EECE 412, Fall 2007

Quiz #2

Your Family name: _____

Your Given name: _____

Your student ID: _____

Name of your left neighbor: _____

Name of your right neighbor: _____

#	Points	Out of
1		2
2		2
3		2
4		4
5		3
6		4
7		6
TOTAL		23

Questions:

1.

(a) What did Ed Helms mean when he said on the Daily Show with Jon Stewart that "today e-voting systems support a robust cryptography architecture using DES key in CBC mode with a random initialization vector"? Spell out all the acronyms in your answer.

Answer: He meant that e-voting systems use Data Encryption Standard in Cipher Block Chaining mode of operation, which is implemented to use random initialization vector.

(b) Given that the show was aired in 2004, what is the obvious weakness of the use of crypto in Debolt systems, as described by Ed Helms, and how would you repair that weakness today?

Answer: DES is known for its key (56 bit) being too short. As a result, DES is vulnerable to brute force search attacks that can be accomplished in several days on modern commodity PCs. The simplest way to repair the weakness today is to replace DES with the Advanced Encryption Standard (AES) (and use 128-bit or longer key).

2. **Which of the following backend database servers are vulnerable to SQL injection attacks. Mark all applicable:**
   - ☐ Microsft SQL Server
   - ☐ Sybase
   - ☐ Oracle
   - ☐ MySQL
   - ☐ DB2

   If you want to, explain the rationale for your answer:

Answer: Whether a web application system is vulnerable to an SQL injection attack depends not on the vulnerability of the back-end database, but on the vulnerability of the front-end. With a vulnerable front-end, any DBMS that supports SQL can fall victim of the SQL injection attack. (Note: Explanation for this problem is optional. Marking all the databases as vulnerable to the SQL injection attack is sufficient for a correct answer.)

3. **What are the two words that computer security is all about? Choose one option.**
   - ☐ **Deterrence & protection**
   - ☐ **Risk avoidance**
   - ☐ **Diffusion & confusion**
   - ☐ **Risk transfer**
   - ☐ **Confidentiality & accountability**
   - ☐ **Risk management**
   - ☐ **Risk reduction**

4. The formula for counter mode encryption is $C_i = P_i \oplus E(IV + i, K)$. Suppose instead we use the formula $C_i = P_i \oplus E(K + i, IV)$. Is this secure? If so, why? If not, describe an attack.

Answer: It's not secure. Since IV is sent in open, the attacker can always compute K from C_0 and IV. After that, the attacker can compute C_1, C_2, etc.

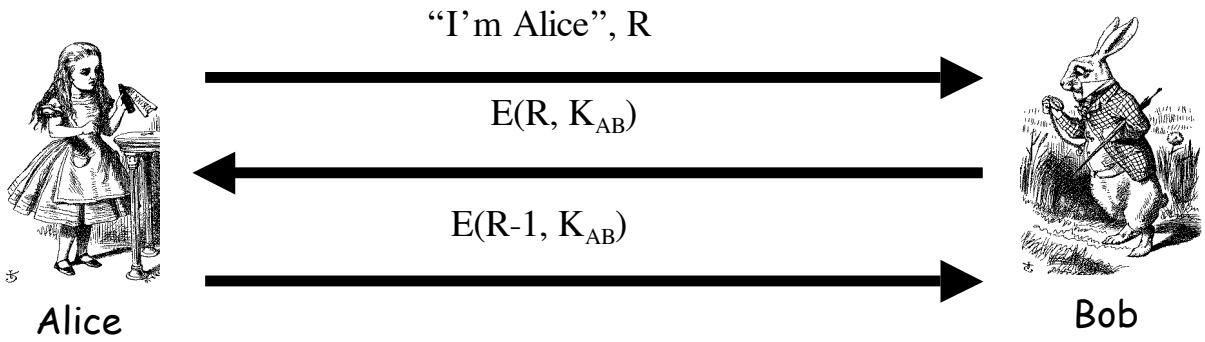
5. A digital signature provides for data integrity and a MAC provides for data integrity. A digital signature also provides for non-repudiation, while MAC does not. Why not? Explain:

Answer: MAC requires shared key. Because the key is shared, Alice can always claim that it was Bob, not her, who computed the MAC. With digital signatures, Alice has to use her private key—which only she is supposed to know—to compute a digital signature.

6. Suppose that a secure cryptographic has function generates hash values that are *n* bits in length. How could an attacker break this hash function (i.e., find two inputs that create a collision) and what is the expected work factor?

Answer: An exhaustive search to break a hash function consists of hashing enough messages so that a collision is found. By the birthday problem, we would need to compute about $2^{n/2}$ hashes (saving and comparing all hash values) before we expect to find a collision.

7. Consider the following mutual authentication protocol, where K_{AB} is a shared symmetric key. Give two different attacks that Trudy can use to convince Bob that she is Alice. Hint: Man-in-the-middle attack does not work.



Answer:
Attack #1: Trudy records and replays to Bob messages 1 & 3. Bob will always reply with message #2.

Attack #2: Trudy opens one connection to Bob and sends first message and receives second message. After that, she opens another connection to Bob and sends R-1 to bob in the first message. Then she uses Bob's response to complete the first connection, and lets the second one to time out.