Aug. 6, 2020

Report Lab2

s1260066 Chiho Iwata

Contents

1. (1) Problem 1: (1) proof of your code run actually (copy & paste of the console screen)
2. (2) Problem 2: (1) proof of your code run actually (copy & paste of the console screen) (2) answer of the following questions
    1. Make graphs of the time measurements [μs] as function of file sizes [bytes] that show: (20 points)
        (a) DESencryption/decryptiontimes.
        (b) RSAencryptiontimes.
        (c) RSAdecryptiontimes.
        (d) SHA-1 digests generation times.
    2. Answer the following questions:
        5. (e) Compare DES encryption and RSA encryption. Explain your observations. (10 points)
        6. (f) Compare DES encryption and SHA-1 digest generation. Explain your observations.
        7. (g) CompareRSAencryptionanddecryptiontimes.Canyouexplainyourobservations?

Problem 1

(1) Run

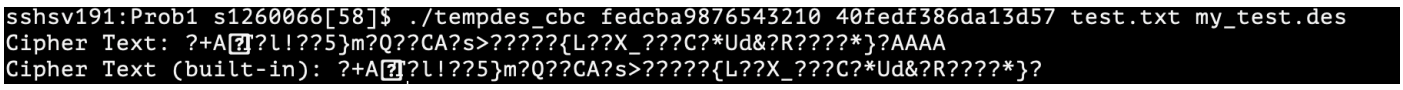
To do this you should use following command: **./tempdes_cbc fedcba9876543210 40fedf386da13d57 test.txt my_test.des**

<result>

[Copy & paste]

```
sshsv191:Prob1 s1260066[58]$ ./tempdes_cbc fedcba9876543210 40fedf386da13d57 test.txt
my_test.des
Cipher Text: ?+A?T?l!??5}m?Q??CA?s>?????{L??X_???C?*Ud&?R????*}?AAAA
Cipher Text (built-in): ?+A?T?l!??5}m?Q??CA?s>?????{L??X_???C?*Ud&?R????*}?
```

[Screen shot]



$ less filename.des

<test.des>

```
?+A?T<D5>^N<l!<E7><CF>^N5}^Zm<E2>Q<C0><FE>CA<9B>s><B5><92><EF><F3><B5><E6>{
L<FF><AF>XESC<DE>_<EA><E0>^\<A9>^H<B7>C<E2>*Ud&<95>R^G<BB>^Z<DD>^F<E4><EE>
*}<ED>
test.des (END)
```

<my_test.des>

```
?+A?<D5>^Nl!<E7><CF>^N5}^Zm<E2>Q<C0><FE>CA<9B>s><B5><92><EF><F3><B5><E6>{
L<FF><AF>XESC<DE>_<EA><E0>^\<A9>^H<B7>C<E2>*Ud&<95>R^G<BB>^Z<DD>^F<E4><EE>
*}<ED>AAAA
my_test.des (END)
```

