____
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity
((OPTION_C))	confidentiality

This is optional	
((OPTION_D)) This is optional	authorization
((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	The KDC encrypts the TGT with a password that only the _____ knows.
((OPTION_A)) THIS IS MANDATORY OPTION	AS
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	TGS
((OPTION_C))	Server

This is optional	
((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	Because no one else needs to be able to see the contents. It's for the server to keep track of the client

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	The essence of Kerberos' system is _____.
((OPTION_A)) THIS IS MANDATORY OPTION	One way authentication
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity

((OPTION_C)) This is optional	Mutual authentication
((OPTION_D)) This is optional	Public authentication
((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 following is not an element/field of the X.509 certificates?
((OPTION_A)) THIS IS MANDATORY OPTION	Issuer Name
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Serial Modifier

((OPTION_C)) This is optional	Issuer unique Identifier
((OPTION_D)) This is optional	Signature
((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	X.509 certificate recommends which cryptographic algorithm?
((OPTION_A)) THIS IS MANDATORY OPTION	RSA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	DES

((OPTION_C)) This is optional	AES
((OPTION_D)) This is optional	Rabin
((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	The standard used in digital certificates that defines its structure, fields, and Values is
((OPTION_A)) THIS IS MANDATORY OPTION	Kerberos
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	End to end encryption

((OPTION_C)) This is optional	X.509
((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 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	X.509 Certificates includes
((OPTION_A)) THIS IS MANDATORY OPTION	Version
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	signature algorithm identifier

((OPTION_C)) This is optional	period of validity
((OPTION_D)) This is optional	extension fields
((OPTION_E)) This is optional. If optional keep empty so that system will skip this option	All of the above
((CORRECT_CHOICE)) Either A or B or C or D or E	E
((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	___ defines a framework for the provision of authentication services by the X.500 directory
((OPTION_A)) THIS IS MANDATORY OPTION	X.509
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	X.508

((OPTION_C)) This is optional	X.505
((OPTION_D)) This is optional	X.609
((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	A digital signature is a mathematical technique used to validate the _____and _____of a message, software or digital document
((OPTION_A)) THIS IS MANDATORY OPTION	Authenticity, integrity
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Integrity, confidentiality

((OPTION_C)) This is optional	Integrity,non-repudiation
((OPTION_D)) This is optional	Authenticity,confidentiality
((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)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Digital signature involves ____ and ____
((OPTION_A)) THIS IS MANDATORY OPTION	Signature verification ,validation
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Signature creation,verification

((OPTION_C)) This is optional	Signature creation,deletion
((OPTION_D)) This is optional	Signature validation,modification
((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	Message digest is computed by applying hash function on the message and then message digest is encrypted using _____key of sender to form the digital signature.
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public

((OPTION_C)) This is optional	Session
((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	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	In digital signature , Receiver decrypts the digital signature using the _____ key of sender
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public

((OPTION_C)) This is optional	Secret
((OPTION_D)) This is optional	Session
((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	In digital signature, The message digest computed by ____ and the message digest (got by decryption on digital signature) need to be ____ for ensuring integrity
((OPTION_A)) THIS IS MANDATORY OPTION	Receiver,same
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Receiver,different

((OPTION_C)) This is optional	Sender,same
((OPTION_D)) This is optional	Sender,different
((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)	2
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	____is like a fingerprint or an attachment to a digital document that ensures its authenticity and integrity.
((OPTION_A)) THIS IS MANDATORY OPTION	Digital certificate
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Digital signature

((OPTION_C)) This is optional	Both
((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	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	Digital signature follows ____
((OPTION_A)) THIS IS MANDATORY OPTION	Digital Signature Standard (DSS)
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	X.509 standard format

((OPTION_C)) This is optional	Both of the above
((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 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In diffie-hellman algorithm, if Alice and Bob wish to communicate with each other, they first agree between them a large prime number n , and _____ g
((OPTION_A)) THIS IS MANDATORY OPTION	Generator
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Small prime number

