Homework 5

Due: December 6, 2023 **Points:** 100

1. (*25 points*) Consider the statement

   if $(x = 1)$ **and** $(y = 1)$ **then** $z := 1$

   where x and y can each be 0 or 1, with both equally likely and z is initially 0. Compute the conditional entropies $H(x|z')$ and $H(y|z')$, where z' is the value of z after the statement is executed.

2. (*24 points*) Cisco routers use a "TCP intercept mode" to prevent network flooding. When the router sees a SYN packet coming from the Internet, it does not forward the packet to its destination. Instead, the router responds, and tries to establish the connection. If the SYN packet is part of a legitimate handshake and a connection is established, the router establishes a connection with the intended destination and merges the two connections. If the SYN packet is part of an attack handshake, the router never sees a following ACK packet, and times the pending connection out without ever contacting the putative destination. The router uses short timeouts to ensure it does not run out of space for pending connections.

   (a) Why does the router not save time by opening a connection to the destination host before the pending connection completes its three-way handshake?

   (b) The router is protecting a target from being flooded. Is the router itself vulnerable to a flooding attack? If not, why not, and why won't the same property make the target immune? If so, does the attack on the router differ from the attack on the target?

3. (*51 points*) Consider a scheme that allows a recipient to reply to a message from a chain of Cypherpunk remailers. Assume that encipherment is used throughout the chain, and the recipient does not know the sender.

   (a) Bob selects a chain of remailers for the return path. He creates a set of keys and enciphers them so that only the key for the current remailer is visible to that remailer. Design a technique by which he could accomplish this. Describe how he would include this data in his message.

   (b) How should Alice's mailer handle the processing of the return address information?

   (c) When Bob receives the reply, what does it contain? How can he obtain the cleartext reply?