Final

The exam should be done individually. You write your solutions on paper by yourself, scan (or photo capture through a mobile application such as CamScanner) and submit them as a single .pdf file. Your solutions have to be handwritten. **Solutions must be submitted electronically before 4 pm on August 27.** No credit will be given to solutions obtained verbatim from the Internet or other sources.

1. (16p) For an RSA public key (N, e) = (35, 5) and a given message m = 2, calculate the ciphertext of the message m. Also, break the encryption scheme and calculate the secret key.

2. For the question, first construct a flow network G using your student id as follows *('14600015' will be used here as an example to show you how the graph is constructed. Note that if your id contains letters, first remove the letters, then apply the following steps. For instance, if your id is '18YZ0345', consider it as '180345')*:

- multiply your id with '123456789'

$$14600015 * 123456789 = 1802470971251835$$

- remove all the zeros

$$1802470971251835 \rightarrow 18247971251835$$

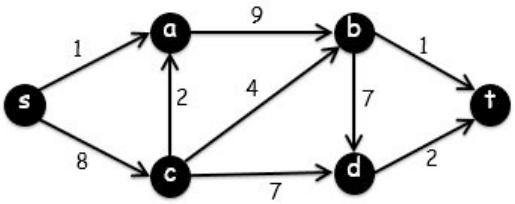
- cut out the first 9 numbers

$$182479712$$

- assign the numbers to the associated edges as capacity

$$(s,a) \rightarrow 1, (s,c) \rightarrow 8, (c,a) \rightarrow 2, (c,b) \rightarrow 4, (c,d) \rightarrow 7,$$
$$(a,b) \rightarrow 9, (b,d) \rightarrow 7, (b,t) \rightarrow 1, (d,t) \rightarrow 2$$

- construct the corresponding flow network



Assume you are using the Ford-Fulkerson algorithm to find the maximum flow, and you have applied the augmenting paths (s – c – d – t) and (s – c – b – t) for the first two steps.

a) (20p) Draw the residual network formed after these two augmenting paths.

b) (16p) List all the augmenting paths that could be chosen as the third augmenting path (if there is any) together with the residual capacity of each path.

3. (30p) For the question, first construct a weighted directed graph G using your student id as follows - similar to the question 2 - *('14600015' will be used here as an example to show you how the graph is constructed. Note that if your id contains letters, first remove the letters, then apply the following steps. For instance, if your id is '18YZ0345', consider it as '180345')*:

- multiply your id with '123456789'

$$14600015 * 123456789 = 1802470971251835$$

- remove all the zeros

1802470971251835 → 18247971251835

- cut out the last four numbers

1835

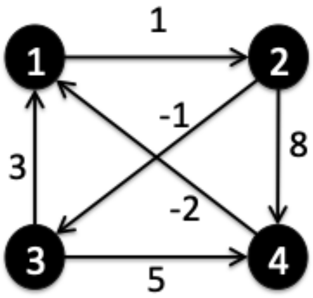
- fill the empty entries in the following adjacency weight matrix with the obtained 6 numbers, with the following order 'from the first row to the last row, and at each row, from left to right'*(the weights of the edges (2, 3) and (4, 1) are fixed as -1 and -2 for all the students)*:

	1	2	3	4
1	0		∞	∞
2	∞	0	-1	
3		∞	0	
4	-2	∞	∞	0

→

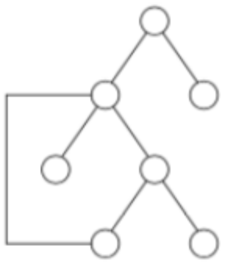
	1	2	3	4
1	0	1	∞	∞
2	∞	0	-1	8
3	3	∞	0	5
4	-2	∞	∞	0

- construct the corresponding graph



Assume you are using the Floyd-Warshall algorithm to find the shortest paths between every pair of vertices, and $D^{(4)}$ is the final matrix output by the algorithm. Just write the matrix $D^{(3)}$ for the answer.

4. (18p) Consider an undirected graph which is formed by taking a binary tree and adding an edge from exactly one of the leaves to another node in the tree. We call such a graph a loop graph. An example of a loop graph could be the following one:



Assume you are given a weighted loop graph (each edge has a positive integer weight). Design an efficient algorithm (better than Kruskal and Prim) for finding the minimum spanning tree of a given loop graph. To get full credit, you need to argue the running time.