Exercise 5 Feedback

5(c): In this exercise, you are asked to address the Coin Flipping Over the Telephone problem.

(i) Assuming that there is only one car, and Alice and Bob have to decide who can have this car (only one of them can have it, i.e. they cannot share it). Alice and Bob cannot see each other, and they do not trust each other. So they have decided to make a decision by flipping a coin over the telephone. Design a protocol to support this using a hash function.

(ii) Identify any factors that you should consider to ensure the security of this protocol.

Answer to 5(c) – (i) (flip a coin over the telephone):
Alice and Bob agree that if the outcome is 1 then Bob takes the car, if it is 0 then the car goes to Alice; Alice and Bob also agree that the first bit in the random number, r, is used to indicate the result of coin flipping.

Here are the protocol steps:

1. Alice generates a random number, *r* (the first bit *b*: 0=heads, 1=tails).
2. Alice computes commitment, x=hash(r).
3. Alice sends *x* to Bob and also asks Bob: heads or tails?
4. Bob sends Alice his choice_B: ‘heads’ (or ‘tails’).
5. Alice compares *b* with choice_B: if b=choice_B, then outcome=1; if not, outcome=0.
6. Alice sends *r* and the comparison outcome to Bob.

Here, Alice makes a commitment simply by sending *x* committing to her choice so that she cannot change her mind later. Later on if Bob disagrees with the outcome, she can reveal her *r*.

Answers to 5(c) - (ii):

- ○ The random number generator used by Alice should be truly random and the random number r should be sufficiently long. Otherwise, Bob could guess r, putting Alice in a disadvantaged position.
- ○ The hash function used should be secure, i.e. one-way and collision resistant. Otherwise, if it is not one-way, Bob could benefit; if it is not collision resistant, Alice could benefit.