Problem 1: Yao’s Garbled Circuits

(a) One application of secure function evaluation is the so-called “dating problem”. Two parties $A$ and $B$ are wondering whether they should date, but none of them wishes to admit their interest unless they know that the other side is interested, too. The solution is to perform a two-party computation on their inputs $a$ and $b$ (where $a$ and $b$ are a bit corresponding to whether $A$ or $B$ wishes to date) that returns $f(a, b) := a \land b$. (We ignore the fact that this is silly: by suggesting to run this SFE, one already expresses interest. But we could consider a case where some app is doing this automatically with all potential matches – a privacy preserving dating app.)

$A$ and $B$ want to use Yao’s Garbled Circuits for this. (We ignore the fact that that protocol only has security against passive adversaries.) That is, $A$ will have to pick some circuit $C$, and $B$ some input $x$ for that circuit. What should $C$ and $x$ be in this concrete case (i.e., how to convert $a$ and $b$ into $C$ and $x$) so that $B$ learns $f(a, b)$?

(b) (Bonus problem) Implement part of Yao’s protocol. That is, implement a function `make_gate` that garbles a single gate. (Given four input keys, and four messages.) And a function `eval_gate` that recovers the message $m_{ij}$ given the corresponding keys.

Use the template in `yao-gate.py`. 