9.

Alice can apply the hash function h on the shared secret key S for n times to generate n one-time pads $p_1, p_2, ..., p_n$. For example, if $n = 3$; then

$$p_3 = h(S),$$
$$p_2 = h(h(S)),$$
$$\text{and} \quad p_1 = h(h(h(S)).$$

Alice can use p_1, p_2, and p_3 as one-time pads to encrypt the first, second, and third packet.

10. Hint: please think from using Hash functions.

11. (5173 Only)

(a) The sender first sends a message with K_0, T_1, and the duration of each interval to all receivers, signed with its private key. Each receiver then authenticates all the items by verifying the signature.

For each message transmitted in time interval I_i, the sender uses K_i to generate a MAC on the message and transmits the message, the MAC, and K_{i-T}. For each message received during time interval I_i, a receiver buffers it until T time intervals later when it receives K_i in time interval $i+T$. The receiver then uses K_i to verify the MAC.

(b) The earliest time for Ki to be disclosed is $T_{i+1} + T$. Thus, the receiver only needs to check if $t < T_{i+T} - \Delta$.