May 10, 2024, Part 1+2, Multiple Answer Questions, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Sara must send a message to Rose, using asymmetric encryption. Which key shall use?	• Rose Public key • Rose Private key • Sara Public key • Sara Private key
WEP – Attacker sees valid auth exchange Challenge = 1001.0100, VictimResponse=0111.1110 To impersonate the Victim, which response must spoof if the next challenge is 0001.1000?	
By randomly generating about 350,000 codes composed of X decimal digits, the probability that two of them are identical is approximately 50%. How many digits are these codes composed of?	
If a cryptographic key is extended by an additional 13 bits, the security level increases by a factor of...	• Approximately 13 • Approximately 105 • Approximately 1300 • Approximately 8000 • Approximately 13000 • Approximately 8 million • Approximately 13 million
A 256 bytes plaintext is encrypted using AES-256-CBC. What is the overall size of the encrypted message?	• 256 bytes • 272 bytes • 288 bytes • 384 bytes • 512 bytes
What is the role of the AUTN in 3G authentication?	• Authenticate the client (user terminal) • Authenticate the network (base station) • Provide the encryption key • Provide the session integrity authentication
When using TSL_DHE_RSA_WITH_xxx…	• Peers can choose between DH and RSA for key mgmt • Peers must use both DH and RSA for key transport • peers use DH, with public coefficients signed by a CA using RSA • Peers use DH, with public coefficients signed by the client/server
Why ENCRYPT AND MAC is insecure?	• Because it is vulnerable to Chosen Plaintext Attacks • Because it is vulnerable to Chosen Ciphertext Attacks • Because it is vulnerable to padding oracle attacks • it is secure
How TLS prevents truncation attacks?	• By authenticating all TLS Record Data Units with HMAC • By sending close-notify alert right before the TCP FIN • By sending close-notify alert right after the TCP FIN • By authenticating the TCP FIN
When a Bleichenbacker's oracle may occur?	• When PKCS1-v1.5 padding is not properly applied • When server tells you if PKCS1 decoding is OK or fails • When server tells you if you guessed the victim's key • Since RSA is malleable, it always occurs, no way to avoid
In Ipsec IKE, a Stateless Cookie is	• A cookie which can be verified without any secret key • A cookie which can be verified without storing it in the server memory • A cookie which can be verified without being first transmitted • A cookie which has no State but can be used in any region of the world