CIS 751 Lecture Assignment 12

Chuck Zumbaugh

November 5, 2025

1 Signing the file

Assuming that we have already generated a public/private key pair (ex. using openssl genrsa), we can sign the file (article.txt) as follows.

```
openssl dgst -sha256 -sign private_key.pem \
-out article.signature article.txt
```

This command will generate a hash of the file using the SHA-256 algorithm and sign it using the private_key.pem file. The signature will then be output in the article.signature file.

2 Verifying the signature

We will use the public key and the original article to verify the signature. This can be done with the below command.

```
openssl dgst -sha256 -verify public_key.pem \
-signature article.signature article.txt
```

This command will use the SHA-256 algorithm, public_key.pem file, the signature in the article.signature file, and the article.txt to verify the signature. Assuming the verification is successful, openssl will print "Verified OK" to the terminal.