11210/IIS500200 Network Security, Fall 2023 **Due: 9-Jan-2024**

Homework 2&3

Instructor: Prof. Amir Rezapour

1. Consider the following hash function. Messages are in the form of a sequence of numbers in Z_n,$M = (a_1, a_2, \ldots, a_t)$. The hash value h is calculated as $(\sum_{i=1}^{t} a_i^2)$ mod n for some predefined value n.

   (a) Does this hash function satisfy any of the requirements for a hash function listed bellow? Explain your answer for each case.

   - It can be applied to a block of data of any size. (5 points)
   - It produces a fixed-length output. (5 points)
   - It is relatively easy to compute for any given input. (5 points)
   - Preimage resistance. (10 points)
   - Secondary preimage resistance. (10 points)
   - Collision resistance. (10 points)

   (b) Compute the hash for $M = (120, 145, 224, 657)$ for $n = 981$. (5 points)

2. The chart below shows an authentication protocol, followed by data exchange, followed by disconnection. Only an initial part of the authentication protocol is shown; here, pw is A's password, J is a key derived from pw, and L is a high-quality key. Assume an attacker that can (1) eavesdrop messages and (2) intercept and spoof messages sent by A (but not those sent by B). Complete the authentication protocol (i.e., Supply the part indicated by the "** .... * *") so that in spite of this attacker

   - B authenticates A,
   - this authentication is not vulnerable to off-line password guessing, and
   - A and B establish a session key S (for encrypting data) such that after A and B disconnect and forget S, even if the attacker learns pw, the attacker cannot decrypt the data exchanged. (15 points)

A (has pw)	B (has J)
send [conn] to B	
	generate random challenge R send [R]
compute J from pw compute X ← encrypt(R) with key J send [X] to B	
	compute Y ← decrypt(X) with key J if Y = R then A is authenticated

3. Suppose that the current replay window spans from 111 to 430. (15 points)

(a) If the next incoming authenticated packet has sequence number 99, what will the receiver do with the packet, and what will be the parameters of the window after that?

(b) If instead the next incoming authenticated packet has sequence number 420, what will the receiver do with the packet, and what will be the parameters of the window after that?

(c) If instead the next incoming authenticated packet has sequence number 566, what will the receiver do with the packet, and what will be the parameters of the window after that?

4. An attacker is intent on disrupting the communication by inserting bogus packets into the communications. Discuss whether such an attack would succeed in systems protected by IPsec. Discuss whether such an attack would succeed in systems protected by SSL. (10 points)

5. Can a packet filter block all incoming email containing the phrase "Homework 2 is out"? If yes, show a packet filtering ruleset that provides this functionality; if no, explain it. (10 points)