ns 6(A). Uses of Intrusion detection system are:

- It keeps our network secure and flag when somebody is trying to break into system, it prevents it.
- It monitors for suspicious activity and issues alerts when such activity is discovered.
- It scans a network or a system for harmful activity.

→ Anomaly Based Method:
It was introduced to detect the unknown malware attacks as new malware are developed rapidly. This detection method uses machine learning to create a defined model of trust worthy activity and compares new behaviour against this trust model. ML based method has a generalized property in comparison to signature based IDS as these models can be trained according to the applications and hardware configuration.

→ Specification based detection:
It works on the basis of manually defined set of constraints and specification. It further induces low false positive rate as compared to the anomaly based detection mechanism. In this mechanism, the specification and constraints are used to describe the correctness of the detection process.

→ Signature based detection:
It detects the attacks on the basis of specific patterns such as no. of bytes or count of 1's & 0's in Network traffic. It originated from antivirus software, which refers to these detected patterns as signatures. It is impossible for it to detect new attacks, for which no pattern is available.

Bantola.