CIS 5371 – Cryptography

Writing Exercise

Instructor: Viet Tung Hoang

1. In class, we learned about the dating problem and the 5-card trick. Prove that the trick protects the privacy of Bob.

Solution: Without loss of generality, assume that Alice's decision is "No date"; otherwise she can infer Bob's answer from the outcome. In other words, initially Alice will need to place her cards as ♡♣. Thus the initial configuration is either ♡♣♡♡♣ or ♡♣♡♣♡. We view this as Bob's secret message (that Alice may have some *a priori* knowledge), and our goal is to prove that the 5-card trick does not give her any additional information.

Recall that under the 5-card trick, Alice makes a private cut, which is a cyclic shift of the cards by $a \in \{0, 1, 2, 3, 4\}$ positions. Likewise, Bob's cut is a cyclic shift of the cards by $b \in \{0, 1, 2, 3, 4\}$ positions. Assume that Bob makes a uniformly random cut. From Alice's perspective, a is known (and she might pick a number a that she finds advantageous), but b is secret and uniformly distributed over $\{0, 1, 2, 3, 4\}$. Due to the two cuts by Alice and Bob, the cards are cyclic shifted by $(a + b) \bmod 5$ positions. In Alice's viewpoint, since $a, b \in \{0, 1, 2, 3, 4\}$ and b is chosen uniformly at random and independent of a, the encryption key $c \leftarrow (a + b) \bmod 5$ is also uniformly distributed over $\{0, 1, 2, 3, 4\}$. Let

$$G = \{♡♡♣♡♣,\ ♣♡♡♣♡,\ ♡♣♡♡♣,\ ♣♡♣♡♡,\ ♡♣♡♣♡\}\ .$$

Note that G contains both two possible initial configurations. For any configuration in G, if we cyclic shift it by $c \xleftarrow{\$} \{0, 1, 2, 3, 4\}$ positions then the resulting configuration is uniformly distributed over G. In other words, regardless of the initial configuration (that is, Bob's message), from Alice's viewpoint, the final configuration (that is, Bob's ciphertext) is uniformly distributed over G, and this distribution is independent of the message. Thus the ciphertext gives Alice no additional information about the message.