Homework 3

Due: November 8, 2019 at 11:59pm **Points:** 100

Questions

Remember to justify your answers.

1. (*32 points*) Consider the Otway-Rees protocol. Assume that each enciphered message is simply the bits corresponding to the components of the message concatenated together. So, for example, in the first message, one must know the names "Alice" and "Bob", and the length of the random numbers r_1 and n, to be able to parse the portion of the first message that is enciphered with k_{Alice}. The separate parts of the enciphered message have no indicators; the recipient is expected to determine them.
   (a) Consider Alice when all 4 steps of the protocol have been completed. How does Alice know that steps 2 and 3 have taken place?
   (b) Massicotte asks us to assume that an adversary Edgar is impersonating Bob, and has sufficient control over the exchange so that he receives the messages intended for Bob. Bob never sees them. What components of the protocol does Edgar know — that is, does he know r_1, r_2, n, or $k_{session}$, or the names of "Alice" and "Bob"? How?
   (c) Given this, in step 4 of the protocol, how might Edgar provide Alice with a session key that he knows?
   (d) How might someone fix this?

2. (*20 points*) The section on public key cryptosystems discussed nonrepudiation of origin in the context of public key cryptosystems. Consider a secret key system (in which a shared key is used). Bob has a message that he claims came from Alice, and to prove it he shows both the cleartext message and the ciphertext message. The ciphertext corresponds to the plaintext enciphered under the secret key that Alice and Bob share. Explain why this does *not* satisfy the requirements of nonrepudiation of origin. How might you modify a classical cryptosystem to provide nonrepudiation?

3. (*30 points*) Consider the set of rights $\{r, w, x, a, l, m, o\}$.
   (a) Using the syntax in Section 2.3, write a command *delete_all_rights*(p, q, o). This command causes p to delete all rights the subject q has over an object o.
   (b) Modify your command so that the deletion can occur only if p has *modify* (m) rights over o.
   (c) Modify your command so that the deletion can occur only if p has *modify* (m) rights over o and q does not have *own* (o) rights over o.

4. (*18 points*) Why should a time-based authentication system invalidate the current password on a successful authentication?

Extra Credit

E1. (*30 points*) The Tor protocol, as discussed in class, is intended to prevent an attacker who can observe a fraction of the links involved from tracing a message. Consider the situation in which an attacker can observe the *entire* Tor network, including entry and exit relays.
   (a) If only one client uses that Tor network to contact a server, how can the attacker determine the source and destination of the circuit?
   (b) Devise a way to prevent this. You may assume multiple clients have Tor proxies, but *not* that more than one client is connecting to a server. Why do you think Tor does not use your method?