Multi-Party Computation (MPC).

- Goal : Alice has some data x
  Bob has some data y.
  They want to compute $f(x,y)$

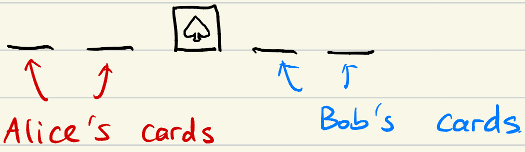
  Most importantly, they do not want the other person to learn anything more than $f(x,y)$.

Problem : $f(x,y) = x$ AND y.
$x, y \in \{0,1\}$

Example : Alice has $x=0$. , Bob has $y=1$.
Both will receive $f(x,y)=0$.

Bob knows $x=0$.
Alice does not know y.

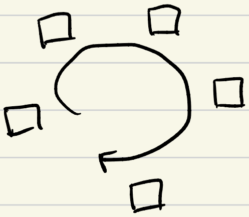
An example protocol : five poker cards.
2 ♡ . 3 ♤



Alice : ♡ ♤ if $x=1$
♤ ♡ if $x=0$.

Bob : ♡ ♤ if $x=0$.
♤ ♡ if $x=1$

(All cards are placed face down).



Rotate these 5 cards randomly.

$f(x,y)=1$. iff
there is "♡ " two adjancent hearts.