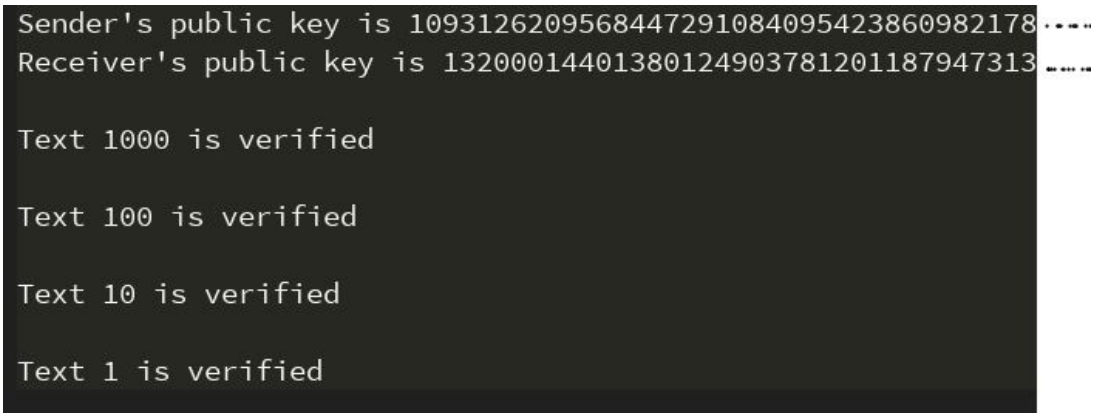
**Yücel Özdemir – 220201009**




**Secrecy:**

Since we didn't apply any encryption process, and contents of messages are common and can be read by everyone, we cannot make interpretation about secrecy.

**Identification:**

Identification is satisfied for the fact that message is singed with private key. Hence private key is personally identifiable and only "the" user knows private key, and this is evidence of which identity it was sent from.

**Integrity:**

Integrity is satisfied. Hash function is applied for whole message, and we get only single hash result. Different messages cannot convert to same hash value due to collision-free. Integrity control can be applied because whatever the same message reaches the same hash value.

**Non-repudiation:**

Identification leads to non-repudiation. In other words, once you've authenticated as yourself, you can't repudiate your identity. Thus, in this project non-repudiation is satisfied so that identification is satisfied.