# EECE 412, Fall 2008

## 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 | | 3 |
| 3 | | 2 |
| 4 | | 3 |
| 5 | | 3 |
| 6 | | 4 |
| 7 | | 6 |
| Bonus | | 5 |
| TOTAL | | 23 |

---

Questions:

1. **Fun with Debolt**

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

Answer: It's not secure. Since IV is sent in open and I is known, the attacker can easily recover $E(P_i, K)$ for each I, which allows the attacker to mount all the attacks that they can do on ECB.

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

Answer: HMAC 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.

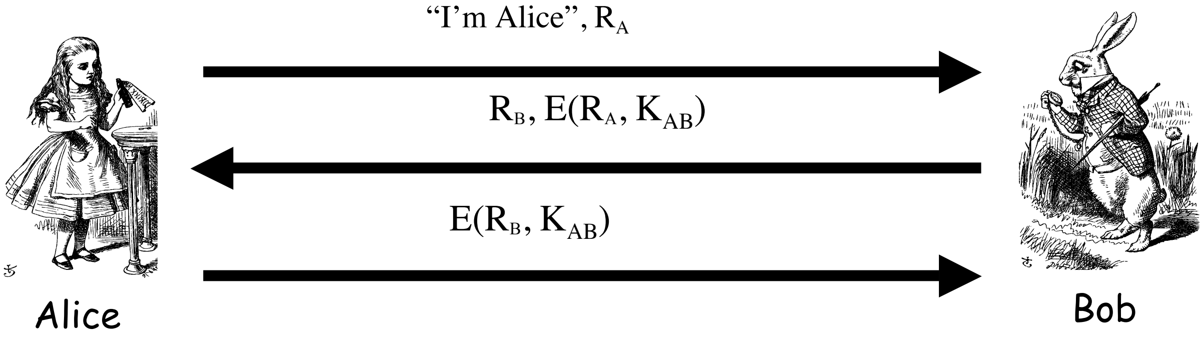
**4. A stream cipher can be viewed as a generalization of one-time pad. Recall that the one-time pad is provably secure. Why can't we prove that a stream cipher is secure using the same argument that was used for the one-time pad?**

Answer: Since a relatively small number of keys generate a much larger number of possible keystreams, the keystreams are not chosen uniformly at random.

**5. Explain the differences and similarities among the following three properties of key establishment protocols and give examples of how each property can be achieved: *backward secrecy*, *forward secrecy*, and *perfect forward secrecy*. For example, backward secrecy can be achieved with producing next key by hashing the previous key.**

Answer: Commonly achieved through using hash of the previous key as the value of next key, Backward secrecy is about keeping previous key secret even if the attacker learns next key. Whereas, forward secrecy is about keeping next key secret even if the attacker knows previous key. Forward secrecy can be achieved by hashing together previous key, along with ALL the messages exchanged during the session. Perfect forward secrecy (PFS) guarantees forward secrecy even if the attacker observed all the messages in the session. PFS can be achieved with Diffie-Hellman key exchange.

**6. Consider the following mutual authentication protocol, where $K_{AB}$ is a shared symmetric key.**



“I’m Alice”, $R_A$

$R_B$, $E(R_A, K_{AB})$

$E(R_B, K_{AB})$

Alice

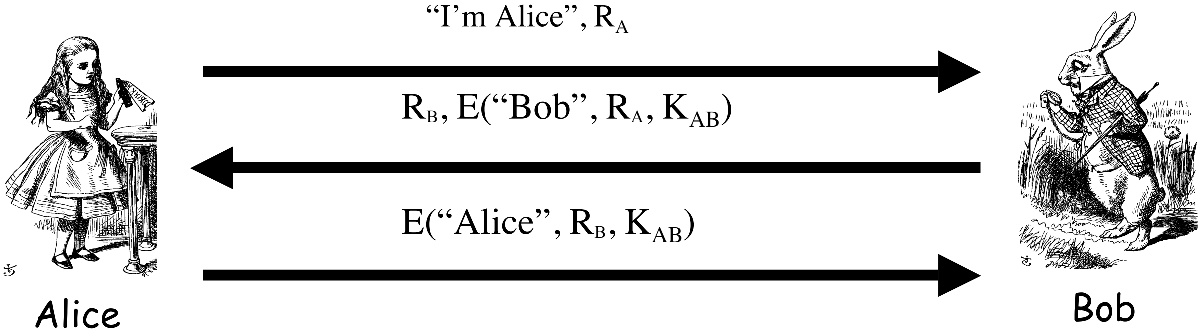
Bob

Show that Trudy can attack the protocol to convince Bob that she is Alice.

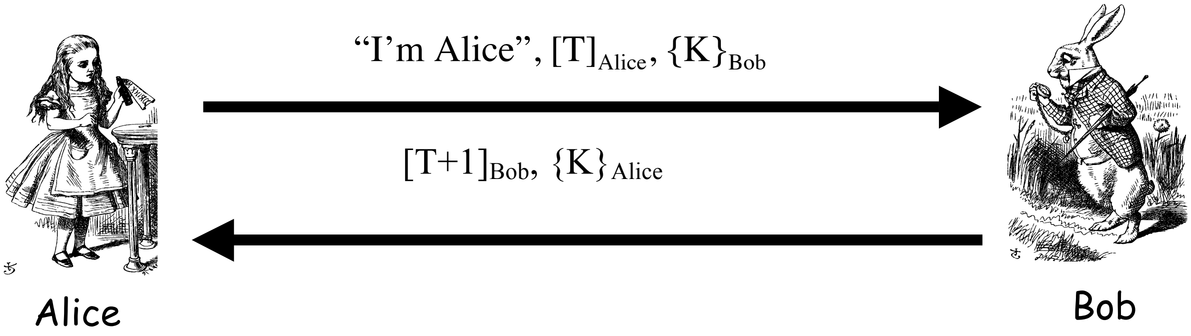
Answer: Trudy can run two concurrent authentication sessions with Bob and challenge Bob with $R_B$ in the second session, then re-use $E(R_B, K_{AB})$, which she received from Bob in the second session, in the first session.

7. **Modify the protocol from the previous problem to prevent the attack you identified.**

Answer:


"I'm Alice", $R_A$
$R_B$, $E(\text{"Bob"}, R_A, K_{AB})$
$E(\text{"Alice"}, R_B, K_{AB})$
Alice
Bob

**8. Bonus question: The following two-message protocol is designed for mutual authentication and to establish a shared symmetric key K. Here T is a timestamp, $\{M\}_A$ is a message M encrypted with the public key of A, and $[M]_A$ is a digital signature of M by the private key of A. The protocol is insecure. Illustrate a successful attack on it.**


"I'm Alice", $[T]_{Alice}$, $\{K\}_{Bob}$
$[T+1]_{Bob}$, $\{K\}_{Alice}$
Alice
Bob

Answer:

a. If Trudy acts within the clock skew, she can send $\{K\}_{Bob}$ to Bob (as herself) and Bob will respond with $\{K\}_{Trudy}$ and Trudy will then know K, which only Alice and Bob should know.

b. Trudy can perform MITM attack by replacing $[T]_{Alice}$ with $[T]_{Trudy}$ in the first message, and then receiving $\{K\}_{Trudy}$ in the second message from Bob. At this point, Trudy has K, which she can encrypt into $\{K\}_{Alice}$ and send it to Alice. At this point, Trudy becomes MITM.