Assignment

Homework 2

Ankita Sharma/50464503/as488@buffalo.edu

CSE565- Computer Security Homework Assignment

University at Buffalo

March 20,2023

Problem 1

I. The chosen programming language and library option above.
II. The timing results that your program measured as specified above.
III. For each performance aspect below, your comments about
(i) the expected performance
(ii) whether the observed performance followed the expected performance
(iii) if there was a difference, your justification of the difference

1.[2 points for 410/565] how per byte speed changes for different algorithms between small and large files
2.[2 points for 410/565] how encryption and decryption times differ for a given encryption algorithm
3.[2 points for 410/565] how key generation, encryption, and decryption times differ with the increase in the key size
4.[2 points for 410/565] how hashing time differs between the algorithms and with increase of the hash size
5.[2 points for 410/565] how performance of symmetric key encryption (AES), hash functions, and public-key encryption (RSA) compare to each other.

Solution.

Please run program using (sh cryptotools.sh) I. Programming languages and libraries used:
a) Program language : Java
b) Libraries used :

- import java.io.*;
- import java.security.*;
- import java.util.*;
- import javax.crypto.*;
- import java.lang.*;
- import java.io.FileInputStream;
- import java.io.FileOutputStream;
- import java.security.KeyPair;
- import java.security.KeyPairGenerator;
- import java.security.PrivateKey;
- import java.security.PublicKey;

- import java.util.Base64;
- import javax.crypto.Cipher;
- import java.io.*;
- import java.security.*;
- import java.nio.file.Files;
- import java.io.File;
- import java.io.FileInputStream;
- import java.io.FileOutputStream;
- import java.security.Key;
- import java.security.NoSuchAlgorithmException;
- import java.util.Arrays;
- import javax.crypto.Cipher;
- import javax.crypto.KeyGenerator;
- import javax.crypto.SecretKey;
- import javax.crypto.spec.IvParameterSpec;
- import javax.crypto.spec.SecretKeySpec;
- import java.io.File;
- import java.io.FileInputStream;
- import java.io.FileOutputStream;
- import java.security.Key;
- import java.security.NoSuchAlgorithmException;
- import java.util.Arrays;
- import javax.crypto.Cipher;
- import javax.crypto.KeyGenerator;
- import javax.crypto.SecretKey;
- import javax.crypto.spec.IvParameterSpec;
- import javax.crypto.spec.SecretKeySpec;
- import java.io.FileInputStream;
- import java.io.FileOutputStream;

- import java.security.KeyPair;
- import java.security.KeyPairGenerator;
- import java.security.PrivateKey;
- import java.security.PublicKey;
- import java.util.Base64;
- import javax.crypto.Cipher;

ii)

