**Assignment – 2**

**Ans 1.**

**A)**  If the middle man can intercept the data travelleing between the routers, then from the IP header he can get the sender and reciever IP address, which can be further used to determine the source and destination original location. The middle man can also access the payload being transferred, but in encrypted state. (if any encryption is used)

**B)**  If C is using NATting on his end, then it will force the router to remap its IP address in some different address, which will later interfere the IP header changing the IP address so that, the middle man cannot have the original source address from where the payload sent.

**C)**  If C and S are communicating via VPN server. The middle man can get the IP address from the IP header, but this time it’ll be not the original source/destination IP address.

**D)**

First disadvantage of using VPN server for communication is **reduced performane.** It is so, because the data from original source is transferred to multiple networks and then tranferred to the original destination address. This offers privacy and security, but takes time and performance in return.

Second disadvantage is **not using trusted VPN service.** If the user is using some free VPN server or not so trusted VPN service, then they are just compromising their privacy and security. As the VPN service provider can do anything with their data rightiosuly.

Third disadvantage could be if  **middle man requests VPN server logs.**  If the middle man gets the user VPN server logs, then the user privacy could be compromised, as it could reveal the user original soruce IP address and payload details. So its always better to use trusted and paid VPN services.

**Ans 2.** The short answer is that nobody knows how to compute the inverse RSA (the "decryption") without knowing the prime factors of the modulus N; and nobody knows how to efficiently recover these prime factors from N alone. ... There is no positive reason which explains why RSA decryption is hard without knowing the private key

**Ans 3. Ciphertext is 1 8 16 16**

**Ans 4.** An Intruder Detection System (IDS) is an auto-mated technology designed and implemented todetect and communicate the presence of a personor object in a designated zone. IDS provides thedetection element in a security system whichholistically deters, detects, delays, and responds.

**Ans 5.**

1. Major disadvantage of facial recognition technology is the possibility of racial bias. Reports that facial recognition isn’t as effective at identifying people of color and women have surfaced.
2. The main disadvantage of the retinal scanner is that the person has to focus on the scanner from about three inches away. This restriction makes the device difficult for ATM use because a person using a cash machine rarely focuses on one area very long and is never close enough.