**Ice Task 1 Principles of security Thomas Knox st10275468**

1. A hash algorithm is a Crpytographic algoritm that is used to encrypt data or information keeping it secure from outsiders.
2. The common uses of hash algorithms is to verify integrity of files and messages and password verification.
3. Good qualities of a hash algorithm is that it is secure, original and unique.
4. The difference between hash functions and ecryption functions is the amount of data they process at a time.
5. Three commonly used hash algorithms include :

* Message Digest 5 (MD5)
* Secure Hash Algorithm(SHA)
* Hashed Message Authentication Code(HMAC)

1. Secure Hash algorithm 1 is considered to be broken because of collision attacks. This is when 2 different inputted data procudes the same output.
2. The difference is that MD5 has 512 bits while SHA-256 has 256 bits. So they differ by 256 bits.