

Item Bank ID	410251	Item Bank Name	Information and Cyber Security	
Item Text	Option Text 1	Option Text 2	Option Text 3	Option Text 4
IPSec is designed to provide security at the _____	Transport layer	Network layer	Application layer	Session layer
_____ operates in the transport mode or the tunnel mode.	IPSec	SSL	PGP	SET
In IPSec ESP protocols stands for	Encryption Special Protocol	Encapsulating Security Payload	Encoding Special Payload	Entry Segment Protocol
In IPSec role of Security Association(SA) is	Security for data	Security from virus	Security from Intrusion	Security for Integrity
VPN is abbreviated as _____	Visual Private Network	Virtual Protocol Network	Virtual Private Network	Virtual Protocol Networking
_____ uses the idea of certificate trust levels.	X509	PGP	KDC	SSL
PGP offers _____ block ciphers for message encryption.	RSA	ECC	AES	IDEA
PGP have not used which cryptographic algorithms? i)DES ii) AES iii)RSA iv)Rabin	i), ii), iv)	i), iii), iv)	ii), iii), iv)	i), ii), iii)
Which one of the following is not a higher –layer SSL protocol?	Alert Protocol	Handshake Protocol	Alarm Protocol	Change Cipher Spec Protocol
Which protocol is used to convey SSL related alerts to the peer entity?	Alert Protocol	Handshake Protocol	Upper-Layer Protocol	Change Cipher Spec Protocol

Number of phases in the handshaking protocol?	2	3	4	5
In the Handshake protocol action, which is the last step of the Phase 2 : Server Authentication and Key Exchange?	Server_done	Server_key_exchange	Certificate_request	Certificate_verify
In SSL the client_key_exchange message uses a pre master key of size –	48 bytes	56 bytes	64bytes	32bytes
Key Management in IPSec is done by_____	Tunnel Mode	Transport Mode	IKE	ESP
Oakley Protocol is used for_____	Encryption of Payload	Encryption Key Exchange	Generate Message Digest	Authorization Services
Typically, _____ can receive application data from any application layer protocol, but the protocol is normally HTTP.	SSL	TLS	Either A or B	Both A or B
_____ is designed to provide security and compression services to data generated from the application layer.	SSL	TLS	Either A or B	Both A or B
In SSL which one of the following is not a session state parameter?	Master Secret	Cipher Spec	Peer Certificate	Server Write Key
In SSL which protocol consists of only 1 bit?	Alert Protocol	Handshake Protocol	Upper-Layer Protocol	Change Cipher Spec Protocol
In the alert protocol the first byte takes the value 1 or 2 which corresponds to _____ and _____ respectively.	Select, Alarm	Alert, Alarm	Warning, Alarm	Warning, Fatal