**CS5285**: **Information Security for eCommerce** Autumn, 2024
Problem Set 2 (Due Date: Dec 3 14:00) Total: 102 points
Submit Q1–Q7 electronic copy (via Canvas).
Submit Q8 as instructed in the question.
No late submissions or any corrections after the deadline will be accepted.

**Questions**:

1. **Password File** (2-2-2-2 points):

   (a) In a system, each user has an entry in the system's password file: (y; s) where y is computed as follows and s is a salt.
   i. $y = H(s; password) \oplus password$
   ii. $y = H(s) \oplus H(password)$
   iii. $y = E_s(H(password))$ where E is AES algorithm
   iv. $y = MAC_{password}(s)$ where MAC is CBC-MAC constructed with AES
   List which of the methods above for computing y are effectively secured by the salt against precomputed dictionary attack. Assume that s is adequately long and random.

2. **TLS** (2-8 points): In TLS you can specify different ciphersuites for communication.

   (a) How many ciphersuites are there in the latest specification TLS 1.3

   (b) For the following mode how is a data message encrypted and session keys generated?

   `TLS_AES_128_CCM_SHA256`

3. **Digital Certificates** (2-2-2-2):

   (a) Find out who issued the certificate for `https://mail.google.com` and how long the certificate will be valid.

   (b) Find out or estimate how many certificates (approximately, no need to count them explicitly) your browser contains.

   (c) What is the significance of a CA certificate being contained in the browser?

   (d) The identity of the certificate for the question above is a DNS hostname. Certificates can also be used for signing and encrypting email. For a certificate used for email, what identifier would be used as the identity in the certificate?

4. **Security Services - Web Security** (10 points):
   We are currently using Zoom (so are a lot of other people). Please provide a short explanation of what"zoombombing" is. Your answer should mention at least two main security services that are failing, as well as the main technical vulnerability that is allowing this to happen. Conclude by providing some mechanisms for mitigating issues for each of the security services you mentioned.

5. **Key agreement/IKE** (10-5-10 points):

   (a) Consider the following key exchange protocol which is similar to IKE Phase 1 Aggressive Mode. $p$ is a large prime number and $g$ is a generator of $Z_p^*$.

   1. $A \rightarrow B : g^a \bmod p,\ \{\text{“}Alice\text{”}\}_{Bob},\ \{R_A\}_{Bob}$
   2. $A \leftarrow B : g^b \bmod p,\ \{\text{“}Bob\text{”}\}_{Alice},\ \{R_B\}_{Alice},\ \text{proof}_B$
   3. $A \rightarrow B : \text{proof}_A$

   where

   $$\text{proof}_A = h(g^{ab} \bmod p,\ g^a \bmod p,\ g^b \bmod p, \text{“}Alice\text{”})$$
   $$\text{proof}_B = h(g^{ab} \bmod p,\ g^b \bmod p,\ g^a \bmod p, \text{“}Bob\text{”})$$
   $$K = h(g^{ab} \bmod p)$$

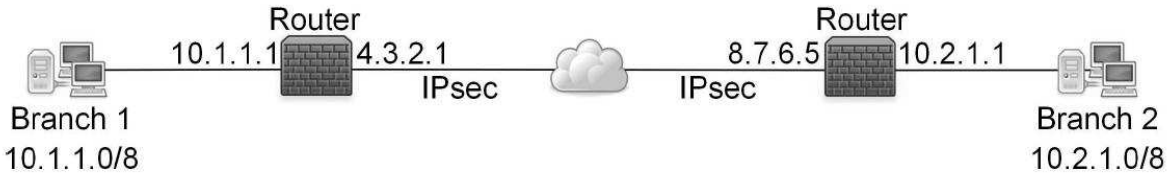
   i) First explain if the protocol authenticates $A$ and $B$, and achieves secure key agreement (discuss key control and key authentication). $\{m\}_X$ denotes a message $m$ encrypted with public key of $x$.
   ii) Modify the protocol so that $R_A$ and $R_B$ can be eliminated but the protocol can mutually authenticate $A$ and $B$. In your modification, no additional protocol message, secret keys or signature can be used.

