1. Investigate and compare Encrypt-then-MAC, MAC-then-Encrypt, and Encrypt-and-MAC. [3 points]

> Encrypt-then-MAC: encrypt the message first, then use the ciphertext to create tag and result in ciphertext-tag pair (c, tag).
>
> Mac-then-Encrypt: Mac the message first, then encrypt the message-tag pair, the result is ciphertext.
>
> Encrypt-and-MAC: Mac the plaintext, and plaintext is encrypted without MAC.

2. Investigate and compare MD5, SHA-1, SHA-2, and SHA-3. [4 points]

> MD5: Original input is divided into fixed-sized blocks, each is processed by the output of prior round and the message, the final output is 128-bit.
>
> SHA-1: compared to MD5, increase rounds of operations and the output length to 160 bit.
>
> SHA-2: increase output length, and slower, more collision-resistant.
>
> SHA-3: competely different from previous three versions. The structure has two parts: absorbing and squeezing. Much faseter than its predecessors and has more advantages but lack of hardware and software support.

3. How Birthday attacks can be used to break a hash code. [3 points]

> Birthday attacks basically use the fraudulent data which has the same hash code with the orignal one to replace it. The memory space of the birthday attack needs $c\sqrt{n}$, i.e. $O(\sqrt{n})$, which largely decrease the seach space of the hash code.