7.1 Question 1

7.1.A Match the following terms within the context of Wireless Security.

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