March 5, 2024, Part 1+2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q1: Multiple answer questions

In WEP authentication, the terminal responds to a challenge with:	1. The hash of the challenge and the secret key K 2. The encryption of the challenge with the secret key K 3. The HMAC of the challenge with the secret key K 4. The modular exponentiation of the key to the challenge
In AES-GCM, the hash function used for integrity is	1. MD5 2. SHA1 3. SHA256 4. Other: specify_____
In cellular systems, the AUTN has the following role:	1. Authenticate the base station 2. Authenticate the user 3. Guarantee location privacy 4. Signal the configuration of the network
A message authentication tag constructed as H(secret, message) is vulnerable to:	1. Hash collisions 2. State precomputation 3. Message expansion 4. It is NOT vulnerable
If a block cipher uses a block size of 16 bits, what would be, in principle, the possible value(s) for the key?	1. At most 16 bit 2. At most 16 bytes = 128 bit 3. At most 2^{16} = 65536 bit 4. Can be more than 2^{16} = 65536 bit
A server reply to a radius access-request message is authenticated as follows:	1. An MD5 hash of the user request message 2. An MD5 hash of the server reply message 3. An HMAC MD5 of the user request message 4. An HMAC MD5 of the server reply message
Which type of nonce is used in TLS during data transfer?	1. Time stamps 2. Sequence numbers 3. Random numbers 4. A combination of random and time stamp
The beast attack applies to which cipher?	1. All block ciphers 2. Only to block ciphers in the AES family 3. Only to block ciphers using CBC 4. Only to block ciphers using ECB
The number of hash computations necessary to construct a full Merkle tree with 8 leafs is…	1. 7 2. 8 3. 15 4. 16
HDKF constructs the i-th block as follows:	1. HMAC(context, i) 2. HMAC(context, HMAC previous block i-1) 3. HMAC(…HMAC(HMAC(context, seed))) i times 4. HKDF does not use HMAC
We refer to Traffic Flow confidentiality as approaches which permit to:	1. Protect a traffic flow from MITM attacks 2. Protect a traffic flow from packet replay attacks 3. Protect a traffic flow from statistical analysis 4. Protect a traffic flow via authenticated encryption
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

March 5, 2024, Part 1+2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q2: A challenge response authentication system uses a block cipher in CBC mode. The authentication scheme is based on the CBC encryption of the challenge message. Assume block sizes of 8 bits and challenges also of 8 bits. An attacker sees the following legitimate exchange from a victim:

← challenge = 1001.0110

Victim Response → (1000.1000) 0110.1110

The attacher now aims to impersonate the victim in a subsequent authentication. If the server sends a new challenge

← newchallenge = 1001.1100

Which response should the attacker spoof to successfully authenticate?
(show either the spoofed message as well as the approach used to compute such message)

Q3: Using the extended Euclidean algorithm, compute the modular inverse $\mathbf{13^{-1} \bmod 41}$

March 5, 2024, Part 1+2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q4: Briefly illustrate the main difference between a Relay and a Redirect agent in Diameter

Q5: Describe the Ephemeral Diffie Hellman Key agreement and discuss why it provides forward secrecy.

March 5, 2024, Part 1+2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q6. (TLS Padding Oracle Attack) – Assume a CBC-based block encryption scheme which uses block sizes of 4 bytes each. Assume that the attacker sees the following ciphertext comprising 6 blocks (hex notation):

f1 aa bb cc || 10 01 02 20 || <u>01 02 03 04</u> || 12 23 34 45 || 65 66 11 11 || ff f0 00 10

Assume now that the server is vulnerable to a Padding Oracle attack, and assume that the third block (the one underlined) contains a secret code which is either:

88 88 88 88 or 88 00 88 88

How many messages should the attacker send to the server/oracle to as to decrypt the code? And which specific modified ciphertext shall the attacker send?