## 9.1 Question 1

### 9.1.A Summarize which databases are mainly responsible for security related purposes in a GSM network. What information do they contain and how are these being used to fulfil their purpose?

The most important databases to ensure security in terms of subscriber identification, authentication and registration are the Equipment Identity Register and the Authentication Center. These are connected via the Mobile Switching Center.
The Equipment Identity Register stores information about the serial number of a device, the so called IMEI. With this information checks can be performed whether the device contains malicious/obsolete software or is reported as stolen.
The AUC on the other hand, stores information about the SIM card of each device containing the IMSI, a random number, the signatur response, the authentication key $K_i$ and the encryption key $K_c$. This database uses the keys in order to authenticate the device and authorize service accesses.

### 9.1.B Describe the process depicted in the diagram below (explaining what each entity is & does). Why aren't we simply using $K_i$ for the job of $K_c$?

The picture is part of the diagram on slide 17 of the lecture:
The VLR - Visitor Location Register - is a database which stores the visiting user's data. $K_i$ and $K_c$ are keys of the device used for authentication and encryption, respectively. RAND is a random number coming from the AUC database. The IMSI is the International Mobile Station Subscriber Identity, the main identifier for each device. This identifier is **A8** is a radio encryption, based on the COMP algorithm - which is not secure.
We don't use $K_i$ because it itself is static and does not change. On the other hand as $K_c$ is created by using a random number which is changed periodically. Therefore if the key is compromised at some point, the later sent messages do not get compromised as the key $K_c$ might have already changed. This would not be the case if this process uses $K_i$ for this process.