CSE 484 In-Class Worksheet #17 – Autumn 2019

Name: _____ UWNetID: _____ Date: _____

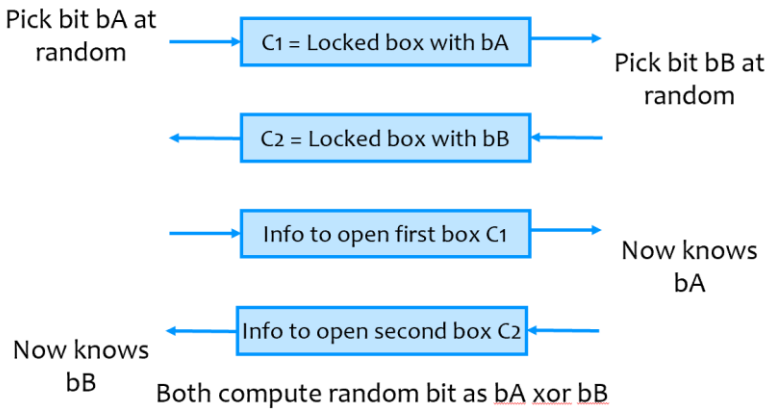
Email address: _____

Partner names for this activity: _____

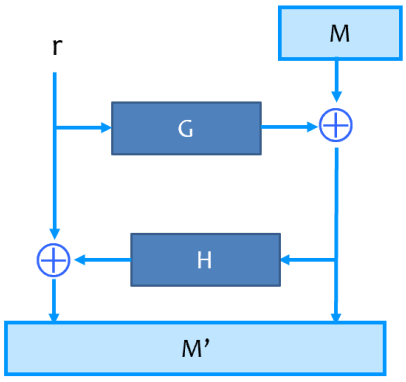
Will you want to pick up your worksheet later? Circle one: Yes / No

Q1: Alice and Bob are both cryptographers, and they are talking on the phone. They want to randomly flip a coin. If they were together, in person, they would flip a real coin and see if it was Heads or Tails. But they are not together, in person, and they don't trust each other enough to have one of them flip a coin and tell the other person the answer.

Using the techniques we've discussed so far in class, how can Alice and Bob effectively flip a random coin together, over the phone, such that they both trust the answer even though they don't trust each other?



Q2: Consider a message encrypted with RSA-OAEP. Given C, how does the recipient recover M? Recall that (e,n) is the public key and (d,n) is the private key, and the RSA decryption primitive is $M'=C^d \bmod n$.



$C = (M')^e \bmod n$