Problem Set 2 – Due Fri, 25 Jan 2019 at 12 pm

Instructions: Same instructions as before, but this time it is due on a Friday. Note that you will not have benefit of discussion sections, due to the holiday on Monday, 21 Jan.

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?

Problem 7. Fix relatively prime numbers a, b ($a, b \geq 2$). Bob proposes the following PRG g to map $(a+b)$-bit strings to ab-bit strings: $g(\boldsymbol{u} \parallel \boldsymbol{v}) = \boldsymbol{u}^b \oplus \boldsymbol{v}^a$ where $|\boldsymbol{u}| = a$ and $|\boldsymbol{v}| = b$. (As usual, exponential notation with strings means repeated concatenation: $\boldsymbol{x}^0 = \varepsilon$ and $\boldsymbol{x}^n = \boldsymbol{x} \parallel \boldsymbol{x}^{n-1}$ when $n \geq 1$.) Show that g is a terrible PRG: describe an efficient adversary D (for "distinguisher") that gets high advantage in distinguishing $g(\boldsymbol{x})$-outputs (for uniformly random $(a+b)$-bit $\boldsymbol{x}$) from a uniformly random ab-bit string $\boldsymbol{c}$. Compute D's advantage when, say, $a = 50$, $b = 51$. *Hint: what you know about linear algebra works out the same way in* $\mathbb{F}_2$.