Date: 10 Nov 2023

Total Marks: 10

CS6160: Cryptology

Quiz 3

Time: 50 min

1. Describe hybrid encryption using RSA.
2. Describe the Diffie-Hellman key exchange scheme.
3. Consider the following method of coin tossing. A trusted party T generates a secret key (p, g, x), where $g \in \mathbb{Z}_p^*$ and publishes the public key (p, g, h) where $h = g^x$. For Alice and Bob to toss a coin, Alice picks a random y and sends (g^y, h^{y+b}) to both T and Bob. Then Bob guesses a value b', picks a random y' and sends $(g^{y'}, h^{y'+b'})$ to T. Bob wins if $b' = b$.

   (a) How does T compute the value of b?

   (b) Can Alice or Bob cheat and win the toss in the above scheme?
4. Consider the following key-exchange protocol:
   - Alice chooses uniform $k, r \in \{0,1\}^n$ and sends $s = k \oplus r$ to Bob.
   - Bob chooses uniform $t \in \{0,1\}^n$ and sends $u = s \oplus t$ to Allice.
   - Alice computes $w = u \oplus r$ and sends w to Bob.
   - The common key is chosen as k by Alice.

   How does Bob compute the common key? Is this scheme secure?
5. Let f be a trapdoor permutation and h be a hard-core predicate for f. Suggest a method using f and h to encrypt a message in $M = \{0,1\}$ securely.