Problem2

(1) Run

$ ./tempdes ./data/test_*.txt

```
sshsv192:Prob2 s1260066[67]$ ./tempdes ./data/test_8.txt
File containes 8 bytes
Encryption time: 31 us
Decryption time: 1 us
sshsv192:Prob2 s1260066[68]$ ./tempdes ./data/test_8.txt
File containes 8 bytes
Encryption time: 37 us
Decryption time: 12 us
sshsv192:Prob2 s1260066[69]$ ./tempdes ./data/test_8.txt
File containes 8 bytes
Encryption time: 32 us
Decryption time: 1 us
sshsv192:Prob2 s1260066[70]$ ./tempdes ./data/test_8.txt
File containes 8 bytes
Encryption time: 16 us
Decryption time: 1 us
sshsv192:Prob2 s1260066[71]$ ./tempdes ./data/test_8.txt
File containes 8 bytes
Encryption time: 32 us
Decryption time: 1 us
```

```
sshsv192:Prob2 s1260066[72]$ ./tempdes ./data/test_64.txt
File containes 64 bytes
Encryption time: 35 us
Decryption time: 5 us
sshsv192:Prob2 s1260066[73]$ ./tempdes ./data/test_64.txt
File containes 64 bytes
Encryption time: 19 us
Decryption time: 2 us
sshsv192:Prob2 s1260066[74]$ ./tempdes ./data/test_64.txt
File containes 64 bytes
Encryption time: 15 us
Decryption time: 2 us
sshsv192:Prob2 s1260066[75]$ ./tempdes ./data/test_64.txt
File containes 64 bytes
Encryption time: 15 us
Decryption time: 2 us
sshsv192:Prob2 s1260066[76]$ ./tempdes ./data/test_64.txt
File containes 64 bytes
Encryption time: 35 us
Decryption time: 4 us
```

```
sshsv192:Prob2 s1260066[77]$ ./tempdes ./data/test_512.txt
File containes 512 bytes
Encryption time: 52 us
Decryption time: 20 us
sshsv192:Prob2 s1260066[78]$ ./tempdes ./data/test_512.txt
File containes 512 bytes
Encryption time: 53 us
Decryption time: 19 us
sshsv192:Prob2 s1260066[79]$ ./tempdes ./data/test_512.txt
File containes 512 bytes
Encryption time: 34 us
Decryption time: 9 us
sshsv192:Prob2 s1260066[80]$ ./tempdes ./data/test_512.txt
File containes 512 bytes
Encryption time: 54 us
Decryption time: 19 us
sshsv192:Prob2 s1260066[81]$ ./tempdes ./data/test_512.txt
File containes 512 bytes
Encryption time: 52 us
Decryption time: 20 us
```

```
sshsv192:Prob2 s1260066[82]$ ./tempdes ./data/test_4096.txt
File containes 4096 bytes
Encryption time: 197 us
Decryption time: 146 us
sshsv192:Prob2 s1260066[83]$ ./tempdes ./data/test_4096.txt
File containes 4096 bytes
Encryption time: 170 us
Decryption time: 144 us
sshsv192:Prob2 s1260066[84]$ ./tempdes ./data/test_4096.txt
File containes 4096 bytes
Encryption time: 200 us
Decryption time: 146 us
