CIS 751 Lecture Assignment 11

Chuck Zumbaugh

October 31, 2025

This document details encrypting/decrypting this article from Nature using openssl. The article was split into 13 chunks due to the size restrictions of RSA, labeled ”article_chunk${i}.txt”. After generating the private/public key pair, all chunks were encrypted. The resulting encrypted files were then decrypted with the private key and combined to generate the original text. While there were some small differences between the original and decrypted files (due to my imperfect chunking with new lines), the article content in the decrypted file matched that of the original. Relevant code snippets are shown below.

RSA public/private key pairs were generated with the following commands:

```
# Generate private key
openssl genrsa -out private_key.pem 4096

# Generate public key
openssl rsa -in private_key.pem -pubout -out public_key.pem
```

We shall use three bash scripts to encrypt, decrypt, and combine article chunks:

```
#!/bin/bash

# Iterate through article chunks and encrypt them
for i in {1..13}; do
        openssl rsautl -encrypt -pubin -inkey public_key.pem \
         -in "article_chunk${i}.txt" -out "enc_chunk${i}.bin"
done
```

```
#!/bin/bash

# Iterate through chunks of encrypted text and decrypt them
for i in {1..13}; do
        openssl rsautl -decrypt -in "enc_chunk${i}.bin" \
        -inkey private_key.pem -out "chunk${i}_decrypt.txt
done

#!/bin/bash

# Go through decrypted chunks and create the article
for i in {1..13}; do
        cat "chunk${i}_decrypt.txt" >> decrypted_article.txt
done
```