Question 1:

- Match the following terms within the context of Wireless Security:

1- Association:	**A-** Disable SSID broadcasting, change SSID to cryptic value, or reduce signal strength.
2- Ad-hoc networks:	**B-** Encrypt the transmissions to avoid eavesdropping.
3- Non-traditional networks:	**C-** Works well in wireless networks since it is easy to direct multiple messages to the target.
4- Identity theft:	**D-** Is an important factor because hardware should not be reached without being noticed.
5- Man-in-the-middle attack:	**E-** Only allow specific computers to the network.
6- Denial of service:	**F-** Works well in wireless networks since the connections are scattered all around the devices.
7- Network injection:	**G-** Peer-to-peer network without central control, so difficult to manage.
8- Signal hiding:	**H-** Against malware code inside network (that could open backdoors).
9- Encryption:	**I-** Makes the system dynamic leading to various introduced risks.
10- Port-based network control:	**J-** Users may connect to an incorrect network and get or send confidential resources.
11- Antivirus:	**K-** Only allow traffic on controlled ports and restrict traffic on specific ports.
12- Whitelist:	**L-** Personalized networks and addresses can lead to spoofing or eavesdropping.
13- Channel:	**M-** The medium through which the messages are being transmitted.
14- Mobility:	**N-** Attacks on access points that are exposed to non-filtered network traffic.
15- Resources:	**O-** Are helpful against computational-demanding attacks.
16- Accessibility:	**P-** Getting access to the MAC of privileged devices.