sshsv192:Prob2 s1260066[85]$ ./tempdes ./data/test_4096.txt
File containes 4096 bytes
Encryption time: 200 us
Decryption time: 145 us
sshsv192:Prob2 s1260066[86]$ ./tempdes ./data/test_4096.txt
File containes 4096 bytes
Encryption time: 92 us
Decryption time: 67 us
```

```
sshsv192:Prob2 s1260066[87]$ ./tempdes ./data/test_32768.txt
File containes 32768 bytes
Encryption time: 1323 us
Decryption time: 1144 us
sshsv192:Prob2 s1260066[88]$ ./tempdes ./data/test_32768.txt
File containes 32768 bytes
Encryption time: 624 us
Decryption time: 529 us
sshsv192:Prob2 s1260066[89]$ ./tempdes ./data/test_32768.txt
File containes 32768 bytes
Encryption time: 646 us
Decryption time: 535 us
sshsv192:Prob2 s1260066[90]$ ./tempdes ./data/test_32768.txt
File containes 32768 bytes
Encryption time: 1419 us
Decryption time: 1188 us
sshsv192:Prob2 s1260066[91]$ ./tempdes ./data/test_32768.txt
File containes 32768 bytes
Encryption time: 616 us
Decryption time: 528 us
```

```
sshsv192:Prob2 s1260066[92]$ ./tempdes ./data/test_262144.txt
File containes 262144 bytes
Encryption time: 9193 us
Decryption time: 4219 us
sshsv192:Prob2 s1260066[93]$ ./tempdes ./data/test_262144.txt
File containes 262144 bytes
Encryption time: 8822 us
Decryption time: 4213 us
sshsv192:Prob2 s1260066[94]$ ./tempdes ./data/test_262144.txt
File containes 262144 bytes
Encryption time: 8544 us
Decryption time: 4200 us
sshsv192:Prob2 s1260066[95]$ ./tempdes ./data/test_262144.txt
File containes 262144 bytes
Encryption time: 9525 us
Decryption time: 4219 us
sshsv192:Prob2 s1260066[96]$ ./tempdes ./data/test_262144.txt
File containes 262144 bytes
Encryption time: 5451 us
Decryption time: 4213 us
```

```
sshsv192:Prob2 s1260066[97]$ ./tempdes ./data/test_2047512.txt
File containes 2047512 bytes
Encryption time: 58338 us
Decryption time: 32897 us
sshsv192:Prob2 s1260066[98]$ ./tempdes ./data/test_2047512.txt
File containes 2047512 bytes
Encryption time: 37720 us
Decryption time: 32883 us
sshsv192:Prob2 s1260066[99]$ ./tempdes ./data/test_2047512.txt
File containes 2047512 bytes
Encryption time: 37556 us
Decryption time: 32897 us
sshsv192:Prob2 s1260066[100]$ ./tempdes ./data/test_2047512.txt
File containes 2047512 bytes
Encryption time: 37592 us
Decryption time: 32953 us
sshsv192:Prob2 s1260066[101]$ ./tempdes ./data/test_2047512.txt
File containes 2047512 bytes
Encryption time: 37799 us
Decryption time: 33449 us
```