Timing results for different algorithms are as follows:

```
ankita@UBL-5CD0119DNV:/mnt/c/Users/Ankita/Desktop/compsec$ sh cryptotools.sh

----------------------------CBC/CTR Mode for AES key size 128--------------------------

Time taken to generate AES key of size 128 bits : 135392500 nanoseconds
Small file size in Kb: 1
Large file size in Kb: 10240
Key Size ---- 128 bits -----

----------------------------CBC Mode for key size 128--------------------------

Time to encrypt 1Kb file with CBC = 6.27212E7 nanoseconds
Encryption speed per byte with CBC = 1.632621824837535E-5 bytes/nanoseconds
Time to encrypt 10Mb file with CBC = 4.972606E8 nanoseconds
Encryption speed per byte with CBC = 0.021087051739068007 bytes/nanoseconds
Time to decrypt 1Kb file with CBC = 3.13547E7 nanoseconds
Decryption speed per byte with CBC = 3.2658580691252026E-5 bytes/nanoseconds
Time to decrypt 10Mb file with CBC = 3.491268E8 nanoseconds
Decryption speed per byte with CBC = 0.030034245437474294 bytes/nanoseconds

----------------------------CTR Mode for key size 128--------------------------

Time to encrypt 1Kb file with CTR = 1.61179E7 nanoseconds
Encryption speed per byte with CTR = 6.353184968265097E-5 bytes/nanoseconds
Time to encrypt 10Mb file with CTR = 3.464205E8 nanoseconds
Encryption speed per byte with CTR = 0.030268878429538668 bytes/nanoseconds
Time to decrypt 1Kb file with CTR = 1.38818E7 nanoseconds
Decryption speed per byte with CTR = 7.376564998775375E-5 bytes/nanoseconds
Time to decrypt 10Mb file with CTR = 4.583785E8 nanoseconds
Decryption speed per byte with CTR = 0.02287576751527395 bytes/nanoseconds
```

```
------------------------------CBC/CTR Mode for AES key size 256---------------------------

Time taken to generate AES key of size 256 bits : 117371900 nanoseconds
Small file size in Kb: 1
Large file size in Kb: 10240
Key Size ---- 256 bits -----

------------------------------CBC Mode for key size 256---------------------------

Time to encrypt 1Kb file with CBC = 2.48517E7 nanoseconds
Encryption speed per byte with CBC = 4.120442464700604E-5 bytes/nanoseconds
Time to encrypt 10Mb file with CBC = 215706000 nanoseconds
Encryption speed per byte with CBC = 0.04861135063466014 bytes/nanoseconds
Time to decrypt 1Kb file with CBC = 16540900 nanoseconds
Decryption speed per byte with CBC = 6.190715136419421E-5 bytes/nanoseconds
Time to decrypt 10Mb file with CBC = 2.231872E8 nanoseconds
Decryption speed per byte with CBC = 0.046981905772374044 bytes/nanoseconds

------------------------------CTR Mode for key size 256---------------------------

Time to encrypt 1Kb file with CTR = 1.51557E7 nanoseconds
Encryption speed per byte with CTR = 6.756533845351914E-5 bytes/nanoseconds
Time to encrypt 10Mb file with CTR = 451781500 nanoseconds
Encryption speed per byte with CTR = 0.023209803854296822 bytes/nanoseconds
Time to decrypt 1Kb file with CTR = 13739800 nanoseconds
Decryption speed per byte with CTR = 7.452801350820245E-5 bytes/nanoseconds
Time to decrypt 10Mb file with CTR = 3.207196E8 nanoseconds
Decryption speed per byte with CTR = 0.032694478291941 bytes/nanoseconds

------------------------------RSA Mode for key size 2048---------------------------

Time taken to generate RSA key of size 2048 bits : 223072100 nanoseconds
Time to encrypt 1Kb file with RSA = 4599700 nanoseconds
Encryption speed per byte with RSA = 2.2262321455747113E-4 bytes/nanoseconds
Time to decrypt 1Kb file with RSA = 21043900 nanoseconds
Decryption speed per byte with RSA = 4.866018181040587E-5 bytes/nanoseconds
Time to encrypt 1Mb file with RSA = 2138441300 nanoseconds
Encryption speed per byte with RSA = 4.90345935612074E-4 bytes/nanoseconds

Time to decrypt 1Mb file with RSA = 17940831900 nanoseconds
Decryption speed per byte with RSA = 5.844634216766726E-5 bytes/nanoseconds
```

```
----------------------------RSA Mode for key size 3072--------------------------

Time taken to generate RSA key of size 3072 bits : 821255700 nanoseconds
Time to encrypt 1Kb file with RSA = 6187500 nanoseconds
