UNIVERSITY OF MARYLAND
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

ENEE 457
Computer Systems Security
Instructor: Charalampos Papamanthou

Homework 3

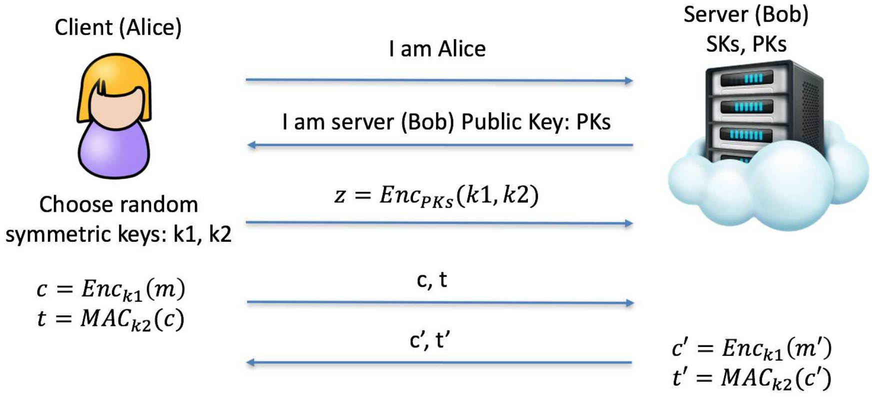
Out: 10/22/18 Due: 10/29/16 11:59pm

Instructions

1. Strictly adhere to the University of Maryland Code of Academic Integrity.
2. Submit your solutions as a pdf document at Canvas. Include your full name in the solutions document. Name the solutions document as x-hw3.pdf, where x is your last name.

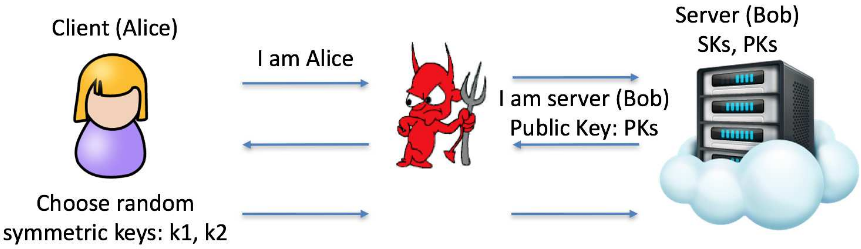
Problem 1 (50 points) Alice wants to send a message m to the server, and the server wants to respond with a message m'. The communication should be confidential, and no man-in-the-middle should be able to tamper with the communication.

The server chooses a public-private key pair (PK_s, SK_s) and keeps SK_s secret.
Alice and the server then communicate as below:



1. Write down the algorithm the server uses to recover m.
2. 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.



3. 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 $z = Enc_{PKs}(k1, k2)$ from Alice, the server sends Alice a tag t which is computed as

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

   Does this prevent the man-in-the-middle attack you came up with in Part 2?
   Explain why or why not.

Problem 2 (50 points)

1. In order to verify the authenticity of SSL certificates, a certificate authority (CA) is used. Sometimes, that CA's certificate may be verified as authentic by another CA. In general, this forms a chain of certificates, each being verified by the one before it in the chain, all the way up to a "root certificate", which is a certificate installed by default in your OS or browser. Explain why, without knowledge of any certificates ahead of time, no system can be built that can allow a client to verify the authenticity of any site's certificate (that is, to verify that a given certificate is owned by a given party). Use the website `https://www.digicert.com/help/` to identify in practice the chain of certificates and the signature algorithms for three widely used web servers (e.g. www.google.com etc.). Please indicate your observations.
2. (a) In TLS, what security properties are achieved, and what components of the TLS protocol enable these properties?
   (b) Recall that in practice, TLS as used on the web typically only provides one-way authentication – that is, when communicating securely over the web, only the server is required to authenticate themselves, and not the client. Why is TLS usually used this way?
   (c) How might a web server authenticate a user? (if the user is not authenticated by TLS)
3. In class, we talked about the Tor protocol which is based on *onion routing*. Onion routing works as follows: When user A wants to send message x to B that has public key pk_B, A downloads the public keys $pk_1, pk_2, \ldots, pk_m$ of m intermediate stations $1, 2, 3, \ldots, m$ and uses these keys to encrypt message x. How does A use onion routing to encrypt message x? How does B decrypt this message? State one security property that onion routing aims to provide to user A. How does Tor protocol improve the performance of onion routing? However, several attacks have been deployed to compromise Tor's anonymity. Read the paper on Routing Attacks on privacy in Tor (`https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-sun.pdf`) and describe one of the attacks mentioned in this paper.