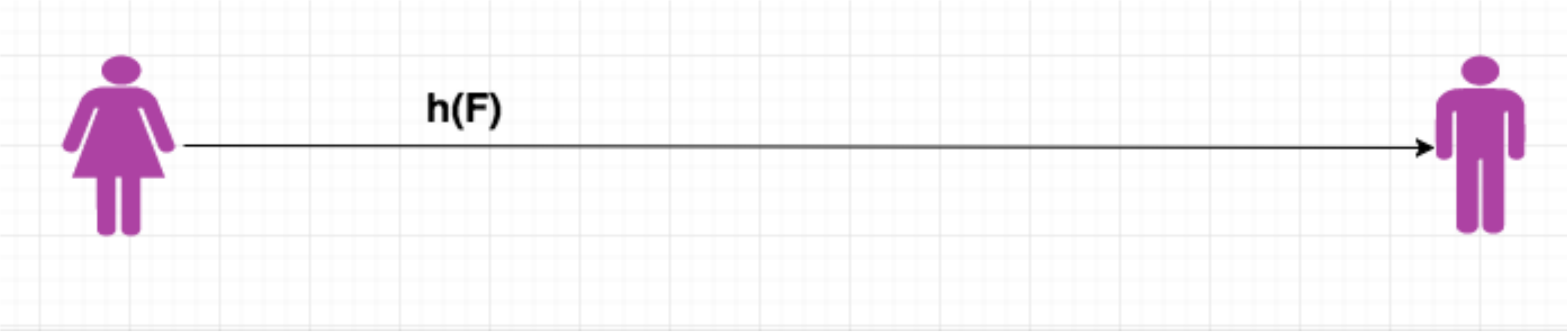
In the keyed hash, the file is hashed with some kind of secret key.

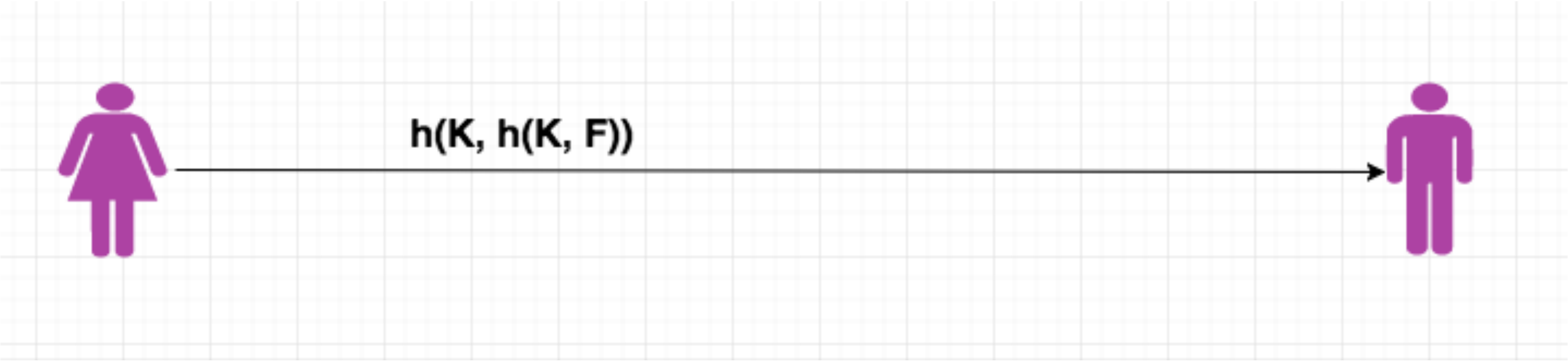
In this we use the same Hash Algorithm, but we add extra value key which makes harder for attacker to find, i.e to change the way of hashing done.

First way of doing it -



1. Random Error - if one bit in the file changes, the whole hash changes that is how we can handle random error in this way.

Second way of doing it -



In this way keyed hash provide an extra protection.

1. Random Error - We still can handle Random error.
2. Intensional Change - even though attacker intensionally changes the file to match hash value, they can't get to know key and can't have full access to file, so it handle both Random Error and Intensional Change.