December 18, 2025, Midterm 1+2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q1: short questions

Sara must **verify** a message digitally **signed** by Rose. Which key shall Sara use for this verification?	• Rose Public key • Rose Private key • Sara Public key • Sara Private key
For the following CBC-encrypted ciphertext: (0010)1101 How should it be modified in order to change the least significant two bits of the hidden plaintext?	• (0001)1101 • (1110)1101 • (0010)1110 • (0010)0001
For the following CRT-encrypted ciphertext: (0010)1101 How should it be modified in order to change the least significant two bits of the hidden plaintext?	• (0001)1101 • (1110)1101 • (0010)1110 • (0010)0001
What is the main purpose of the Request Authenticator in RADIUS?	• Provide freshness to be used for request authentication • Provide freshness to be used for reply authentication • Provide an IV for encrypting the Radius request • Provide material for exchanging the secret key
How does a DIAMETER redirect agent handle a request?	• Forwards the request to the destination server • Caches the associated response for future requests • Establishes a new security association • Replies with the address of a suitable server
Why are substitution ciphers insecure?	• They are based on too short keys • They allow chosen-ciphertext attacks • They preserve statistical structure of plaintext • They rely on symmetric keys
Why is SHA-256 a poor choice for password hashing?	• It produces too long outputs • It is too slow • It is too fast • It is not collision resistant
Why, in cellular systems, is SQN concealed with an anonymity key?	• To prevent tracking of the subscriber • To prevent subscriber IMSI catching • To guarantee fresh nonce in the authentication • To protect integrity of the SQN
In IPsec tunnels, being S and D the original source and destination, and X and Y the IP addresses exposed by the VPN gateways, which IP addresses are used inside and outside the tunnel?	• Outer IP: S→D, inner IP: X→Y • Outer IP: X→Y, inner IP: S→D • Outer IP: S→D, inner IP: encrypted payload only (no IPadd) • Outer IP: X→Y, inner IP: encrypted payload only (no IPadd)
Which IPsec protocol provides confidentiality?	• AH • ESP • IKE • IPCONF

December 18, 2025, Midterm 1+2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q2: **The following four data chunks of fixed size 4 bits each must be organized into a Merkle tree:**

A = 0100 B = 1110 C = 0001 D = 0011

Assume the following toy hash function that compress 4 bits in 2 bits: H({a, b, c, d}) → {a $\oplus$ b, c $\oplus$ d} – examples: H(1111) = 00; H(1101)=01; H(0101)=11

1. Compute the root of the Merkle Tree
2. Show which extra data should be provided to verify that D=0011 is included in the Merkle tree.
3. Suggest how you could ADD a fifth chunk E=1001 to the tree, without rebuilding the previous tree (highlight the changes necessary).

1:

H(A) = 10 H(B) = 01 H(C) = 01 H(D) = 00

H(H(A)|H(B))=11 H(H(C)|H(D))=10

ROOT = H(H(H(A)| H(B)) | H(H(C)|H(D)) = 01

2: Siblings S1= H(C)=01; S2= H(H(A)|H(B))=11

3: add H[E] as new separate block → NEWROOT = H[ROOT,H(E)] = 10

Q3. Briefly describe the TLS Renegotiation attack.

See lectures

December 18, 2025, Midterm 1+2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q4. A MAC scheme works as follows. It divides a message M in chunks M1, M2, …, Mn, uses an integrity key K, and produces the tag as:

HMAC(M1|1) ⊕ HMAC(M2|2) ⊕ … ⊕ HMAC(Mn|n)

By constructing an explicit (chosen message attack) example, show that this MAC is insecure (suggestion: use chosen messages comprising two chunks each).

Solution using messages with 2 chunks:

- Construct: → send to oracle
  - Ma = A C → ta = HMAC(A|1) ⊕ HMAC(C|2)
  - Mb = D B → tb = HMAC(D|1) ⊕ HMAC(B|2)
  - Mc = D C → tc = HMAC(D|1) ⊕ HMAC(C|2)
- And now forge new msg
  - M' = A B
- Whose tag can be computed by XORing tags provided by oracle, i.e.,
  - Tag[M'] = ta ⊕ tb ⊕ tc = **HMAC(A|1)** ⊕ ~~HMAC(C|2)~~ ⊕ ~~HMAC(D|1)~~ ⊕ **HMAC(B|2)** ⊕ ~~HMAC(D|1)~~ ⊕ ~~HMAC(C|2)~~ = **HMAC(A|1) ⊕ HMAC(B|2)**

Alternative solution using msgs of variable size:

  - Ma = C → ta = HMAC(C|1)
  - Mb = C B → tb = HMAC(C|1) ⊕ HMAC(B|2)
  - Mc = A → tc = HMAC(A|1)
- And forge new tag for M'=A B by XORing these three tags as before.

Q5. Forward Secrecy in TLS: discuss

1) Why RSA key transport does not provide FS
2) Why DHE provides FS

See lectures

December 18, 2025, Midterm 1+2, Computer & Network Security

SURNAME:_____ NAME: _____ MATRICOLA:_____

Q6: Consider an RSA system using **modulus N =253** = 11x23 and **public key exponent e=13**.

1. **using the Extended Euclidean Algorithm**, compute the corresponding private key d.

D=17

2. You now see a **ciphertext CT=112**, and you know that the corresponding plaintext is **either PT=6 or PT=7**. Assume now that the server exposes a **Bleichenbacher-type oracle**, which responds ACK if the PT is in the binary form **1111xxxx** and NACK otherwise. Which modified ciphertext CT' would you submit to determine the value of the hidden PT?

Being 240=11110000 we need to find a value r such that 6r<240 and 7r>=240. This is simply ceil(240/7) = 35 (indeed: 35x6=210=11010010, while 35x7=245=11110101). In conclusion: CT' = CT x (35)^e mod N = 112 x (35)^13 mod 253 = 112 x 52 mod 253 → **CT'=5**

3. **using the Square&Multiply algorithm**, and using the private key d computed at step (1) verify the answer to step (2) by **explicitly decrypting CT**.

PT = (112)^17 = 7

4. **without explicitly computing the CT' (but detailing how the attacking ciphertexts should be obtained)**, repeat question (2) by this time assuming that the hidden plaintext is either **PT=99 or PT=98**

CT' = CT * r^e, where r is selected such that it triggers the oracle only for one of the two values (r=5 is the smallest value which works)