December 18, 2024, Midterm 1+2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q1: **short questions**

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
which nonces are used as challenges in 3g+ mutual authentication?	• random challenges in both directions • sequence # for network auth, random for user authentication • random for network auth, sequence # for user authentication • time stamp + random + seq.# for both authentications
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
	•
	•
In a stream cipher, the IV:	• Must be truly random • Must be unpredictable • Must be constant • Must never repeat
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

December 18, 2024, Midterm 1+2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

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

Q2: **A binary Merkle tree** contains 8 data chunks, represented as leaves **L1, L2, …, L7, L8**. The Merkle root **R** has already been published.

1. Draw the structure of the binary Merkle tree, labeling all the intermediate hashes and the Merkle root **R**.
2. List the **exact quantities** (nodes / hash values) which must be provided to verify the integrity of leaf **L5**, and show how, exactly, the verifier reconstructs the Merkle root **R** using **L5** and the provided quantities.

Q3. Show how to provide **Forward Secrecy** in a system based on **constant pre-shared keys**

December 18, 2024, Midterm 1+2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

December 18, 2024, Midterm 1+2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q4. Prove that ENCRYPT **and** MAC is not IND-CPA secure

Q5. A CBC-based encryption scheme is used to secure network packets, where each block size is **4 bytes** (32 bits). Assume that the **first plaintext block** contains the **destination IP address** of a packet, and you know that the destination is an address in the 132.68/16 subnet (i.e. an address of the type 132.68.x.y). Given the IV (in red) and the ciphertext (in black), change the cyphertext so as to change the IP subnet destination into 140.64/16.

[10010111.10001110.00011111.11010011][00101001.11010011.00110101.01111000][……]

December 18, 2024, Midterm 1+2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q6: Consider an RSA system using modulus N =253 = 11x23.

1. Which, among the following potential public keys can be used?

- e=5 T F
- e=9 T F
- e=11 T F
- e=23 T F

2. let's now use e=7: **using the Extended Euclidean Algorithm**, compute the corresponding private key d.

3. **Using the Square&Multiply Algorithm**, encrypt message M=10.

4. Exploiting Parity Leak in RSA Encryption. In the above RSA scenario, the server inadvertently leaks the **parity** of the plaintext when an RSA-encrypted message is submitted, i.e. it reveals whether the decrypted plaintext is **odd** or **even.** Now assume that you see a ciphertext **CT=193**, which you know contains either **PT=128** or **PT=192**. Assuming that you CANNOT submit 128 or 192 as chosen plaintext, but you can modify the message via malleability, which **modified ciphertext** would you submit to the server, and why? Provide a clear explanation of your approach and reasoning.