HW1 Reference Answers.

(Reference answers are based on textbook and online resources.)

1. (10 points) Research by yourself and explain the following concepts. Try google.

- What are botnets?

A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. Most of the case botnets means illegal and malicious. it could be used to send spam email or participate in distributed denial-of-service attacks.

- What's phishing?

Phishing is the attempt to acquire sensitive informationsuch as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. It works in ways of email, website, and malicious software.

- What's rootkit?

Rootkit is a malicious software which is designed to hide the existence of certain processes or programs (normally malicious) from normal methods of detection once the attacker obtained the root or administrative access to a computer.

- What's heartbleed bug?

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

- What is Stuxnet?

Stuxnet is a computer worm that was designed to attack industrial programmable logic controllers (PLCs). The attacked machines basically uses microsoft windows operating systems. Stuxnet has three modules: a wormthat executes all routines related to the main payload of the attack; a link filethat automatically executes the propagated copies of the worm; and a rootkitcomponent responsible for hiding all malicious files and processes, preventing detection of the presence of Stuxnet

2. (5 points) Problem 2 on page 57 in textbook.

Hash can be recreated by the attacker and appended to the modified message. This authentication solution is not secured.

3. (5 points) Problem 3 on page 57 in textbook.

They are equally insecure. Alice can obtain Carol's key when communicate with Carol, then Alice could impersonate Carlo to Bob. Knowing other people's keys, any one of the three can impersonate the other to the third.

4. (5 points) Problem 5 on page 58 in textbook.

As the problem statement said, the hint is that Alice can open two connections to Bob. As Figure 2-1 shows, Alice can send r_A to Bob and receive r_A encrypted by K_{AB} from Bob. After receiving the challenge r_B from Bob, Alice can open a second connection and send r_B to Bob, and Bob will send back r_B encrypted by K_{AB}. Next, Alice can use it in the first connection to authenticate to Bob.

5, (5 points) Problem 3 on page 92 in textbook.

Possible keys: 2^56

Ciphertext blocks: 2^64

On average: 2^56 / 2^64 = 1/256

6. (10 points) Problem 6 on page 92 in textbook.

Bits are not used equally.

The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Each round 8 bits are left out. After 16 rounds totally 8*16 = 128 bits are left out. Since the key size (56 bits) does not divide 128 bits that are left out, each bit can not be used equal number of times. [5 pts]

The bits that are not used for each of the 16 keys are as follows [5 pts]:

round #	Bits not used
1	6 7 11 12 43 46 50 52
2	3 4 35 38 42 44 61 62
3	19 22 26 45 46 52 55 57
4	3 6 10 29 30 36 39 41
5	13 14 23 25 49 52 53 59
6	7 9 28 33 36 37 43 61
7	12 17 21 27 45 49 54 58
8	1 5 11 29 33 38 42 63
9	3 21 25 28 30 34 55 58

10	5 9 12 14 18 39 42 52
11	2 20 23 26 36 58 61 63
12	4 7 10 42 45 47 49 51
13	26 29 31 33 35 54 55 59
14	10 13 15 17 19 38 39 43
15	1 3 22 23 27 28 59 62
16	14 15 19 20 51 54 58 60

7.(5 points) Problem 8 on page 93 in textbook.
DES weak keys are keys that consist either of all 0's or 1's or half 0's and half 1's. The 16 subkeys generated by DES are all equal, so the sequence K1,K2,...,K16 is the same as sequence K16, … K2,K1. As a result, the encryption operation is the same as the decryption operation.

8. (5 points) Problem 9 on page 94 in textbook.
Referencing Q7, The DES semi-weak keys are keys that generate only two switched around subkeys. Decryption is the same as encryption if the key schedule reversed, namely using a semi-weak key, encryption is equivalent to decryption using its complementary pair.

9. (5 points) Problem 12 on page 94 in textbook.

b1⊕82⊕85⊕9d =2b;
64⊕e5⊕10⊕45 =d4;
77⊕1a⊕42⊕f1 =de;
e0⊕31⊕63⊕1f =ad.

10. (5 points) Problem 1 on page 114 in textbook.
By applying Ex(), OFB pad sequence is Ex(IV), Ex(Ex (IV)), Ex(Ex(Ex (IV))), …[1 pt]
In Q7 we know that a weak DES key is its own inverse, so Ex(Ex (IV)) = IV. [3 pts]
The pseudo-random block stream generated by 64-bit OFB is Ex(IV), IV, Ex(IV), IV, · · · · [1 pt]

11. (5 points) Problem 5 on page 114 in textbook.

After encryption by using EEE with CBC on the inside by three times. A modification to ciphertext block n propagates to plaintext blocks n through n+3.

12. (10 points) Problem 6 on page 114 in textbook.

This will work. [5 pts]

If all blocks of plaintext are same, it will produce identical ciphertext. [5 pts]

13. (5 points) Describe at least one attack against this scheme.

One possible solution is as follows:

Let define the 96-random pad as k_{0}, on which Bob and Alice agreed upon before the system initialization. Let F: {0,1}^{96}->{0,1}^{96} is a public one-way function (e.g. derived from SHA-1). Further, encryption and decryption are performed with XOR operation. Last, (P_{j}-C_{j}) corresponds j'th (plaintext-ciphertext) pair associated with j'th transaction.

Assume that Alice and Bob performs their transaction as follows:

a) For each transaction j, Alice updates the one time key as k_{j+1}=F(k_{j}), and deletes k_{j}.

b) Alice encrypts P_{j+1} as C_{j+1}=P_{j+1} XOR k_{j+1}.

c) Bob can decrypt C_{j+1} by following the similar procedure that Alice used.

In this case, assume that the adversary obtained the plaintext associated with transaction x. The adversary then can obtain the secret key of this transaction as: k_{x}=P_{x} XOR C_{x}, where C_{x} can be observed over communication line simply.

After this point, for each transaction (j>=x), the adversary can compute the corresponding key and decrypt the corresponding ciphertext. Therefore, the scheme is broken starting from transaction x.

Note: In this question, answers mentioning simple XOR operation without making explicit and clear assumption list will not be given full credit.