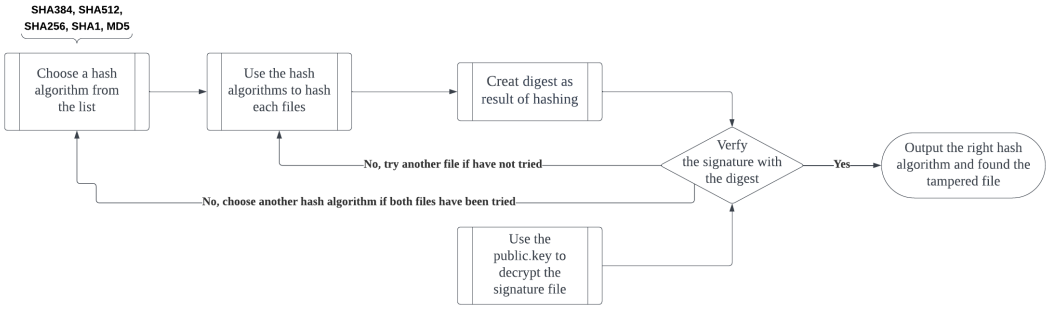
1 File integrity report

1.1 How we solve the question

The question requests to find the file which has been tampered with due to being stored in the unsecured server without opening both files. We noticed two additional files, *signature.pem* and *public.key*. We assumed that both files were initially provided by TechnoWizard, and there was no modification made by the third party. If the signature and public key are correct, it will match the same hash as the original file. Then we decided to find out which hash algorithm the signature used; there are two ways to find out; one way is to brute force the cryptographic keys and another is, as we know, one of the files is a verified file, so it would use the proper hash algorithm as signature does, we need to use a list of hash algorithms to brute force each file, using the result to verify with the signature, if it is verified, meaning this is the proper file and another does not; if not, we will try again until found it. The instructions have been shown in Figure 1.



Figur 1: Process

1.2 Result

The file that has been tampered with is: *messageTwo.txt*, and the hash algorithm used is: $SHA256$.

1.3 Justification about why made this identification

Firstly, we chose to use the hashed result of each file to verify the signature because we knew there was a file that had been stored in the secure folder, and therefore the correct file must have the same hash algorithm as the signature. In addition, as shown in Figure 1, we chose $SHA384, SHA512, SHA256, SHA1, MD5$ as a set of brute force algorithms because these algorithms were been widely used and had higher possibilities of making success.