CS 478: Network Security (Spring 2016)

Instructor: Dr. Attila A Yavuz

Homework 1 (04/07/2016)

(Assigned on 04/07/2016, deadline (sharp) on 04.21.2016)

Remarks: This homework focuses on basic concepts, symmetric ciphers, DES, AES, cryptographic hash functions, use of encryption and MACs, and security properties/definitions. This homework aims at extending your knowledge on the complementary aspects of the topics covered during the class (so it goes beyond the material simply put on the slides, as described and emphasized before).

Requirements: HW will be completed by each student **individually (no collaboration)**.

Directly borrowing (e.g., copy-paste) from any material and putting in solutions (e.g, from online solutions, Wikipedia, or research papers) is **plagiarism** (see Syllabus for its corresponding actions). Please cite very carefully each resource you use, but citing a solution does not give a license to directly put it as an answer**. All of your answers must be in your in own words and interpretations.**

HW should be prepared by a text editor (e.g., Microsoft Word or Latex). Handwritten submissions are *not* accepted.

---

1) [5] Question about basic concepts:

- (2) What are the main security/performance trade-offs for symmetric and asymmetric cryptography to be deployed in practice? Could you give real-life scenarios where symmetric and asymmetric crypto could be more suitable?
- (2) OTPs are highly secure, but why we do not see them much in practice?
- (1) Does Kerckhoffs's principle contradict with the "secret algorithm" practice in military systems? Given sufficient financial capability, how could you incorporate Kerckhoffs's principle into such high-end systems?

2) [8] Data Encryption Standard (DES). DES has weak keys.

- (3) What is the difference between a weak key, a semi-weak key and a possible weak key?
- (3) What is double DES? What kind of attack on double DES makes it useless?
- (2) What is triple DES? How many keys are use in triple DES process?

3) [8] Block Cipher Design Principles and AES

- (2) What is the basic design technique, which is frequently used to construct modern symmetric ciphers?
- (2) What are the main security properties achieved via this designed technique? (4) Given the example of AES, which functional steps enable achieving these properties? Please provide specific names of these operations and briefly explain how they are applied in AES (all answers are brief for this question)?
- (4) What are the benefits of the use of finite field arithmetic in AES?

4) [12] We have discussed various Symmetric Encryption Modes. Each of these modes satisfies certain properties, which can be an advantage or disadvantage for a given application. Construct a table providing a summary information about each mode and its corresponding properties. For example, each row of the table will be properties (e.g., parallel operation, ciphertext manipulation, pre-computation, etc., please see course notes for more properties) and columns are Modes (e.g., CBC, CTR…). Each cell will take a value such as "Yes", "No", "partially", "high", "low" etc. according to given encryption mode and property.

5) [10] "Ciphertext manipulability" is generally considered as an undesirable property for Encryption Modes. However, for modes that operates in stream cipher fashion (discussed in class), by design, it is possible to flip bits in plaintext by flipping bits of ciphertext.

- (1) Why is this possible?
- (5) Is there a way to turn this (potentially) undesirable property into an advantage, describe how if there is one?
- (4) Which extra cryptographic function (a group of functions discussed in the class) can be applied to the ciphertext so that the aforementioned advantage can be obtained without compromising the security?

Hints: (i) Consider noisy communication channels as application domain to exploit this feature. (ii) The extra cryptographic function will require annexing a small-constant tag to the ciphertext.

6) [6] Encryption *(E)* and Compression *(C)* are generally used together to achieve confidentiality and efficiency simultaneously. Given a message M, with which order function *E* and *C* must be applied? What are the reasons behind of this particular order?

7) [20] In symmetric key cryptography, it is desirable to achieve both confidentiality and authentication (also provides integrity) of the data. These properties can be achieved via Encryption *(E)* and Authentication Functions *(A)*, respectively. What is the correct order of these operations? Lets assume the specific notation and order of these operations are as follows:

Authenticate-then-Encrypt (AtE)
Encrypt-then-Authenticate (EtA)
Encryption and Authentication (E&A) or the opposite way as (A&E)

Discuss the security implications of these choices, which one is recommended and why?

Mention important crypto papers (at least one, cite it), in which the security of an important real-life protocol (Hint: the protocol that securely connects your VPN for each e-commerce transaction!) analyzed based on the above orders. Explain why this order matters a lot in practice? You may provide some discussions from these papers (please be brief, just hit on important points).

8) [11] Given a modern cryptographic hash function (e.g., SHA) with *m-bit* length output, what is the maximum security it can provide in terms of *m* (lets call it *x-bit* security)? A generalized proof for any given *m-bit* hash function is available to show why it can achieve at best *x-bit* security. Please describe this generalized proof (related birthday attack concept) that simply connects *m-bit* to *x-bit*.

9) [10] What is the hash length extension attack? Please describe by giving some specific real-life examples.

10) [10] Properties of cryptographic hash function

- (5) What are the essential properties that a cryptographic hash function must satisfy?
- (5) What is a Random Oracle and how does it play a role in the security proofs in general (what is its relation with cryptographic hash functions?).