1. 
SSH does not encrypt the TCP/IP header. It would not be possible to encrypt information such as the routing information, as that would not allow the packets to reach the destination or the initial handshake information where the client/server determine protocols.

2. 
Message authentication codes make sure that the data has been received intact and unmodified. It can be done using hashing.

3. 
Key exchange can be used in SSH to make it so one doesn’t have to use a password when logging in. The server will recognize a key certificate that the client presents. Also, after authentication key exchange can refer to the synchronization of encryption between client and server.

4. 
SSH supports both public key and symmetric key.
5.

Diffie-Helman is able to allow two parties communicating in cleartext to create a secret that can is only known to the two parties and not anyone who is potentially eavesdropping on the communication. This is done by using a equation that is easy to solve for two parties that are communicating but computationally difficult for anyone attempting to intercept the communication.