April 19, 2024, Part 1+2, Multiple Answer Questions, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

To encrypt a message to be sent to Bob, Alex uses…	1. Alex Public key 2. Alex Private key 3. Bob Public key 4. Bob Private key
In AES-CTR, the hash function used for integrity is	1. MD5 2. SHA1 3. SHA256 4. Other: specify_____
In cellular systems, the Anonymity Key has the following role:	1. Authenticate the base station 2. Authenticate the user 3. Guarantee location privacy 4. Encrypt the IMSI
If you wish to increase robustness to brute force attacks to the key of a factor of about **8 millions**, how many extra bits you should add to the key?	1. 8 2. 13 3. 23 4. 64
A hash function has a 48 bit digest. What is, approximately, the collision probability after having computed about 10 million hash?	1. Lower than 1% 2. Around 10-30% 3. Around 50-60% More than 90%
In a fixed DH, the public coefficient g^x sent by peer A to peer B is	1. Signed with A private key 2. Signed with B private key 3. Encrypted with B public key 4. Signed by a certification authority
In RSA with modulus n=77, if the public key is e=3, the private key d is…	1. 74 2. 26 3. 1/3 4. Impossible as e=3 is not a valid public key.
With a TLS renegotiation attack, the adversary is able to:	1. Perform a session truncation attack 2. Read and modify the victim's data exchange 3. Insert plaintext before the victim's data exchange 4. Append plaintext after the victim's data exchange
The Bleichenbacher Oracle is…	1. A CPA attack to RSA 2. A CCA attack to RSA 3. A MITM attack to RSA 4. A reflection attack to RSA
In IPsec ESP in tunnel mode…	1. The inner IP header is integrity protected & encrypted 2. The inner IP header is only integrity protected 3. The outer IP header is integrity protected & encrypted 4. The outer IP header is only integrity protected