

- (b) John wants to send a digitally signed message to Rachel using a public-key cryptosystem. Who needs to publish a public key, John or Rachel? Why? Describe how the key is used.
4. (6 points) State the (a) public and (b) private information a user of RSA needs to produce.
5. (a) (6 points) Describe Batcher's Odd-Even Merge in pseudocode.
- (b) (6 points) Let $M(n)$ denote the number of parallel steps (clock beats) required by Batcher's Odd-Even Merge. Evaluate $M(n)$ exactly. Assume $n = 2^k$.
6. (G only, 6 points) Solve the following problem in linear time: INPUT: a digraph. OUTPUT: either a topological sort or an odd cycle.