1. The idea of common knowledge is important because it is able to extend the idea of collective knowledge(where everybody knows ϕ) with recursion, so that everybody knows that ... everybody knows ϕ. This creates a new way of reasoning within a group, as more information is available to each individual about what is known. In the paper it is stated that this idea of common knowledge makes driving on the road possible(because everybody has to know that everybody else knows the rule to even dare to drive). Another possible idea of

2. I dont know...

3. $$(M,s) \models C_G\varphi \Leftrightarrow (M,s) \models E_G(\varphi \wedge C_G\phi) \tag{1}$$

   Can be rewritten as:

   $$(M,s) \models C_G\varphi \Leftrightarrow (M,s) \models E_G(\varphi) \wedge E_G(C_G\varphi) \tag{2}$$

   Because of the definition on page 43 this can be rewritten as:

   $$(M,s) \models C_G\varphi \Leftrightarrow (M,s) \models E_G(\varphi) \wedge E_G(E_G^{k-1}\varphi) \text{ for } k = 2,3,... \tag{3}$$

   When we set $(M,s) \models C_G\varphi$ to true this can be rewritten as:

   $$(M,s) \models E_G^k\varphi \text{ for } k = 1,2... \Leftrightarrow (M,s) \models E_G(\varphi) \wedge E_G(E_G^{k-1}\varphi) \text{ for } k = 2,3,... \tag{4}$$

   More rewriting:

   $$(M,s) \models E_G^k\varphi \text{ for } k = (1,2... \Leftrightarrow (M,s) \models E_G(\varphi) \wedge E_G^k\varphi \text{ for } k = 1,2,... \tag{5}$$

   If E_G^k is true then $E_G(\varphi)$ as well, so that:

   $$(M,s) \models E_G^k\varphi \text{ for } k = 1,2,... \Leftrightarrow (M,s) \models E_G^k\varphi \text{ for } k = 1,2... \tag{6}$$

   In case $(M,s) \models C_G\varphi$ is not set to true the derivation could not be made, hence the case would be that $(M,s) \models \neg E_G(\varphi \wedge C_G\varphi$

4. For an attack to happen not only does the second commander have to receive the messenger, but also does the first commander need to know the second

commander knows that he wants to plan the attack and agrees to it. The second commander than nees to know that de first commandeer knows this and so on. Common knowledge in this case would enable the attack happening as then both parties would know that the other party new indefintely.

5. *Synchronous* in this problem means that all non faulty(not lying) generals after the same amount of time choose for the same time to attack
   Searching for agreement is the process for the non faulty processors to agree upon one and the same strategy, while the fault processors in *Byzantine failure* mode try to confsue these faulty processesors without their knowledge.
   Point to point means that all generals are fully connected to all other generals, and so is the messaging.

6. In the paper is stated that always SBA can me made, but in the case of *Byzantine failure* mode for faulty processors there have to be at least $n = 3 * f + 1$ more nonfaulty processors than faulty ones (where n is non faulty and f is faulty), else no agreement can be made. This is only true when signatures can be forgeable, else SBA can be made with arbitrary many faulty processors. The SBA can be made in f+1 rounds, where f is the upper bound of faulty processors in the system.