This quiz concerns pseudorandomness.

1. Alice and Bob discuss the practicality of private-key encryption schemes. Bob says that there is not much difference between the cost of the one-time pad, private-key encryption with pseudorandom generator, and private-key encryption with pseudorandom function, in practice. He says: “all three need roughly the same amount of randomness to encrypt a message m of length n.”

   (a) one-time-pad, \(c = m \oplus k\): needs \(|k| = n\) random bits.
   (b) encryption with PRG, \(c = G(k) \oplus m\): needs \(|k| = n/\ell\) random bits, where \(\ell\) the expansion factor of \(G\) (e.g., for an expansion factor of 2: \(|k| = n/2\)).
   (c) encryption with PRF, \(c = \langle r, F_k(r) \oplus m \rangle\): needs \(|k| \approx n\) random bits

Alice says that Bob is missing the point because “it is all about sharing”. What does she mean?

2. We discussed four modes of operations of block ciphers: ECB, CBC, OFB and CTR. What do these abbreviations stand for:

   (a) ECB ........................................
   (b) CBC ........................................
   (c) OFB ........................................
   (d) CTR ........................................

3. Some of these modes offer stronger protection than others. Use the following abbreviations to describe their strengths/weaknesses: D = deterministic, Pr = probabilistic, I = indistinguishable encryptions in the presence of an eavesdropper, CPA = CPA-secure, Pa = parallelizable. Assume that the block cipher is a pseudorandom permutation.

   (a) ECB: ........................................
   (b) CBC: ........................................
   (c) OFB: ........................................
   (d) CTR: ........................................