((OPTION_C)) This is optional	Natural number
((OPTION_D)) This is optional	Factorial
((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	In D-H algorithm if X_a is private key of user then public key is calculated by ____
((OPTION_A)) THIS IS MANDATORY OPTION	$g^{X_a} \bmod n$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$n^{X_a} \bmod n$

((OPTION_C)) This is optional	$g^n \bmod p$
((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 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm, ____ keys of each other should be known
((OPTION_A)) THIS IS MANDATORY OPTION	Private
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Session

((OPTION_C)) This is optional	Public
((OPTION_D)) This is optional	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	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 D-H algorithm, shared secret key is calculated by ____
((OPTION_A)) THIS IS MANDATORY OPTION	$(g^a \bmod n)^b \bmod n$
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	$(g^b \bmod n)^a \bmod n$

((OPTION_C)) This is optional	Both of the above
((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 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In D-H algorithm, the resulting shared secret will be the ____ every time
((OPTION_A)) THIS IS MANDATORY OPTION	Same
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Different

((OPTION_C)) This is optional	Maybe same
((OPTION_D)) This is optional	Can't say
((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	_____ the first widely used method of safely developing and exchanging keys over an insecure channel
((OPTION_A)) THIS IS MANDATORY OPTION	RSA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	RSS

((OPTION_C)) This is optional	Diffie Hellman
((OPTION_D)) This is optional	AES
((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	Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Their D-H key is
((OPTION_A)) THIS IS MANDATORY OPTION	3
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	4

((OPTION_C)) This is optional	5
((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	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	In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value $q = 17$ and primitive root $= 5$. If Alice's secret key is 4 and Bob's secret key is 6, what is the shared secret key they exchanged?
((OPTION_A)) THIS IS MANDATORY OPTION	16
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	17

((OPTION_C)) This is optional	18
((OPTION_D)) This is optional	19
((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	Each round of MD5 consist of ____ operations
((OPTION_A)) THIS IS MANDATORY OPTION	14
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	15

((OPTION_C)) This is optional	16
((OPTION_D)) This is optional	18
((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	Each buffer of MD5 algorithm is ____ bit long
((OPTION_A)) THIS IS MANDATORY OPTION	32
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	64

((OPTION_C)) This is optional	128
((OPTION_D)) This is optional	512
((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	RSA is _____ cryptography
((OPTION_A)) THIS IS MANDATORY OPTION	Asymmetric
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public key

((OPTION_C)) This is optional	Both
((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 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Value generated by hash function is referred as ____
((OPTION_A)) THIS IS MANDATORY OPTION	Message digest
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Hash

((OPTION_C)) This is optional	MAC
((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)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	Which of the below is not service of digital signature
((OPTION_A)) THIS IS MANDATORY OPTION	Authentication to message
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Data integrity

((OPTION_C)) This is optional	Non-repudiaton
((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	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	___ digitally signs this entire information and includes digital signature in the certificate
((OPTION_A)) THIS IS MANDATORY OPTION	CA
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	KDC

((OPTION_C)) This is optional	PKI
((OPTION_D)) This is optional	DB
((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	In RSA ,e is used as ____
((OPTION_A)) THIS IS MANDATORY OPTION	Private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public key

((OPTION_C)) This is optional	Euler's totient
((OPTION_D)) This is optional	Session 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	

((MARKS)) QUESTION IS OF HOW MANY MARKS? (1 OR 2 OR 3 UPTO 10)	1
((QUESTION)) ENTER CONTENT. QTN CAN HAVE IMAGES ALSO	In RSA, d is referred as ____
((OPTION_A)) THIS IS MANDATORY OPTION	Private key
((OPTION_B)) THIS IS ALSO MANDATORY OPTION	Public key
((OPTION_C)) This is optional	Totient function
((OPTION_D)) This is optional	Session key
((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 E	A
((EXPLANATION)) This is also optional	