Problem Set 2 – Dew Thu, 11 Apr 2024

Definition: **dew**: _adjective_. 1. An assignment is _dew_ on a certain date if it can be turned on that date, cannot be turned in at a later date, but and need not be turned in at all.

**Problem 5.** Alice shuffles a deck of 52 cards and deals it out to herself and Bob so that each gets half of the cards. Alice now wants to send a secret message $M$ to Bob. Eavesdropper Eve is watching and sees the transmissions.

**Part A.** Suppose Alice’s message $M \in \{0, 1\}^{48}$ is a string of 48 bits. Describe how Alice can communicate $M$ to Bob in a way that achieves perfect privacy.

**Part B.** Now suppose Alice’s message $M \in \{0, 1\}^{49}$ is 49 bits. Prove that there does not exist a protocol that allows Alice to communicate $M$ to Bob in a way that achieves perfect privacy.

**Problem 6.** Alice wants to deal a one-byte secret to shareholders 1, 2, and 3 such that any two of them can reconstruct the secret, but no single player knows anything about it. She decides to use Shamir secret sharing over the smallest prime field that will work for this situation. She represents bytes and points in this field in the natural way. Players 1 and 2 end up with shares of $209 = 0xD1$ and $34 = 0x22$, respectively. What secret was shared? What was player 3’s share?