$ ./temprsa ./data/test_*.txt

```
sshsv192:Prob2 s1260066[110]$ ./temprsa ./data/test_8.txt
File containes 8 bytes
Encryption time: 169 us
Decryption time: 5621 us
sshsv192:Prob2 s1260066[111]$ ./temprsa ./data/test_8.txt
File containes 8 bytes
Encryption time: 168 us
Decryption time: 5526 us
sshsv192:Prob2 s1260066[112]$ ./temprsa ./data/test_8.txt
File containes 8 bytes
Encryption time: 169 us
Decryption time: 5456 us
sshsv192:Prob2 s1260066[113]$ ./temprsa ./data/test_8.txt
File containes 8 bytes
Encryption time: 157 us
Decryption time: 5524 us
sshsv192:Prob2 s1260066[114]$ ./temprsa ./data/test_8.txt
File containes 8 bytes
Encryption time: 137 us
Decryption time: 4407 us
```

```
sshsv192:Prob2 s1260066[115]$ ./temprsa ./data/test_64.txt
File containes 64 bytes
Encryption time: 121 us
Decryption time: 4178 us
sshsv192:Prob2 s1260066[116]$ ./temprsa ./data/test_64.txt
File containes 64 bytes
Encryption time: 120 us
Decryption time: 4179 us
sshsv192:Prob2 s1260066[117]$ ./temprsa ./data/test_64.txt
File containes 64 bytes
Encryption time: 129 us
Decryption time: 4478 us
sshsv192:Prob2 s1260066[118]$ ./temprsa ./data/test_64.txt
File containes 64 bytes
Encryption time: 155 us
Decryption time: 5436 us
sshsv192:Prob2 s1260066[119]$ ./temprsa ./data/test_64.txt
File containes 64 bytes
Encryption time: 156 us
Decryption time: 5475 us
```

```
sshsv192:Prob2 s1260066[120]$ ./temprsa ./data/test_512.txt
File containes 512 bytes
Encryption time: 12 us
Decryption time: 9 us
sshsv192:Prob2 s1260066[121]$ ./temprsa ./data/test_512.txt
File containes 512 bytes
Encryption time: 10 us
Decryption time: 8 us
sshsv192:Prob2 s1260066[122]$ ./temprsa ./data/test_512.txt
File containes 512 bytes
Encryption time: 10 us
Decryption time: 7 us
sshsv192:Prob2 s1260066[123]$ ./temprsa ./data/test_512.txt
File containes 512 bytes
Encryption time: 9 us
Decryption time: 23 us
sshsv192:Prob2 s1260066[124]$ ./temprsa ./data/test_512.txt
File containes 512 bytes
Encryption time: 10 us
Decryption time: 7 us
```

```
sshsv192:Prob2 s1260066[125]$ ./temprsa ./data/test_4096.txt
File containes 4096 bytes
Encryption time: 9 us
Decryption time: 8 us
sshsv192:Prob2 s1260066[126]$ ./temprsa ./data/test_4096.txt
File containes 4096 bytes
Encryption time: 12 us
Decryption time: 9 us
sshsv192:Prob2 s1260066[127]$ ./temprsa ./data/test_4096.txt
File containes 4096 bytes
Encryption time: 12 us
Decryption time: 9 us
sshsv192:Prob2 s1260066[128]$ ./temprsa ./data/test_4096.txt
File containes 4096 bytes
Encryption time: 10 us
Decryption time: 8 us
sshsv192:Prob2 s1260066[129]$ ./temprsa ./data/test_4096.txt
File containes 4096 bytes
Encryption time: 11 us
Decryption time: 9 us
```

```
sshsv192:Prob2 s1260066[130]$ ./temprsa ./data/test_32768.txt
File containes 32768 bytes
Encryption time: 11 us
Decryption time: 8 us
sshsv192:Prob2 s1260066[131]$ ./temprsa ./data/test_32768.txt
File containes 32768 bytes
Encryption time: 8 us
Decryption time: 23 us
sshsv192:Prob2 s1260066[132]$ ./temprsa ./data/test_32768.txt
File containes 32768 bytes
Encryption time: 9 us
Decryption time: 23 us
sshsv192:Prob2 s1260066[133]$ ./temprsa ./data/test_32768.txt
File containes 32768 bytes
Encryption time: 12 us
Decryption time: 9 us
sshsv192:Prob2 s1260066[134]$ ./temprsa ./data/test_32768.txt
File containes 32768 bytes
Encryption time: 9 us
Decryption time: 23 us
```

```
sshsv192:Prob2 s1260066[136]$ ./temprsa ./data/test_262144.txt
File containes 262144 bytes
Encryption time: 11 us
Decryption time: 9 us
sshsv192:Prob2 s1260066[137]$ ./temprsa ./data/test_262144.txt
File containes 262144 bytes
Encryption time: 9 us
Decryption time: 8 us
sshsv192:Prob2 s1260066[138]$ ./temprsa ./data/test_262144.txt
File containes 262144 bytes
Encryption time: 5 us
Decryption time: 4 us
sshsv192:Prob2 s1260066[139]$ ./temprsa ./data/test_262144.txt
File containes 262144 bytes
Encryption time: 11 us
Decryption time: 15 us
sshsv192:Prob2 s1260066[140]$ ./temprsa ./data/test_262144.txt
File containes 262144 bytes
Encryption time: 6 us
Decryption time: 4 us
```

```
sshsv192:Prob2 s1260066[141]$ ./temprsa ./data/test_2047512.txt
File containes 2047512 bytes
Encryption time: 11 us
Decryption time: 19 us
sshsv192:Prob2 s1260066[142]$ ./temprsa ./data/test_2047512.txt
File containes 2047512 bytes
Encryption time: 11 us
Decryption time: 9 us
sshsv192:Prob2 s1260066[143]$ ./temprsa ./data/test_2047512.txt
File containes 2047512 bytes
Encryption time: 11 us
Decryption time: 10 us
sshsv192:Prob2 s1260066[144]$ ./temprsa ./data/test_2047512.txt
File containes 2047512 bytes
Encryption time: 11 us
Decryption time: 9 us
sshsv192:Prob2 s1260066[145]$ ./temprsa ./data/test_2047512.txt
File containes 2047512 bytes
Encryption time: 11 us
Decryption time: 9 us
```

