Isfahan University of Technology
Information Technology Engineering
Dr. Manshaei
Homework 1: Module B.2 Implementing Trustworthy Computing
Deadline: Wednesday 30^{th} **Azar, 1401, at** 23 : 59

We only accept the homework **delivered via (yekta.iut.ac.ir), before the deadline**.

1. Consider two prime numbers p=23 and q=19. Calculate the public/private key pair using these numbers and encrypt "00110010" using the calculated public key.

2. Consider the variation of MAC algorithm (following figure) where Sender sends $(M, H(M)+S)$. Could Trudy break in this system? How? Show the decryption diagram in receiver!

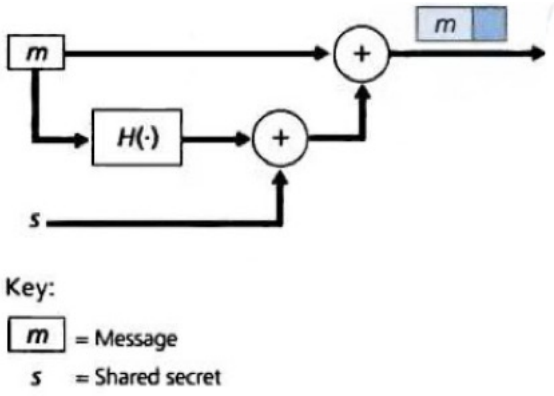

Figure 1:

3. Why the public key is not used to encrypting entire messages and only used for signing message's digest?

4. Suppose Alice has a message that she is ready to send to anyone who asks. Thousands of people want to obtain Alice's message, but each wants to be sure of the integrity of message. In this context, which schema do you suggest for providing a suitable integrity check? Why?

5. Suppose that Alice and Bob shared a secret key (S) and they authenticate each other based on challenge-response mechanism. Their authentication procedure shown in following figure. How Trudy can impersonate her to Alice as Bob?

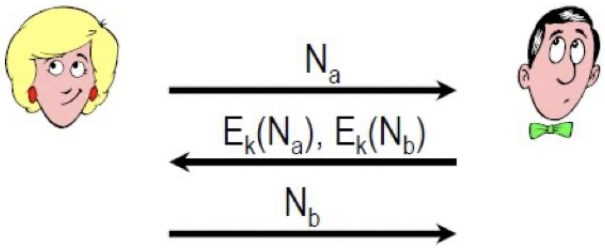

Figure 2:

6. Suppose Bob initiates a TCP connection to Trudy who is pretending to be Alice. In what step of the SSL handshake algorithm will Bob discover that he is not communicating with Alice? How?

7. With one example, explain the main difference between Stateful Packet Filters and Stateless (or Traditional) Packet Filters in firewalls.

8. **Research Question:** Explain why using RC4 was not a good option for WEP in IEEE 802.11 WiFi network.