**21. What is the purpose of utilizing Diffie-Hellman (DH) algorithms as part of the IPsec standard?**

DH algorithms allow unlimited parties to establish a shared public key that is used by encryption and hash algorithms.  
DH algorithms allow two parties to establish a shared public key that is used by encryption and hash algorithms.  
**DH algorithms allow two parties to establish a shared secret key that is used by encryption and hash algorithms.\***  
DH algorithms allow unlimited parties to establish a shared secret key that is used by encryption and hash algorithms.

**18. Which two algorithms use Hash-based Message Authentication Code for message authentication? (Choose two.)**

AES  
DES  
3DES  
**MD5\***  
**SHA\***

**6. Which three statements describe the building blocks that make up the IPsec protocol framework? (Choose three.)**

**IPsec uses encryption algorithms and keys to provide secure transfer of data.\***  
IPsec uses Diffie-Hellman algorithms to encrypt data that is transferred through the VPN.  
IPsec uses 3DES algorithms to provide the highest level of security for data that is transferred through a VPN.  
**IPsec uses secret key cryptography to encrypt messages that are sent through a VPN.\***  
IPsec uses Diffie-Hellman as a hash algorithm to ensure integrity of data that is transmitted through a VPN.  
**IPsec uses ESP to provide confidential transfer of data by encrypting IP packets.\***

**15. What two encryption algorithms are used in IPsec VPNs? (Choose two.)**

IKE  
DH  
PSK  
**3DES\***  
**AES\***

**12. What is the purpose of the generic routing encapsulation tunneling protocol?**

to support basic unencrypted IP tunneling using multivendor routers between remote sites  
to provide fixed flow-control mechanisms with IP tunneling between remote sites  
**to manage the transportation of IP multicast and multiprotocol traffic between remote sites\***  
to provide packet level encryption of IP traffic between remote sites

**5. What is an IPsec protocol that provides data confidentiality and authentication for IP packets?**

AH  
**ESP\***  
RSA  
IKE

**10. What is one benefit of using VPNs for remote access?**

lower protocol overhead  
**potential for reduced connectivity costs \***  
increased quality of service  
ease of troubleshooting

**14. A network design engineer is planning the implementation of an IPsec VPN. Which hashing algorithm would provide the strongest level of message integrity?**

**512-bit SHA\***  
AES  
SHA-1  
MD5