

Mental poker

Each player is dealt five of the 52 cards. Each player can see his hand and not any other player's hand. Players bet based on their hands. The "best" hand wins. In some variations, some cards are revealed and some cards may be replaced by cards not yet dealt.

The "e-mail" or "mental" protocol for poker requires a fair deal: Players see their own hands, but not other hands. The hands are disjoint. All hands are equally likely. A player can "draw" (replace) selected cards. A player can reveal individual cards one at a time without revealing other cards. All players can check at the end of the game that there was no cheating.

We use a variation of Pohlig-Hellman to implement mental poker.

Assume there are two players, Alice and Bob. (There are similar protocols for three or more players.)

The players jointly choose a large prime p as modulus. Each secretly chooses e_A, d_A, e_B, d_B , as in Pohlig-Hellman. Define $E_A(M) = M^{e_A} \bmod p$, etc. Recall that these functions commute: $E_A \circ E_B = E_B \circ E_A$, etc. Let M_1, \dots, M_{52} be the encoded) deck (more if there is a joker).

1. Bob enciphers the cards as $C_i = E_B(M_i)$ for $i = 1, \dots, 52$. Bob sorts the C_i and sends them to Alice.

2. Alice selects five cards C_i at random and sends them to Bob, who decrypts them as his hand.

3. Alice selects five more random cards, say C_1, \dots, C_5 (her hand) and enciphers them as $C'_i = E_A(C_i)$. She sends them to Bob.

4. Bob decipheres the C'_i (they are still enciphered with E_A after he applies D_B to undo E_B) and sends them back to Alice.

5. Alice decipheres the five cards and uses them as her hand. They bet and play poker.

6. At the end of the hand, Alice and Bob exchange their keys e_A , etc., and check everything that happened.

Quadratic residues

Unfortunately, one can cheat in mental poker because E_A , E_B , etc., preserve quadratic residues.

Definition. a is a *quadratic residue* modulo n if $\gcd(a, n) = 1$ and there is an integer x such that $x^2 \equiv a \pmod{n}$. Such an x called a *square root* of a modulo n . a is a *quadratic non-residue* modulo n if $\gcd(a, n) = 1$ and there is no integer x such that $x^2 \equiv a \pmod{n}$.

Theorem. Let $0 < a < n$, $\gcd(a, n) = 1$, and $\gcd(e, \phi(n)) = 1$. Then a is a QR mod n iff a^e is a QR mod n .

Proof: Let d be the inverse of e mod $\phi(n)$: $ed \equiv 1 \pmod{\phi(n)}$. If a is a QR mod n , then there exists an x so that $x^2 \equiv a \pmod{n}$. Let $y = x^e \pmod{n}$. Then

$$y^2 \equiv (x^e)^2 \equiv (x^2)^e \equiv a^e \pmod{n}.$$

This shows that a^e is a QR mod n . Conversely, if a^e is a QR mod n with $y^2 \equiv a^e \pmod{n}$, then $(y^d)^2 \equiv a^{ed} \equiv a \pmod{n}$, so a is a QR mod n .

Alice can use this theorem to cheat: Perhaps most high cards are QR and most low cards are QNR. It is like playing with a deck in which most high cards are “marked”. This attack can be foiled by (a) appending extra bits to each M_i or (b) multiplying some M_i by a fixed QNR in order to make all cards be QR or all cards be QNR.

In order for Alice to cheat and in order to foil the attack, one must be able to distinguish between QR and QNR mod p (at least for prime p) quickly. This has been known for 200 years.