CS/ECE 7349
Data and Network Security
Exam 1

Exam 1: Directions

This document contains the questions for the exam. For your answers, create a pdf document that clearly identifies every question number and your answer to that question. Name the file containing your answers 'yourLastNameCS7349Exam1.pdf'. For example, the file for Shaibal Chakrabarty would have the name ChakrabartyCS7349Exam1.pdf. Submit your pdf file.

Answer each question fully and completely. The highlighted words are your response guide – missing them will result in points deduction. Show all of your work and state your assumptions where appropriate. The questions may have 'hints' embedded within them regarding the answer. Treat these as directions. Follow these hints as appropriate for full points.

Collaboration is expected and encouraged; however, each student must hand in their own exam. To the greatest extent possible, answers should NOT be copied but, instead, should be written in your own words. Copying answers from anywhere is plagiarism, this includes copying text directly from the textbook. Any copied answers, identical answers to other students in the course (past or present) or otherwise plagiarized answers will receive a grade of zero. More than one plagiarized answer will result in a grade of 'F' for the exam with zero points earned and the procedure for academic dishonesty will be initiated. Do not copy answers. Always use your own words. Directly under each question list all persons with whom you collaborated and list all resources used in arriving at your answer. Resources include but are not limited to the textbook used for this course, papers read on the topic, class presentations and Google search results. Note that Google is not a reference. It is a tool to find references. Don't forget to place your name in the document itself.

ALWAYS provide references, your collaborators, and submit your answers in the format, and font, of the questions, in a .pdf file. Write the question and provide the answer in the same order (numbering) as the question.

Exam 1: Questions

1) In cryptography, what is a *cipher*? [Hint: be sure to define each of the answers as they relate to cryptography and choose the answer that is most appropriate to what has been discussed in class.]
   a) An encrypted message
   b) An algorithm for performing encryption and decryption
   c) A zero
   d) A code
2) Consider the modes of operation for a block cipher. Which of the following modes of operation creates a keystream to be XORed with the plaintext for encryption? [Hint: explain each of the identified modes of operation and use a diagram to help explain how it operates.]
   a) Counter Mode
   b) Output Feedback Mode
   c) Stream Mode
   d) All of the above.
   e) None of the above.
3) What is the foundation of all security on the Internet? [Hint: in your explanations of the not correct options, for each not correct option explain how the option depends upon your chosen answer.]
   a) Cryptography Encryption and Decryption
   b) Trust
   c) Authentication
   d) Public Key Certificates
   e) Digital Signatures

4) What does it mean to be secure?
   a) Security means the coercive capability to stop an aggressor. Security is freedom from war, and the ability to deter or defeat aggressive attacks.
   b) Security refers to safety from vulnerabilities (both external and internal) that could harm the state, societies within the state, and the values of those societies.
   c) Security means freedom to enjoy the things that are most important to human survival and well-being, such as food, health care, and the opportunity to live well.
   d) All of the above.
   e) None of the above.
5) Consider the modes of operation for a block cipher. Which of the following modes of operation allows for the decryption on each block to be performed in parallel? [Hint: explain each of the identified modes of operation and in 1-2 sentences describe how decryption operates (identify the parallelism for your answer(s) if any).]
   a) Counter Mode
   b) Cypher Block Chaining Mode
   c) Electronic Codebook Mode
   d) All of the above.
   e) None of the above.
6) Which of the following are properties of a secure hash function? [Hint: explain each of the properties and explain why your chosen property(ies) is (are) required of a secure hash function.]
   a) The hash value is preimage resistant.
   b) The hash value is second preimage resistant.
   c) The hash values are collision resistant.
   d) All of the above.
   e) None of the above.
7) Which of the following best describes someone who gains illegal access to a computer system? [Hint: go beyond any single definition of a term and look at each term's historical and other meanings to identify the best answer.]
   a) Hacker
   b) Identity Thief
   c) Intruder
   d) Cyber-terrorist
8) Which of the following are ethical issues facing the use of technology in business today? [Hint: explain why each of the possible answers a, b and c either is or is not an ethical issue.]
   a) e-mail privacy
   b) Software piracy
   c) Intellectual property rights and copyrights
   d) All of the above
   e) None of the above
9) Which of the following are desired characteristics of a pseudorandom number generator? [Hint: explain why each of the answers a, b and c either is or is not a desired characteristic and why.]
   a) Scalability
   b) Backward Predictability
   c) A Shared Initialization Vector
   d) All of the above
   e) None of the above
10) Which of the following is primarily used to provide integrity protection for a message sent between Alice and Bob? [Hint: for each of the answers a, b and c, explain how it is typically used and the security functionality (e.g., integrity) that is provided with that typical usage. For those choices that may be used to provide integrity protection, explain how it is used to provide integrity protection if that is not its typical usage.]
   a) Hash function
   b) Private key operation
   c) Symmetric key operation
   d) All of the above
   e) None of the above