Encryption speed per byte with RSA = 1.654949494949495E-4 bytes/nanoseconds
Time to decrypt 1Kb file with RSA = 39213600 nanoseconds
Decryption speed per byte with RSA = 2.6113389232307157E-5 bytes/nanoseconds
Time to encrypt 1Mb file with RSA = 2852087100 nanoseconds
Encryption speed per byte with RSA = 3.676521660225594E-4 bytes/nanoseconds
Time to decrypt 1Mb file with RSA = 36793884600 nanoseconds
Decryption speed per byte with RSA = 2.8498648930371435E-5 bytes/nanoseconds

----------------------------Hashing Algorithms--------------------------

SHA-256 hash value for 1K.txt: aaea059fd2eb5cc6c116e7bce0990175338c60923c6e99da9d39f8f5b8c64459
Time to hash message with SHA-256 algorithm = 72710800 nanoseconds
Per byte time to hash message with SHA-256 algorithm = 71006 nanoseconds
SHA-512 hash value for 1K.txt: 4eb4fd1c9738d5e4dcc35021bea374f288e560a910de2ef3085bbd6adc6b97fca2fad5102f8e31c09902f9dfa468f6f646e4b1fca567d4faae08c74f6d66b727
Time to hash message with SHA-512 algorithm = 4824400 nanoseconds
Per byte time  to hash message with SHA-512 algorithm = 4711 nanoseconds
SHA3-256 hash value for 1K.txt: c73b221e74275833b54e4c875895d9c8cc6946592f31f11bf748ada6c9cfde9b
Time to hash message with SHA3-256 algorithm = 5518900 nanoseconds
Per byte time  to hash message with SHA3-256 algorithm = 5389 nanoseconds
SHA-256 hash value for 10M.txt: 64ef6c48dfa771287c5168c492930414f8b29bd3775c345dbf825f6a88d17bfc
Time to hash message with SHA-256 algorithm = 121093200 nanoseconds
Per byte time  to hash message with SHA-256 algorithm = 11 nanoseconds
SHA-512 hash value for 10M.txt: 75bbff908443b96cedb96d666d4ea46e9a7c7a1a0421cd0634fcb557b6bcbc1a5dbb857bff6c20ae49494a4eb2e586fa8035781ab4cdf64835ce40ace961ff46
Time to hash message with SHA-512 algorithm = 114822000 nanoseconds
Per byte time  to to hash message with SHA-512 algorithm = 10 nanoseconds
SHA3-256 hash value for 10M.txt: a9b0279d50eac823d5211d0d53ba73c28dfe2bcd9c30ab6a3605d55aaee2fbcb
Time to hash message with SHA3-256 algorithm = 168840700 nanoseconds
Per byte time  to hash message with SHA3-256 algorithm = 16 nanoseconds
Total time taken to hash both files with multiple algorithms = 487810000 nanoseconds

----------------------------DSA Mode for key size 2048--------------------------

Time taken to generate DSA key of size 2048 bits : 20922200 nanoseconds
Time taken to sign the message of size 1Kb with Digital Signature : 7096800 nanoseconds
Per byte time  to sign the message of size 1Kb with Digital Signature = 6930 nanoseconds
Signature for 1K.txt verified: true
Time taken to verify the message of size 1Kb with Digital Signature : 211700 nanoseconds
Per byte time  to verify the message of size 1Kb with Digital Signature = 206 nanoseconds
Time taken to sign the message of size 10Mb with Digital Signature : 45401300 nanoseconds
Per byte time  to sign the message of size 1Kb with Digital Signature = 4 nanoseconds
Signature for 10M.txt verified: true
Per byte time  to verify the message of size 1Kb with Digital Signature = 3 nanoseconds
Time taken to verify the message of size 10Mb with Digital Signature : 33949600 nanoseconds
```

```
----------------------------DSA Mode for key size 3072--------------------------

Time taken to generate DSA key of size 3072 bits : 30565100 nanoseconds
Time taken to sign the message of size 1Kb with Digital Signature : 11068700 nanoseconds
Per byte time  to sign the message of size 1Kb with Digital Signature = 10809 nanoseconds
Signature for 1K.txt verified: true
Time taken to verify the message of size 1Kb with Digital Signature : 305000 nanoseconds
Per byte time  to sign the message of size 1Kb with Digital Signature = 297 nanoseconds
Time taken to sign the message of size 10Mb with Digital Signature : 74708100 nanoseconds
Per byte time  to sign the message of size 1Kb with Digital Signature = 7 nanoseconds
Signature for 10M.txt verified: true
Per byte time  to sign the message of size 1Kb with Digital Signature = 3 nanoseconds
Time taken to verify the message of size 10Mb with Digital Signature : 33179300 nanoseconds
```

