Assignment 2

1. AmbulanceLagbe is an ambulance calling app designed to help those who are in need of emergency ambulance services.

   The calling process of an ambulance requires the user to request an ambulance providing several information. The request manager then receives the request and checks if the request is an emergency request or not. If the request is an emergency request, then the search module executes a search for an ambulance within a 2-kilometer radius. If not found, the request manager shows a message, "Ambulance not available" to the user. On the other hand, if the request is not an emergency, the search manager executes a regular search and the same message is displayed in the case of no available ambulance. However, for both cases, if an ambulance is found, the search manager sends the user location and contact information to the ambulance driver simultaneously. The ambulance driver then accepts the request. After that, the request manager does the following at the same time:

   - Sends the live location of the ambulance to the user, then shows the estimated time of arrival
   - Shows the direction to the ambulance driver.

   Now design **an activity diagram** based on the given scenario. Using swimlanes is not mandatory.

2. The following scenario shows a successful authentication of a client using the mobile OTP solution.

   The authentication is initiated when a user requests access to a service that requires authentication. The SP notifies the authenticator that a user needs to be authenticated. The session is redirected to the authenticator and the user is asked to enter a username. The username is sent to the AS which gets the secret key for this client and from this generates an OTP. The OTP is also based on a challenge. A different challenge is used every time so the generated OTP is always changing. At last a message authentication code (MAC) based on the secret key is calculated over the OTP. The AS sends the triplet (challenge, MAC, OTP) to the Authenticator which

relays the challenge and the MAC to the client. Upon receiving the challenge the client calculates the OTP. Then it calculates the MAC and compares it to the one received from the Authenticator. If the values match the client can authenticate the AS since the AS has proved that it is in possession of the shared key. The client then sends the OTP back to the Authenticator. If the MAC is wrong the authentication is aborted. The Authenticator compares the OTP with the one received from the AS and if they match, notifies the SP that the client is authenticated. A mutual authentication of the client and server has been achieved and the session is redirected back to the SP which grants the user access to the service.

Design a **sequence diagram** based on the above information.