Final Exam Practice Questions Solution
(50.020 Security)

Question 1: We discussed Man-in-the-Middle (MitM) attacks in the lecture. Please summarise the general idea, and which goals the attacker can achieve with it. In addition, please describe a network setting in that the attacker can launch such a MitM attack.
Up to 4 points for the general description. Up to 4 points for the goals of the attacks. Up to 4 points for description of the network setting that enables the MitM attack.

Solution:
General description:
In a MITM attack, the attacker is intercepting traffic between Alice and Bob
All traffic exchanged will first go to attacker, and then forwarded to destination
What to achieve:
Attacker can read, manipulate, drop, delay traffic at will
Attacker can also replay recorded traffic if needed
Setting:
Attacker is network provider: ISP, school IT, Internet backbone
Attacker does local ARP spoofing attack, or fake AP attack

Question 2: Please suggest reasonable key lengths to use with AES, RSA, and OTP encryption.
For each, provide a short comment on why you propose the respective length.
Up to 4 points for each algorithm's suggested key length, together with short comment (12 points total).

Solution: AES is secure with 128 bit key (default key size of AES128). RSA keys should at least be 2048 bit long (as suggested on slides). OTP keys need to have same length as the plaintext.

Question 3: We discussed the Diffie-Hellman protocol in the lecture. Please give a brief summary of the protocol: what is the goal? Which data is assumed to be publicly known before the protocol starts? Which messages are exchanged? How can both parties compute the final result from the exchanged messages?
Up to 5 points for the correct summary of the protocol. Up to 4 points for the correct exchanged messages. Up to 4 points for the correct description of the computation

of the final result.

Solution: Diffie-Hellmann allows two parties to establish a shared key, without leaking that key to a passive third party eavesdropper.
Alice and Bob initially agree on a g and prime modulus n. Then, Alice sends Bob $A = g^a \bmod n$, and Bob sends Alice $B = g^b \bmod n$. Both parties are now able to compute $g^{ab} \bmod n$, while no external eavesdropper can do the same (due to hardness of DLP).

Question 4: Please list the four properties that are required to be fulfilled for the operation of a group. Up to 2 points for each axiom's classification (8 points total).

Solution:
- Associativity
- Closure
- Invertibility
- Identity

Question 5: AES can be used with different key length. Please explain a) which key lengths are supported, b) what the main reason for using longer/shorter keys is, c) how the key length influences the general steps involved in AES.

Up to 3 points for correct key lengths, up to 3 points for the discussion of key length choice, and up to 3 point on the effect of key length on en/decryption in AES.

Solution: 128,192,256 bit length. Rounds: 10,12,14. Short keys=faster. Long keys=more secure against attacks.

Question 6: Please explain why users should only accept CA certificates of CAs they fully trust. What could a malicious CA do?
Up to 4 points for correct argument.
Solution: Malicious CA can sign any certificate, attacker can always MitM.

Question 7: Which of the following algebraic structures are groups, rings, and/or fields?

1) $\mathbb{Z}^+$ and –
2) $\mathbb{Z}$ and *, /
3) $\mathbb{Z}$ and –, *

Solution: None of the structures are groups, rings, or fields. In particular, - is not associative, and * is not distributive over /. - also has no closure over $\mathbb{Z}^+$.

Question 8: (6 points) Compute 5^{32} mod 7 using *square and multiply* algorithm. Show your working in detail.

Solution: Correct approach: square and multiply. 32=0b100000. So 5 rounds of squaring of 5 mod 7. Round 1: 4. Round 2: 2. Round 3: 4. Round 4: 2. Round 5: 4. Solution: 4

Question 9: For p = 5 and q = 7, compute a valid pair of public and private RSA keys. Note: the key might be somewhat untypical, and is obviously not very secure against brute-force attacks.
Up to 3 points for correct approach, up to 3 points for correct solution.

Solution: n=35. find de=k*phi(n)+1
Example: 5*5=1*24+1 so e=5 and d=5 is a valid pair (obviously not a good one)

Question 10: Alice wants to send a message m = 4 to Bob, using Elgamal. For the following Elgamal parameters, compute the ciphertext c sent from Alice to Bob: **modulus p = 7, generator g = 3, contributions from Alice and Bob a = 2, b = 3**.

Up to 3 points for correct steps in calculation, up to 2 points for correct result.

Solution:

$$B = g^b \mod p = 3^3 \mod 7 = 6$$
$$A = g^a \mod p = 3^2 \mod 7 = 2$$
$$c = m * B^a \mod p = 4 * 6^2 \mod 7 = 4$$

Question 11: Please compute a simple RSA signature for message $m = 2$, with public key $e = 3$, private key $d = 7$, and modulus $n = 33$.
Up to 6 points for correct steps in calculation, up to 3 points for correct result.

Solution: We can use square and multiply.

$$2^7 = (2^2 * 2)^2 * 2 \mod 33$$
$$2^7 = 8^2 * 2 \mod 33 = 64 * 2 \mod 33$$
$$2^7 = 31 * 2 \mod 33 = 29$$

So the resulting ciphertext is 29.

Question 12: Alice's public RSA key is $e = 7$, modulus $n = 91$. What is her private key d?
Up to 6 points for correct steps in calculation, up to 3 points for correct result.

Solution: We have to factorize $n = 91$, ideally starting with small prime numbers. $2, 3, 5$ are trivially not factors. $p = 7$ is a factor, leading to $q = 91/7 = 13$. So we can compute $\phi(n) = 72$. Now we have to compute Extended Euclidean Algorithm to find the multiplicative inverse of $e = 7$ such that $de = 1 \mod 72$, which is 31. So the private key $d = 31$.

Question 13:
(a) Consider the following key establishment scheme:
A trusted central server Charly can be used to store user's private (k_d) and public (k_e) RSA keys (to simplify discussion, assume a constant and public modulus n for all users). All users initially have the public key k_{ec} of the server. To register, Alice will send two messages to the server which contain her public and private keys, respectively, encrypted by using the public key of the server: $c_1 = (k_{eA})^{k_{ec}} \mod n$ and $c_2 = (k_{dA})^{keC} \mod n$. Charly will decrypt the keys, and (as confirmation) reply to Alice with a signature over the public key: $s = (k_{eA})^{kdC} \mod n$.

The attacker Eve was able to eavesdrop c_1 and c_2, and would like to obtain k_{dA}.
She is allowed to register one public/private key pair with Charly. Describe a way how could she be able to obtain k_{dA}.
Up to 12 points for the steps to conduct a working attack to obtain k_{dA}.

Solution: There are many possible attacks. As example: attacker sends c_2 as new c_1', and old c_1 as new c_2'. Server will then reply with a signature over k_{dA}. With the given signature scheme, it should be possible to recover Alice's private key from that.

(b) Propose a way to prevent the attack found in the previous part.
Up to 8 points for working suggestions on how to prevent the attack (e.g. changes to messages, additional messages, or processes on the server).

Solution: The easiest solution is to include an identifier in the two initial messages, e.g. $c_1 = (0||k_{eA})^{k_{eC}} \mod n$ and $c_2 = (1||k_{dA})^{k_{eC}} \mod n$. That will prevent replay attacks that change the context of the message. In addition, nonces could be used, the server could validate the key pair by testing it, and/or the server could use separate key pairs for encryption and signatures.

Question 14: Assume that two blocks in Bitcoin have identical hash values and identical headers, but contain different transactions. Is this a problem? Explain why it is (or not).
Up to 5 points for correct arguments.

Solution: This breaks the blockchain, as participants cannot know which set of transactions is legitimate.