CS / ECE 478: Introduction to Network Security (Spring 2018)

Instructor: Dr. Attila A Yavuz

Homework 2
(Assigned 4/23/18, Due 5/07/18 in class)

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 own words and interpretations.

HW should be prepared by LaTeX or Word. Handwritten submissions are not accepted.

1) Data Encryption Standard (DES). DES has weak keys. [8 m]
   - (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?

2) Block Cipher Design Principles and AES [8 m]
   - (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?

3) 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? [6 m]

4) 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). [16 m]

5) Name a mode of encryption that can achieve full parallelization (both encryption and decryption), pre-computability, random memory access, security against ciphertext manipulation and error spreading. Describe, for each property, how does this mode of encryption achieve them. [8 m]

6) RSA basics [12 m]
What is the role of Euler-Function, Extended Euclid Algorithm and Fermat Little Theorem in RSA encryption? Explain the role of each by showing the specific step in RSA encryption and decryption process. [4 m]

Using Euclid’s algorithm (Not extended, but just Euclid), calculate the g

gcd(16261, 85652). Using Fermat’s little theorem, compute 3^31 (mod 7) (Hint: Decompose the exponent) [4 m]

In RSA, public key e can be smaller than the private key d. What are the performance and security implications of this? What should be considered for selecting public exponent e as a security metric? [4 m]

7) RSA based primitives [16 m]
In RSA encryption and signatures, the use of private/public key pair between sender and verifier is swapped. Why this is the case? (Hint: Think about the purpose of signatures and encryption. Also, think about the purpose of authentication and its difference from encryption) [8 m]

Textbook implementation of RSA is subjected to timing-based side-channel attacks. Explain why (Hint: see how square and multiply algorithm works and tie this to a side-channel attack). Describe a simple blinding technique that can prevent this basic side-channel attack. This technique is also called masking. [8 m]