11) Which of the following can be used to increase the strength of a specific cipher? [Hint: explain how each of the answers a, b and c either can or cannot be used to make a cipher more secure. Hint Hint: ask yourself if any of the answers would cause the cipher to be changed as a result - in which case, it doesn't increase the strength of a specific cipher.]
    a) Shared Secret Key
    b) Keep Algorithm Details Secret
    c) Use a Key with a Larger Number of Bits
    d) All of the above
    e) None of the above
12) Which of the following are basic block cipher design principles? [Hint: explain why each of the answers a, b and c either is or is not a basic design principle.]
    a) Use both linear and non-linear functions.
    b) Use one or two more rounds than the minimum to achieve randomness.
    c) Have good avalanche properties.
    d) All of the above
    e) None of the above
13) Which of the following is an authenticated encryption (AE), also called authenticated encryption with associated data (AEAD), cipher? [Hint: provide a brief description for each of the named ciphers, and a published reference paper for each.]
    a) Grain 128-A
    b) Hummingbird 2
    c) Keyak
    d) All of the above
    e) None of the above
14) In public key cryptography, one key is made public (the public key) and one key is made private (the private key). Which of the following statements is true of public key ciphers?
    a) The public key encrypts only, so it must take the plaintext as input.
    b) The private key is used only for decryption of ciphertext encrypted with the public key.
    c) In RSA in theory, once the keys are calculated, if the 'public key' is kept secret and the 'private key' is made public, the cipher is not secure.
    d) All of the above
    e) None of the above
15) Which of the following are attacks that can be mitigated by a secure message authentication code? [Hint: for each answer a, b and c, describe the attack and show how a message authentication code mitigates (or not) the attack.]
    a) Message authentication code modification
    b) Message modification
    c) Source repudiation
    d) All of the above
    e) None of the above
16) Explain the birthday paradox and provide an example illustrating it's detrimental impact on the security of a system. Create a table illustrating the birthday paradox for variables of bit size $n = 16, 32, 64, 128, 256$ and 512. [Hint: your answer should include at least two paragraphs and a table. Calculate the table values yourself.]
17) Computer networks are designed following a layered model. For the five layer network model, for each layer identify at least one specific security protocol that is used for communications at that layer. Identify at least one peer reviewed published paper or RFC standard (look to RFCs first) that defines security for a particular layer and in 2-3 paragraphs explain the security protocol. Note that unique security protocols exist at every layer, including the Physical Layer. [Hint: search peer reviewed publications and standards for security at each layer. Use a table to summarize each layer security.]
18) A Denial of Service (DoS) attack is a security event that occurs typically over the Internet. Identify and describe two approaches/mechanisms that attackers use or have used to carry out DoS (or Distributed DoS - DDoS) attacks. For each attack approach, identify an article (peer reviewed, white paper or non-peer reviewed) that describes how the attack was used in an actual attack. Summarize the attack in 2-3 paragraphs and identify potential approaches that could be used or have been implemented to mitigate the attack.
19) Describe how a man-in-the-middle attack can be defeated during the process of establishing a secure communication channel between Alice and Bob. You may use symmetric key ciphers, public key ciphers, certificates, hash algorithms, or any other security mechanism discussed in class. [Hint: describe the complete sequence of steps in as much detail as possible. Do not skip steps. Do not skip details. Draw a communication diagram that illustrates each step.]