CS2910 Exercise: Cryptographic Algorithms

Names: ____

Protecting Confidentiality

1. Suppose a message is encrypted using a block cipher resulting in the following blocks, represented as hex values

A492B20E	3F739193	D5886EEf	151BC788	A492B20E	BC35AA52

   a. ***Write*** how many bytes of data are in each encrypted block.

   b. ***Write*** what you can determine about the original message from the encrypted data. (Hint: You can determine something.)

   c. ***Write*** how the message could have been made more secure.

2. Stream Cipher. A message is encoded by exclusive-or'ing each bit with a random bit stream. (In exclusive or, 0⊕0 = 0, 1⊕0 $= 1$, $0 \oplus 1 = 1$, and $1 \oplus 1 = 0$.)

   a. Recover the original message from the random stream and encrypted stream, by ***filling*** in the blanks in the "Recovered" and "ASCII" rows.

Message:	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?
Random	1	0	1	0	0	0	0	0	1	0	1	0	0	1	1	1	0	0	1	0	0	1	0	1
Encrypted	1	1	1	1	0	0	1	0	1	1	1	1	0	1	0	0	0	1	1	0	0	1	0	0
Recovered																								
ASCII																								

   b. ***Write*** that this method does or does not have the same problems as the block cipher in Problem 1. ***Explain*** your answer.

   c. ***Write*** two ways that the sender and receiver might share the "Random" stream. ***Write*** an advantage for each way.

3. (Challenge) Caesar Cipher. ***Decrypt*** this message: IAAP IA WP PDA WPDHAPEY BEAHZO WP 2LI. The key is not provided.

Confidentiality with Public-Key Cryptography.

4. Suppose Alice has a public key K_A^+, a private key K_A^-, and that Bob has a public key K_B^+, and a private key K_B^-.
   a. If Bob encrypts a message M with his private key to yield the ciphertext $C = K_B^-(M)$ …
      i. ***Circle one***. This message is secure/insecure (accessible to Trudy)
      ii. ***Circle one***. This message is accessible/inaccessible to Alice
      iii. ***Explain*** your choices.

   b. If Bob encrypts a message M with his public key to yield the ciphertext $C = K_B^+(M)$ …
      i. ***Circle one***. This message is secure/insecure (accessible to Trudy)
      ii. ***Circle one***. This message is accessible/inaccessible to Alice
      iii. ***Explain*** your choices.

   c. If Bob encrypts a message M with Alice's public key to yield the ciphertext $C = K_A^+(M)$ …
      i. ***Circle one***. This message is secure/insecure (accessible to Trudy)
      ii. ***Circle one***. This message is accessible/inaccessible to Alice.
      iii. ***Explain*** your choices.

   d. ***Write*** why Bob can't encrypt a message with Alice's private key K_A^-.

Message Integrity and Authentication with RSA

5. Suppose Alice would like to send a message to Bob. Alice creates a message M, and computes a cryptographic hash H = hash(M) of the message, and sends both the message and hash to Bob without encryption: (M,H). Trudy intercepts the message before it reaches Bob. Trudy edits the message to her desired text M2. Trudy also recomputes the hash H2 = hash(M), and sends both (M2,H2) on to Bob.

   Based on this story, ***write*** whether Bob can tell that the message (M2, C2) has been altered.

6. Suppose Alice now writes a message M, computes the cryptographic hash H = hash(M), and then encrypts the hash using her private key, $C=K_A^-(M)$.

   Based on this story,
   a. ***write*** how Bob can recover the hash. ***Explain*** your answer.

   b. ***write*** whether Trudy can modify the message to make it appear that it is from Alice. ***Explain*** your answer.

7. Suppose Alice now writes a message M, computes the cryptographic hash H = hash(M), and then encrypts the hash using Bob's public key, $C=K_B^+(M)$.

   Based on this story,

   a. ***write*** how Bob can recover the hash. ***Explain*** your answer.

   b. ***write*** whether Trudy can modify the message to make it appear that it is from Alice. ***Explain*** your answer.

8. Suppose Alice now writes a message M, computes a ***non-cryptographic*** hash H = hash(M), and then encrypts the hash using her private key, $C=K_A^-(M)$.

   Next, after careful investigation, Trudy discovers that she can create a forged message M2 that hashes to the same non-cryptographic hash H = hash(M2). ***Explain*** how Trudy can use this discovery to modify the message (M,C) from Alice and make the resulting message appear to be from Alice still.

Chosen-plaintext attack

9. Suppose Alice encrypts a message M with Bob's public key $C = K_B^+(M)$, and that Trudy obtains C. Trudy has a guess what the message from Alice is – or at least a list of 1000 guesses, one of which is correct. ***Explain*** how Trudy can recover the message, without using Bob's private key K_B^-.

Session Key Change with Public Key Cryptography

10. (Challenge) Suppose Alice would like to send a randomly-generated session key to Bob, to be used for encrypting the rest of their traffic.

    a. ***Explain*** (possibly symbolically) a procedure that Alice can use to encrypt this key so that (1) only Bob can read it and (2) Bob knows it comes from Alice.

    b. ***Explain*** how Bob can extract the key.