You should be able to...

- ...explain how to use frequency analysis to break the Vigenere cipher and a substitution cipher. [Section 1]

- ...to apply frequency analysis to break the Vigenere and the substitution cipher. (In simple cases where no big computations are needed.) [Section 1]

- ...distinguish between ciphertext-only attacks, known-plaintext attacks, chosen-plaintext attacks, and chosen-ciphertext attacks. [Section 2]

- ...determine whether an encryption scheme has perfect secrecy. [Given: definition of perfect secrecy] [Section 3]

- ...explain the drawbacks of the one-time pad (both in terms of practicality and security). [Section 4]

- ...construct an attack on a scheme that uses the one-time pad incorrectly. [Given: definition of the one-time pad]

- ...list what disadvantages are unavoidable in schemes with perfect secrecy.

- ...for any part of the definition of perfect secrecy, explain why this part of the definition is as it is. [Given: definition of perfect secrecy]

- ...describe the components of a stream cipher. [Section 4]

- ...explain which properties a key stream should have and why.

- ...describe how an LFSR is constructed and how it can be used to build a stream cipher (an insecure one, though).

- ...from a fragment of the keystream produced by an LFSR derive the initial state (key) of the LFSR.

- ...describe the advantages and disadvantages of “best-effort design” and provable security.

- ...give examples of both.

- ...tell whether a given function is negligible or not (for common cases). [Given: definition of negligible]
• ...explain the different parts of the definition of IND-OT-CPA, i.e., why the definition is the way it is. [Given: definition of IND-OT-CPA]

• ...given a variant of the definition in which one of the parts are changed, give an example why this leads to undesirable consequences. (E.g., by describing a scheme that satisfies the definition while having drawbacks that are excluded by the original definition.) [Given: definition of IND-OT-CPA]

• ...explain the different parts of the definition of PRG, i.e., why the definition is the way it is. [Given: definition of PRG]

• ...given a variant of the definition in which one of the parts are changed, give an example why this leads to undesirable consequences. (E.g., by describing a scheme that satisfies the definition while having drawbacks that are excluded by the original definition.) [Given: definition of PRG]

• ...describe how to build a streamcipher from a PRG and sketch the reason for its security. [Given: definition of IND-OT-CPA]

• ...explain why a streamcipher constructed from a PRG is not IND-CPA secure.

• ...given an encryption scheme that is not IND-OT-CPA secure, explain why it is not IND-OT-CPA by giving an attack.

• ...describe how to make a PRG suitable for a streamcipher from a PRG that has 1-bit expansion. [Section 5]

• ...give an intuitive explanation why the resulting scheme is a PRG.

• ...describe what a block cipher is. [Section 6]

• ...describe what a Feistel network is.

• ...explain how to decrypt a ciphertext encrypted with a Feistel network.

• ...given the description of a block cipher similar in structure to DES, identify the objectives behind different parts of the block cipher (e.g., why is the key XORed in at a given place, why do we have a key schedule, why are certain bits permuted, why are S-boxes applied, why is the construction repeated, etc.)

• ...describe the meet-in-the-middle attack.

• ...explain why Double DES is not a big improvement over DES in terms of security while 3DES is.

• ...in variants of 3DES, estimate (very roughly) the number of steps needed for a meet-in-the-middle attack (e.g., 4DES, 3DES with repetitions of the key, 3DES with different key lengths in the different parts, etc.)
• ...explain the different parts of the definition of strong PRP, i.e., why the definition is the way it is. [Given: definition of strong PRP]

• ...given a variant of the definition in which one of the parts are changed, give an example why this leads to undesirable consequences. (E.g., by describing a scheme that satisfies the definition while having drawbacks that are excluded by the original definition.) [Given: definition of strong PRP]

• ...given an encryption scheme that is not a strong PRP, explain why it is not a strong PRP (e.g., by giving an attack).

