* HS256 (HMAC with SHA-256), on the other hand, is a symmetric algorithm, with only one (secret) key that is shared between the two parties. Since the same key is used both to generate the signature and to validate it, care must be taken to ensure that the key is not compromised.  
  If you will be developing the application consuming the JWTs, you can safely use HS256, because you will have control on who uses the secret keys. If, on the other hand, you don’t have control over the client, or you have no way of securing a secret key, RS256 will be a better fit, since the consumer only needs to know the public (shared) key.