Midterm (1 hour)

1. Consider symmetric key encryption, public key encryption, hash function. Which encryption technique should you use for providing:
2. Confidentiality? (4 points)
3. Message integrity? (3 points)
4. Non-repudiation? (3 points)
5. Draw the layered structures (including all layers’ names) of OSI reference model and TCP/IP model. (10 points)
6. Alice needs to securely send a large amount of confidential video data to Bob. Since Alice’s computer is slow, which of the following methods should she choose for achieving the best efficiency and confidentiality? RSA, AES-128, MD5, SHA1, cleartext. Why? (10 points)
7. Assume Alice would like to send message M with an one-time transmission. She encrypts in the following manner:

*C1= Hash(M), C2= Enc\_Kpub(M)*

Then (*C1,C2*) will be sent to Bob together. *Enc()* denotes the encryption function. Kpub denotes the public key.

1) What security property, in terms of confidentiality, message integrity, and authenticity, could be achieved? (5 points)

2) In order to provide such security, whose public key is used? (5 points)

1. Assume Alice chooses a very uncommonly used encryption scheme to protect her message’s confidentiality sent to Bob. She thinks since this scheme is not commonly used so there is no need to keep her key secret. Is her choice correct? If not, which of the ‘9-principles’ is that against with. (10 points)
2. A stream ciphertext received by Bob is this: 0010 1011 0101. The key is 1011 0101 1001. What is the plaintext? (10 points)
3. A MySQL user account created for pulling records from a database doesn’t need admin rights. Which 9-principles this is following? (10 points)
4. TCP connect() port scanning will establish a connection with the target device. Such a behavior will be recorded by the target device. To avoid being recorded, what else **TCP** port scanning method could we use? (10 points)
5. For the linux user login system, could an attacker figure out whether two users’ passwords are the same? Why? Assume the attacker could have access to the system files that store user login information. (10 points)
6. For Question 4, if Alice repeatedly sends different messages M1, M2, M3 ....... to Bob using the same method, is there any security threat? If yes, why? (10 points)