Turnitin Assignment (1500 words)

In your own words, compare and contrast the use of different cryptographic methods to ensure authentication, integrity and confidentiality in the following client/server settings

- client server interaction where a client application accesses a public API and uses hashed message authentication codes (HMAC)
- secure access to Web applications (HTTPS) (use of digital signatures and digital certificates and other techniques)
- secure remote login (SSH)

You should address the use of cryptographic hash functions, symmetric and asymmetric key encryption, digital signatures and digital certificates as applied to hashed message authentication codes (HMAC), secure HTTP (HTTPS) and secure shell (SSH).

Your report should be based on the algorithms covered in the course. In addition you should include code snippets from the labs. Code snippets should also be based on lab exercises.

Marks will be given for how well you integrate the technical terms into the report where appropriate from the following:
confidentiality, integrity, authentication and non-repudiation, cryptographic hash function, message authentication codes, symmetric and asymmetric key encryption, checking digital signatures and checking digital certificates, keystores and trust stores.

You should structure the report as follows:

1. Introduction (short and possibly including some definitions)	5%
2. Client Accesses a Public API (HMAC)	20%
3. Secure Access to Web Applications (HTTPS)	40%
4. Secure Shell (SSH)	20%
5. Overview and Conclusion (including comparison)	15%

The report will be evaluated based on the following criteria:

- How well you identify the importance of each property (authentication, integrity and confidentiality) in a particular setting (HMAC, HTTPS, SSH)
- How well you outline the requirements, uses and functioning of each technique (cryptographic hash function, symmetric and asymmetric key encryption, digital signatures and digital certificates)
- How these techniques are applied and how they provide the identified properties (authentication, integrity and confidentiality)
- Comparison and contrasting of the different techniques and client/server settings
- Overall structure of the report.

You should include **your own diagrams** where appropriate and **you should explain them**.
Introduce the techniques as you need them in the report. (Obviously if a technique is introduced in one section and is needed in a second section it is not necessary to explain it again).

Note that this is not a research report. This report can be completed based on the material covered in the lectures and labs.