iii)

Encryption speed/byte

Speed in Bytes/Nanoseconds					
Input Size	AESCBC128	AESCTR128	AESCTR256	RSA2048	RSA3072
1 Kilobyte	$1.63 * 10^-5$	$6.35 * 10^-5$	$6.76 * 10^-5$	$2.27 * 10^-4$	$1.65 * 10^-4$
10 Megabyte	$2.11 * 10^-2$	$3.03 * 10^-2$	$2.32 * 10^-2$	-	-
1 Megabyte	-	-	-	$4.9 * 10^-4$	$3.67 * 10^-4$

Decryption speed/byte

Speed in Bytes/Nanoseconds					
Input Size	AESCBC128	AESCTR128	AESCTR256	RSA2048	RSA3072
1 Kilobyte	$3.27 * 10^-5$	$7.38 * 10^-5$	$7.45 * 10^-5$	$4.87 * 10^-5$	$2.61 * 10^-5$
10 Megabyte	$3.00 * 10^-2$	$2.29 * 10^-2$	$3.27 * 10^-2$	-	-
1 Megabyte	-	-	-	$5.84 * 10^-5$	$2.85 * 10^-5$

Encryption Time

Time in Nanoseconds							
Input Size	AESCBC128	AESCTR128	AESCTR256	RSA2048	RSA3072	DSA	DSA3072
1 Kilobyte	$6.27 * 10^7$	$1.61 * 10^7$	$1.52 * 10^7$	$4.6 * 10^6$	$4.6 * 10^6$	$7.1 * 10^6$	$1.11 * 10^7$
10 Megabyte	$4.97 * 10^8$	$3.46 * 10^8$	$4.52 * 10^8$	-	-	$7.1 * 10^6$	$7.4 * 10^7$
1 Megabyte	-	-	-	$2.14 * 10^9$	$2.85 * 10^9$	-	-

Decryption Time

Time in Nanoseconds							
Input Size	AESCBC128	AESCTR128	AESCTR256	RSA2048	RSA3072	DSA	DSA3072
1 Kilobyte	$3.14 * 10^7$	$1.39 * 10^7$	$1.65 * 10^7$	$2.1 * 10^7$	$3.92 * 10^7$	$2.18 * 10^5$	$3.05 * 10^5$
10 Megabyte	$3.49 * 10^8$	$4.58 * 10^8$	$3.28 * 10^8$	-	-	$3.39 * 10^7$	$3.38 * 10^7$
1 Megabyte	-	-	-	$1.79 * 10^{10}$	$3.67 * 10^{10}$	-	-

Key generation Time

Time in Nanoseconds					
AES	AES256	RSA2048	RSA3072	DSA	DSA3072
$1.35 * 10^8$	$1.17 * 10^8$	$2.23 * 10^8$	$8.21 * 10^8$	$2.09 * 10^7$	$3.06 * 10^7$

Hashing Algorithm Time

Time in Nanoseconds			
Input Size	SHA-256	SHA-512	SHA3-256
1 Kilobyte	$7.27 * 10^7$	$4.82 * 10^6$	$5.51 * 10^6$
10 Megabyte	$1.21 * 10^8$	$1.14 * 10^8$	$1.69 * 10^8$

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

— Encryption and Decryption speed/byte increases with change in file size.As file size is increased the speed is increased.However for RSA speed/byte remains the same for both the files.

How encryption and decryption times differ for a given encryption algorithm

— Encryption and Decryption time for AES algorithm are almost same but Decryption time when compared to Encryption algorithm takes more time to decrypt that encrypt.

RSA algorithm takes much more time to encrypt than symmetric AES algorithm.

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

—

Key Generation - For AES key generation takes almost same time while RSA and DSA takes slightly longer time when key size is increased. Encryption Time and Decryption Time are not much affected by change in Key sizes.

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

— Hashing time of SHA-256 is more than hashing time of SHA3-256 and SHA-512 for small file of 1Kb. With increase in hash size there's a decrease in hash time. For large file, the hashing time is almost similar.

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

– AES symmetric Key algorithm is faster than RSA.Hash functions are faster than both public key encryption and symmetric key encryption.However,symmetric key encryption are generally faster than hash functions and public key encryption.