Problem Set 2 — Due Wednesday, April 13, 2011

Problem 5. Here is an elegant physical-world solution to the dating problem. Assume that Alice and Bob have access to five cards, three identical hearts (♥) and two identical clubs (♣). Alice and Bob each get one heart and one club. The remaining heart is put on the table face-down. Next Alice and Bob place their cards on the table, also turned over. Alice places her two cards on the left of the heart that is already on the table, and Bob places his two cards to the right of the turned-over heart. The order in which Alice and Bob put their two cards depends on their input as follows. If Alice’s input bit is \( a = 1 \) (she wants to go on a date with Bob) then she places her cards as \( \Box♥♣ \) where the box (\( \Box \)) denotes the overturned heart. Otherwise (\( a = 0 \)) she places her cards as \( ♥♣\Box \). Bob, on the other hand, places his card in the opposite order: if he wants to go on a date with Alice (\( b = 1 \)) then he places his cards as \( 2♥♣ \); otherwise (\( b = 0 \)), he places his cards as \( 2♣♥ \). When all cards have been placed on the table, the cards are piled up. Alice and Bob then each take turns to privately cut the pile of cards once each, so that the other person does not see how the cut is made. Finally, all cards are turned over. If there are three hearts in a row, then they go on a date. Otherwise they do not.

Convincingly argue that the protocol secure computes \( f(a, b) = a \land b \).

Problem 6.

Part A. Alice would like to private send a bit \( a \in \{0, 1\} \) to Bob. An adversary should get \textit{no} information about \( a \). Alice and Bob share a uniformly random key \( k \in \{0, 1, 2\} \). How can Alice securely send her bit to Bob?

Part B. Alice shuffles a deck of cards and deals it out to herself and Bob so that each gets half of the 52 cards. Alice now wishes to send a secret message \( M \) to Bob by saying something aloud. Eavesdropper Eve is listening in: she hears everything Alice says (but Eve can’t see the cards).

Suppose Alice’s message \( M \) is a string of 48-bits. Describe how Alice can communicate \( M \) to Bob in such a way that Eve will have \textit{no} information about what is \( M \).

Part C. Now suppose Alice’s message \( M \) is 49 bits. Explain why there exists no protocol that allows Alice to communicate \( M \) to Bob in such a way that Eve will have \textit{no} information about \( M \).

Problem 7. Do problem 1.9 from Paar and Pelzl.

Problem 8. Do problem 2.7 from Paar and Pelzl.

---

\( ^1 \)Typesetting note to those trying to learn \LaTeX: symbols \( \heartsuit, \clubsuit, \text{and} \Box \) are \texttt{\textbackslash heartsuit}, \texttt{\textbackslash clubsuit}, and \texttt{\textbackslash Box}. Add \texttt{\usepackage{amssymb,amsmath,latexsym}} to make sure to bring in such symbols.