• ...explain the different parts of the definition of IND-CPA (symmetric case), i.e., why the definition is the way it is. [Given: definition of IND-CPA]

• ...given a variant of the definition in which one of the parts are changed, give an example why this leads to undesirable consequences. (E.g., by describing a scheme that satisfies the definition while having drawbacks that are excluded by the original definition.) [Given: definition of IND-CPA]

• ...given an encryption scheme that is not IND-CPA, explain why it is not IND-CPA (e.g., by giving an attack). [Given: definition of IND-CPA]

• ...motivate why IND-CPA encryption (i.e., security against chosenplaintext attacks) is necessary. (I.e., why do we have to assume that the adversary can provide plaintexts of his choosing to be encrypted. – Example setting?) [Given: definition of IND-CPA]

• ...describe the relation between the different security definitions of encryption schemes (IND-OT-CPA, IND-CPA, strong PRP). Which implies which? Which does not imply the which (separating example)? [Given: definition of IND-OT-CPA, IND-CPA, strong PRP]

• ...determine in which situation which definition is needed and why (e.g., given the description of a use-case, tell which definition is necessary and why). [Given: definition of IND-OT-CPA, IND-CPA, strong PRP]

• ...describe ECB mode (either in formulas, or pictorially in the special case of a message consisting of a few blocks).

• ...explain the security drawbacks of ECB mode. [Given: description of ECB mode]

• ...describe CBC mode (either in formulas, or pictorially in the special case of a message consisting of a few blocks).

• ...explain why it is important that the IV is random in CBC mode. (Give attack for fixed IV against IND-CPA security.)
• ... describe CTR mode (either in formulas, or pictorially in the special case of a message consisting of a few blocks).

• ... sketch why CTR mode is IND-CPA secure and how it is related to stream ciphers.

• ... tell which of ECB, CBC, and CTR mode satisfy which security property.

• ... show that none of these is IND-CCA secure by giving an attack. [Given: description of ECB/CBC/CTR, definition of IND-CCA]

• ... describe what is the difference between symmetric and public-key cryptography, and what are the advantages of public-key cryptography. [Section 7]

• ... describe text-book RSA.

• ... show that decryption returns the correct message in text-book RSA.

• ... explain the relation between text-book RSA and the RSA assumption (in particular: if the RSA assumption holds, what do we know about the security of text-book RSA). [Given: definition of the RSA assumption].

• ... describe the ElGamal encryption scheme.

• ... show that decryption returns the correct message in ElGamal.

• ... explain the different parts of the definition of IND-CPA (public key case), i.e., why the definition is the way it is. [Given: definition of IND-CPA]

• ... given a variant of the definition in which one of the parts are changed, give an example why this leads to undesirable consequences. (E.g., by describing a scheme that satisfies the definition while having drawbacks that are excluded by the original definition.) [Given: definition of IND-CPA]

• ... given an encryption scheme that is not IND-CPA, explain why it is not IND-CPA (e.g., by giving an attack). [Given: definition of IND-CPA]

• ... explain the different parts of the definition of DDH assumption, i.e., why the definition is the way it is. [Given: definition of the DDH-assumption]

• ... explain why ElGamal is secure under the DDH assumption (i.e., explain why $m \cdot h^y \mod p$ hides $m$ if the DDH assumption holds). [Given: definition of ElGamal, DDH-assumption]

• ... explain what malleability means.
• ...given a malleable encryption scheme (ElGamal or text-book RSA), and a specific setting in which malleability poses a problem, describe an attack that makes use of the malleability. (Similar to the auction example and the chosen ciphertext attack example in Section 7.3) [Given: definition of ElGamal/text-book RSA]

• ...explain the different parts of the definition of IND-CCA (public key case), i.e., why the definition is the way it is. [Given: definition of IND-CCA]

• ...given a variant of the definition in which one of the parts are changed, give an example why this leads to undesirable consequences. (E.g., by describing a scheme that satisfies the definition while having drawbacks that are excluded by the original definition.) [Given: definition of IND-CCA]

• ...given an encryption scheme that is not IND-CCA, explain why it is not IND-CCA (e.g., by giving an attack). [Given: definition of IND-CCA]

• ...explain why IND-CCA security implies that a scheme is not malleable. [Given: definition of IND-CCA, description of what malleability means in a specific context]

• ...explain how hybrid encryption works.

