Mental Poker

The mental poker protocol is a kind of *multi-party* computation, and is based on a public-key encryption scheme with the following commutative composition property:

$$E_B(E_A(M)) = E_A(E_B(M)),$$

where E_X denotes encryption using X's public key. Likewise, we use D_X to denote decryption using X's private key.

In the mental poker problem, three players, Alice, Bob, and Carol, wish to play poker using networked communication (e.g., email). The dealer for this hand is assumed to be Alice, but Bob and Carol both want to make sure they are dealt a fair hand. A possible protocol for this problem is as follows:

1. Alice generates 52 distinct random numbers $x_1, x_2, \ldots, x_{52}$, where we assume that a sorted listing of these numbers corresponds to a sorted deck of cards. That is, the smallest x_i is the Ace of spades, the second smallest is the Ace of clubs, and so on.

2. Alice encrypts each of the x_i's using her own public key and sends the list of encrypted values, $E_A(x_1), E_A(x_2), \ldots, E_A(x_{52})$, to Bob.

3. Bob picks five of these encrypted numbers as his hand, say at indices $\{i_1, i_2, i_3, i_4, i_5\}$, and computes $E_B(E_A(x_{i_1}))$, $E_B(E_A(x_{i_2}))$, $E_B(E_A(x_{i_3}))$, $E_B(E_A(x_{i_4}))$, and $E_B(E_A(x_{i_5}))$, and sends these encrypted numbers to Alice. Bob also sends the remaining unchosen 47 "cards" to Carol.

4. Carol picks five of these encrypted numbers as her hand, say at indices $\{j_1, j_2, j_3, j_4, j_5\}$, and computes $E_C(E_A(x_{j_1}))$, $E_C(E_A(x_{j_2}))$, $E_C(E_A(x_{j_3}))$, $E_C(E_A(x_{j_4}))$, and $E_C(E_A(x_{j_5}))$, and sends these encrypted numbers to Alice. In addition, Carol picks five of the remaining 42 "cards" as Alice's hand, and sends these to Alice.

5. For each i_k, $k = 1, 2, \ldots, 5$, Alice computes

   $$D_A(E_B(E_A(x_{i_k}))), \text{ which is the same as } E_B(x_{i_k}),$$

   and she sends these values to Bob. She also computes, for each i_k, $k = 1, 2, \ldots, 5$,

   $$D_A(E_C(E_A(x_{j_k}))), \text{ which is the same as } E_C(x_{j_k}),$$

   and she sends these values to Carol.

6. Bob and Carol decrypt the values of the cards they picked, Alice reveals the list of numbers $x_1, x_2, \ldots, x_{52}$, and all the players learn their hands (and who is the winner).