1. Please compare hash function and cryptographic hash function and give an example.

一般來說，加密雜湊函數(cryptographic hash function)是雜湊函數(hash function)中的一種特例，也就是雜湊函數未必要是加密雜湊函數。

**加密雜湊函數(ex SHA-256…)**相對一般的雜湊函數，必須要提供更多的安全保障，要具有以下特質：相同的訊息輸入hash過後的輸出就要相同，Pre-image attack resistant(不容易找到特定輸出值的輸入訊息)，collision resistant(幾乎不會有不同的輸入訊息產生出相同的輸出的情況)，有了以上特點，因此適合用在指紋辨識等安全性需求較高的應用上。

而一般的雜湊函數在安全性上就並不如此注重，只需要避免惡意輸入造成的collison情形，例如常用在偵測是否因為網路不穩定而造成收到的封包訊息有偏誤；此外值得一提的是MD5, SHA1在能夠反向破解後，已從加密雜湊函數降格為一般的雜湊函數。