• ...argue (without formal proof) why hybrid encryption is secure.

• ...say under which conditions a hybrid encryption scheme is IND-CPA/IND-CCA secure.

• ...describe collision-resistance.  \[\text{Section 8}\]

• ...give examples what collision-resistance is good for.

• ...explain the different parts of the definition of collision-resistance, i.e., why the definition is the way it is. [Given: definition of collision-resistance]

• ...given a variant of the definition in which one of the parts are changed, give an example why this leads to undesirable consequences. (E.g., by describing a scheme that satisfies the definition while having drawbacks that are excluded by the original definition.) [Given: definition of collision-resistance]

• ...given a hash function that is not collision-resistant, explain why it is not collision-resistant (e.g., by giving an attack). [Given: definition of collision-resistance]

• ...explain what a compression function is.

• ...explain how to construct a hash function from a compression function using the Iterated Hash construction.
• ...say under which conditions Iterated Hash is collision-resistant and which are its restrictions (in terms of security).

• ...construct a collision for Iterated Hash (given $x^*$ with $F(iv || x^*) = x^*$), potentially under certain additional requirements on the messages that should collide (as long as this does not lead to an attack substantially different from the one in the lecture notes). [Given: definition of Iterated Hash]

• ...explain why the Merkle-Damgård removes the restrictions of Iterated Hash (in terms of security). [Given: definition of Merkle-Damgård]

• ...for simple variations in the padding of Merkle-Damgård, explain why they are not collision-resistant. [Given: definition of the Merkle-Damgård]

• ...describe the birthday attack, its approximate running time and memory consumption.

• ...explain what a MAC is and what it is for. [Section 9]

• ...explain the different parts of the definition of EF-CMA (MAC case), i.e., why the definition is the way it is. [Given: definition of EF-CMA]

• ...given a variant of the definition in which one of the parts are changed, give an example why this leads to undesirable consequences. (E.g., by describing a scheme that satisfies the definition while having drawbacks that are excluded by the original definition.) [Given: definition of EF-CMA]

• ...given a MAC that is not EF-CMA, explain why it is not EF-CMA (e.g., by giving an attack). [Given: definition of EF-CMA]

• ...explain why the naive construction $MAC(k, m) := H(k || m)$ is insecure (assuming that $H$ is Merkle-Damgård constructed) by giving an attack. [Given: description of the naive construction, of Merkle-Damgård, definition of EF-CMA]

• ...explain why this (or a similar) attack does not work on the HMAC scheme. [Given: description of HMAC]

• ...list under which conditions HMAC is EF-CMA secure.

• ...explain under which conditions CBC-MAC is a secure. [Given: description of CBC-MAC, definition of EF-CMA]

• ...show that CBC-MAC is not secure by describing an attack. [Given: description of CBC-MAC, definition of EF-CMA]

• ...explain why that attack does not work on DMAC. [Given: description of DMA, CBC-MAC, definition of EF-CMA]
• ... tell what properties are needed from a hash function to use it to extend the message space of a MAC without losing EF-CMA security. [Given: definition of EF-CMA]

• ... sketch why EF-CMA security is not lost when using a suitable hash function for extending the message space [Given: definition of EF-CMA, definition of collision-resistance]

• ... describe the relation between the PRFs and MACs. Which implies which? Which does not imply the which (separating example)? [Given: definition of MAC, PRF]

• ... describe roughly how a cache-timing attack works. [Section 10]

• ... given the description of an S-box, compute entries in a linear approximation table. [Given: description of the row/column labels of the linear approximation table]

• ... given a linear approximation table, compute the probability that the XOR of a given set of inputs/outputs of an S-box is 0. [Given: description of the row/column labels of the linear approximation table]

• ... given a linear trail and a linear approximation table, compute the probability that the XOR of a given sets of plaintext/ciphertext bits is 0. [Given: description of the row/column labels of the linear approximation table]

• ... explain the different parts of the definition of one-way functions, i.e., why the definition is the way it is. [Given: definition of one-way functions]

• ... given a variant of the definition in which one of the parts are changed, give an example why this leads to undesirable consequences. (E.g., by describing a function that satisfies the definition while having drawbacks that are excluded by the original definition.) [Given: definition of one-way functions]

• ... given a function that is not one-way, explain why it is not one-way (e.g., by giving an attack). [Given: definition of one-way functions]

• ... explain why, if the encryption function of an encryption scheme is one-way, this does not make it a good encryption scheme (in terms of security). [Given: definition of one-way functions]

• ... explain the random-oracle model / the random-oracle heuristic. [Section 12]

• ... give an example why the random-oracle heuristic is unsound.

