Computer Security
Homework-2

Diptangshu De
50466657

Question 1

The chosen programming language and library option above

Solution:

I have used Java programming language. I have used java.security and javax.crypto packages to achieve the results.

Question 2

how per byte speed changes for different algorithms between small and large files

Solution:

For all the different algortihms time to encrypt and decrypt is directly proportional to the file size. On the other hand for RSA algorithms the time to encrypt and decrypt doesn't change depending on the file size.

Question 3

how encryption and decryption times differ for a given encryption algorithm;

Solution:

For all AES algorithms the encryption times and decryption times are nearly the same respectively for both the file sizes. Though the decryption times are more than the encryption times. For RSA algorithms

Question 4

how key generation, encryption, and decryption times differ with the increase in the key size;

Solution:

For AES Key generation 256 bit key generation takes more time than 128 bit key generation. On the other hand RSA key generations take the same time. For large files, larger key sizes take more time in encryption and decryption than smaller key sizes.

Question 5

how hashing time differs between the algorithms and with increase of the hash size;

Solution:

As hash sizes increase the hashing time decreases.

Question 6

how performance of symmetric key encryption (AES), hash functions, and public-key encryption (RSA) compare to each other.

Solution:

When encrypting huge volumes of data, symmetric key encryption, like AES is typically quicker and more effective than public-key encryption, like RSA. But, symmetric encryption needs a safe method for the communicating parties to exchange keys.

On the other hand, hash functions are incredibly quick and effective, but because they are one-way functions, they cannot be utilized for encryption. Instead, they are employed to check the accuracy of data and guarantee that it has not been altered.