We now have all of the tools in place to start building secure protocols. The “simple” Internet protocols described in class are a good start, but there are many additional features that one might like to have in such protocols.

1. Show how to modify the basic RSA-based Internet protocol described in class to employ Diffie-Hellman key exchange rather than RSA. Do this without adding any additional rounds of message passing.

2. Describe how to modify the basic Internet protocol described in class to allow a dropped or stale session to be re-established without having to pay the expense of public key operations to exchange a new session key. What information should or should not be provided for re-establishment?

3. Services often have “premium” content that they are willing to deliver over the Internet for a fee. Examples include audio files, music videos, and full length movies. Using standard protocols, these data would be re-encrypted for each user to whom they are sent, but this re-encryption may prove to be prohibitively expensive for large data sets. Design an Internet protocol that enables services to transmit valuable data securely without having to individually encrypt the data for each customer.

4. Suppose that a virtual private network (VPN) is to be established across the Internet. Describe a protocol that allows a client to “log-in” to a server securely and maintain a secure connection under the assumption that the client has a password (or preferably a strong key) established with the server. In such a case where there is a pre-existing relationship, can the VPN be established with fewer rounds of message passing than for the basic Internet protocol that assumes no pre-existing relationship? Explain.

5. Describe how to establish a VPN when the client does not have a shared password with the server but instead has a public key that is certified by an entity trusted by the server.