• ... given a protocol that is secure in the random-oracle model, and given a sketch of the main argument of the security proof, decide (and justify) whether this is a case where the random-oracle heuristic may or should not be applied (in view of its unsoundness).
• . . . explain what a signature is and what it is for.

• . . . explain the different parts of the definition of EF-CMA (signature case), i.e., why the definition is the way it is. [Given: definition of EF-CMA]

• . . . given a variant of the definition in which one of the parts are changed, give an example why this leads to undesirable consequences. (E.g., by describing a scheme that satisfies the definition while having drawbacks that are excluded by the original definition.) [Given: definition of EF-CMA]

• . . . given a signature scheme that is not EF-CMA, explain why it is not EF-CMA (e.g., by giving an attack). [Given: definition of EF-CMA]

• . . . tell what properties are needed from a hash function to use it to extend the message space of a signature scheme without loosing EF-CMA security. [Given: definition of EF-CMA]

• . . . sketch why EF-CMA security is not lost when using a suitable hash function for extending the message space [Given: definition of EF-CMA, definition of collision-resistance]

• . . . explain how to use text-book RSA as a signature scheme. [Given: description of text-book RSA encryption]

• . . . show that text-book RSA (as a signature scheme) is not EF-CMA secure by giving an attack. [Given: description of text-book RSA, definition of EF-CMA]

• . . . explain the difference between signatures and one-time signatures.

• . . . describe how to construct one-time signatures from one-way functions (Lamport’s scheme).

• . . . sketch why that construction is EF-OT-CMA secure. [Given: definition of EF-OT-CMA]

• . . . describe the chain based construction of stateful signatures from one-time signatures.

• . . . explain why that scheme is now a normal signature scheme (as opposed to one-time).

• . . . explain what the disadvantages of stateful signatures are.

• . . . sketch the construction of tree-based signatures (no need to cover: usage of PRFs to fix the randomness).

• . . . describe the RSA-FDH scheme.

• . . . explain why the attack that breaks the EF-CMA security of text-book RSA signatures does not break the security of RSA-FDH.
• ...list under what conditions RSA-FDH is EF-CMA secure (don’t over-
look the random oracle).

• ...discuss what we know about the security of RSA-FDH if we use a
real-life hash function $H$ instead of a random oracle.

• ...discuss advantages/disadvantages of symbolic cryptography.

• ...given a simple protocol, write down the adversary deduction rules.
  [Given: the deduction rules corresponding to the cryptographic primitives]

• ...given a set of deduction rules, write down the grammar of all messages
  that can be derived using these rules.

• ...given a grammar of all messages that can be derived by the adversary,
  and a security definition, and given a protocol, decide whether the protocol
  is secure in the symbolic model.

• ...given a set of deduction rules and a given message, show that the
  message can be deduced (e.g., by drawing a derivation tree).

• ...explain what zero-knowledge proofs are useful for.
  [Section 15]

• ...given a concrete setting and problem (similar to, e.g., the Peggy-Vendor
  example) describe how to use ZK proofs for solving the problem.

• ...explain what zero-knowledge means on a high-level (“the verifier learns
  nothing” is too high, the role of the simulator has to become clear).

• ...explain the different parts of the definition of computational soundness,
  i.e., why the definition is the way it is. [Given: definition of computational
  soundness]

• ...describe the graph isomorphism proof system.

• ...explain why it has soundness (what soundness error?). [Given: defini-
  tion of computational soundness]

• ...explain why a proof system with soundness error $\frac{1}{2}$ is not useful on its
  own, but can be used to construct a proof system with negligible soundness
  error.