   (b) Consider the following simplified IKE Phase 1 in Aggressive Mode.

   $$A \rightarrow B :\ \text{“}Alice\text{”}, \text{“}Bob\text{”}, g^a \bmod p$$
   $$A \leftarrow B :\ \text{“}Bob\text{”}, \text{“}Alice\text{”}, g^b \bmod p, [g^a \bmod p]_B$$
   $$A \rightarrow B :\ \text{“}Alice\text{”}, \text{“}Bob\text{”}, [g^b \bmod p, g^a \bmod p]_A$$

   $[X]_A$ denotes a signature on message $X$ generated by $A$. The session key established between $A$ and $B$ is $g^{ab} \bmod p$. Show that this simplified version is insecure (allows attacker to establish a key with one of the participants while pretending to be the other participant) . Hint: consider that this IPSec system has multiple users.

6. **IPSec** (10 points): Imagine two branches of a corporate network are connected through the Internet. Specifically, each of the two branches has a router facing the Internet, communicating with the router of the other branch over IPsec (ESP in tunnel mode).




The network is setup such that two nodes from the two branches can communicate transparently. Imagine node 10.1.1.5 from branch 1 is sending a packet to node 10.2.1.6 from branch 2. Describe in detail the steps of how the packet travels between the two nodes and how it is encapsulated and decapsulated on the way.

7. **Password Files** (4-4-4-4 points): Use hashcat to execute a brute-force search to recover the passwords from the three files provided (**give some screenshots to prove that you did calculate the answer – no screenshot no mark**): file1.txt, file2.txt, file3.txt
You can download hashcat here: http://hashcat.net/hashcat/
It is a command line program (no GUI), so you if you would like to run it in Windows you need to do so from the command prompt.

   The new version of hashcat you need to specify the processor option. You can use the -I option to see compatible processors, then use -D option to specify using CPU (not GPU). Hashcat sometimes likes to provide false negatives but it works in almost all cases. Try it on a different machine (suggest a Windows machine), or with different/no -D option before thinking it does not work.

   General instructions for using hashcat
   `http://hashcat.net/wiki/doku.php?id=hashcat`

   Details on brute force attack here:
   `http://hashcat.net/wiki/doku.php?id=mask_attack#example1`
   Doing this optimally the search for File1 and File 2 should be not more than few minutes.

   Information about the password files

   - File1 and File2 has six 5-character passwords (from the set A-Z,a-z,0-9). MD5 is the hash function used.
   - File3 is the same but has six 6-character passwords
   - File1 uses the same salt for all entries (all the salt values are the same, equal to 0 so the stored value is h(0,pwd))
   - File2 uses a 8-bit salt (the stored value is h(s,pwd))
   - File3 uses a 8-salt for all entries (same format as file2), but the password is now 6 characters long.

While hashcat is running you can press [s]tatus and it will show you a progress update.

(a) Recover the passwords in file1 and file 2

(b) Recover the passwords in file 3

(c) How much longer should it take to recover file2 compared to file1. Did the result support the theory?

(d) How much longer did it take to find the 6 character passwords?

8. **PGP eMail** (5-5-5 points): In this problem we will ask you to familiarize yourself with PGP and ultimately send an encrypted and signed message using PGP to the tutor (see below for more details).
Unless you are already familiar with using PGP, we suggest you use Thunderbird (a free email client) to accomplish this. The setup of this will require the following steps:

- Download and install Thunderbird
- You should have version 78 (or later)
- Thunderbird from 78 has PGP support, no need for plugin

You can see information about setting up and sending email here `https://support.mozilla.org/en-US/kb/openpgp-thunderbird-howto-and-faq`. Once you have successfully setup the required software, please complete the following assignments:

(a) Create your own PGP keypair.

(b) Import the course public PGP key. You can find the key tsgexercise_cert.asc on Canvas.

(c) Send an email to email address tsgexercise@gmail.com, encrypted with the course public key and signed with your newly created key. The subject of the email should include "CS5285 PS2 EncryptedMail XXXXXXXX" where "XXXXXXXX" is your 8-digit student id. Make sure you include your public key as an attachment in the message.

*NOTE*: The points for tasks (a) and (b) will be awarded when completing task (c), so make sure to complete task (c).