1. The encryption algorithm of a probabilistic encryption scheme takes in two inputs—a key $K$ and a message $M$. In contrast, the encryption algorithm of an authenticated-encryption scheme (an AEAD scheme) takes in four inputs. Name them, and briefly describe what each input is for. I will start you out with the first two:

1. $K$: The key that the communicating parties share.

2. $M$: The message (plaintext) that the sender wants encrypted and authenticated.

3. 

4. 

2. Describe the main security property that is expected of a cryptographic hash function.