Exercise_2

1.

- Confidentiality: protect the user data like password;
- Authentication: Assure the operation is conducted by the real user
- Data Integrity: Assure the data communication between user and the online shopping company is safe
- Non-Repudiation: protect against false denial of the action that user or company have taken

2.

TZUYH-->FIGHT

3.

It's impractical.

- Truly random (as opposed to pseudorandom) one-time pad values, which is a non-trivial requirement.
- Secure generation and exchange of the one-time-pad values, which must be at least as long as the message.
- The key can only be used one time so it has to be treat carefully to prevent any reuse in whole or part.