University of Tartu | Prof. Dr. Dominique Unruh

Cryptology I

Exam study guide, spring 2018

Last Update: July 19, 2018

About the exam. The exam will be a written exam. You may not use external tools or notes. You are, however, allowed to bring one A4 page of handwritten notes (one page, not one sheet!). In the list below, sometimes it says "[Given: xxx]". In this case, you will be given "xxx" as part of the exam question. After the exam has been corrected, you will have to opportunity to look at the correction and, if present, point out mistakes in the correction. A re-exam will be scheduled only if needed.

Topics that were not mentioned in last year's exam study guide are marked in red. (Mainly for those who already started learning using the previous exam study guide.) Topics removed from last year's guide are not marked.

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.)
- ... 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).
- ... 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

- ... describe the advantages and disadvantages of "best-effort design" and provable security.
- ... give examples of both.
- ... 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 what a block cipher is. Section 5
- ... 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 AES, 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.)
- ... 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 chosen-plaintext attacks) is necessary. (I.e., why do we have to assume that the adversary can provide plaintexts of his chosing 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.)
- ... tell which of ECB and CBC mode satisfy which security property.
- ... show that none of these is IND-CCA secure by giving an attack. [Given: description of ECB/CBC, 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 6
- ... 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 $m \cdot h^y \bmod p$ 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 6.3.) [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. [Given: definition of IND-CPA/IND-CCA]
- ... describe collision-resistance. Section 7
- ... 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 limitations (in terms of security). [Given: definition of Iterated Hash]
- ... construct a collision for Iterated Hash (given x^* with $F(iv\|x^*) = iv$), 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 8
- ... 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 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 DMAC, 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 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]
- ... describe the relation between PRFs and MACs. Which implies which? Which does not imply the which (separating example)? [Given: definition of MAC, PRF]
- ... 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] Section 10

- ... 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]
- ... list which of the different cryptographic primitives discussed in the lecture (like PRGs, IND-CCA symmetric encryption, IND-CPA public key encryption, etc.) can be constructed from OWFs and which cannot.
- ... explain the random-oracle model / the random-oracle heuristic. Section 11
- ... 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. Section 12
- ... 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 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]
- ... 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]
- ... 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. [Given: definition of RSA-FDH]
- ... list under what conditions RSA-FDH is EF-CMA secure (don't overlook the random oracle). [Given: definition of RSA-FDH]
- ... discuss what we know about the security of RSA-FDH if we use a real-life hash function H instead of a random oracle. [Given: definition of RSA-FDH]
- ... discuss advantages/disadvantages of symbolic cryptography. Section 13
- ... 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 14
- ... 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 soundness, i.e., why the definition is the way it is. [Given: definition of soundness]
- ... describe the graph isomorphism proof system.
- ... explain why it has soundness (what soundness error?). [Given: description of the graph isomorphism proof system, definition 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. [Given: definition of soundness]
- Good luck!