$ ./tempsha1 ./data/test_*.txt

```
sshsv192:Prob2 s1260066[160]$ ./tempsha1 ./data/test_64.txt
File containes 64 bytes
sha1 = a07705f4fe324ceda80f53913746a4b5713494ad
Encryption time: 459 us
sshsv192:Prob2 s1260066[161]$ ./tempsha1 ./data/test_64.txt
File containes 64 bytes
sha1 = a07705f4fe324ceda80f53913746a4b5713494ad
Encryption time: 345 us
sshsv192:Prob2 s1260066[162]$ ./tempsha1 ./data/test_64.txt
File containes 64 bytes
sha1 = a07705f4fe324ceda80f53913746a4b5713494ad
Encryption time: 366 us
sshsv192:Prob2 s1260066[163]$ ./tempsha1 ./data/test_64.txt
File containes 64 bytes
sha1 = a07705f4fe324ceda80f53913746a4b5713494ad
Encryption time: 362 us
sshsv192:Prob2 s1260066[164]$ ./tempsha1 ./data/test_64.txt
File containes 64 bytes
sha1 = a07705f4fe324ceda80f53913746a4b5713494ad
Encryption time: 369 us
```

```
sshsv192:Prob2 s1260066[155]$ ./tempsha1 ./data/test_8.txt
File containes 8 bytes
sha1 = 5873c0c700cf0599a82cc2c4800c1af1cc53dd85
Encryption time: 401 us
sshsv192:Prob2 s1260066[156]$ ./tempsha1 ./data/test_8.txt
File containes 8 bytes
sha1 = 5873c0c700cf0599a82cc2c4800c1af1cc53dd85
Encryption time: 463 us
sshsv192:Prob2 s1260066[157]$ ./tempsha1 ./data/test_8.txt
File containes 8 bytes
sha1 = 5873c0c700cf0599a82cc2c4800c1af1cc53dd85
Encryption time: 604 us
sshsv192:Prob2 s1260066[158]$ ./tempsha1 ./data/test_8.txt
File containes 8 bytes
sha1 = 5873c0c700cf0599a82cc2c4800c1af1cc53dd85
Encryption time: 440 us
sshsv192:Prob2 s1260066[159]$ ./tempsha1 ./data/test_8.txt
File containes 8 bytes
sha1 = 5873c0c700cf0599a82cc2c4800c1af1cc53dd85
Encryption time: 348 us
```

```
sshsv192:Prob2 s1260066[165]$ ./tempsha1 ./data/test_512.txt
File containes 512 bytes
sha1 = fd3bfc0c8067eca1bfd5f03a49774a8e076a660f
Encryption time: 639 us
sshsv192:Prob2 s1260066[166]$ ./tempsha1 ./data/test_512.txt
File containes 512 bytes
sha1 = fd3bfc0c8067eca1bfd5f03a49774a8e076a660f
Encryption time: 500 us
sshsv192:Prob2 s1260066[167]$ ./tempsha1 ./data/test_512.txt
File containes 512 bytes
sha1 = fd3bfc0c8067eca1bfd5f03a49774a8e076a660f
Encryption time: 371 us
sshsv192:Prob2 s1260066[168]$ ./tempsha1 ./data/test_512.txt
File containes 512 bytes
sha1 = fd3bfc0c8067eca1bfd5f03a49774a8e076a660f
Encryption time: 463 us
sshsv192:Prob2 s1260066[169]$ ./tempsha1 ./data/test_512.txt
File containes 512 bytes
sha1 = fd3bfc0c8067eca1bfd5f03a49774a8e076a660f
Encryption time: 370 us
```

```
sshsv192:Prob2 s1260066[170]$ ./tempsha1 ./data/test_4096.txt
File containes 4096 bytes
sha1 = 2844d852054cdad1e5767e8c89d16b34dfc910dc
Encryption time: 361 us
sshsv192:Prob2 s1260066[171]$ ./tempsha1 ./data/test_4096.txt
File containes 4096 bytes
sha1 = 2844d852054cdad1e5767e8c89d16b34dfc910dc
Encryption time: 504 us
sshsv192:Prob2 s1260066[172]$ ./tempsha1 ./data/test_4096.txt
File containes 4096 bytes
sha1 = 2844d852054cdad1e5767e8c89d16b34dfc910dc
Encryption time: 506 us
sshsv192:Prob2 s1260066[173]$ ./tempsha1 ./data/test_4096.txt
File containes 4096 bytes
sha1 = 2844d852054cdad1e5767e8c89d16b34dfc910dc
Encryption time: 478 us
sshsv192:Prob2 s1260066[174]$ ./tempsha1 ./data/test_4096.txt
File containes 4096 bytes
sha1 = 2844d852054cdad1e5767e8c89d16b34dfc910dc
Encryption time: 375 us
```

```
sshsv192:Prob2 s1260066[175]$ ./tempsha1 ./data/test_32768.txt
File containes 32768 bytes
sha1 = 72fa141ace53668bef49bba86e31fe5148153f13
Encryption time: 593 us
sshsv192:Prob2 s1260066[176]$ ./tempsha1 ./data/test_32768.txt
File containes 32768 bytes
sha1 = 72fa141ace53668bef49bba86e31fe5148153f13
Encryption time: 801 us
sshsv192:Prob2 s1260066[177]$ ./tempsha1 ./data/test_32768.txt
File containes 32768 bytes
sha1 = 72fa141ace53668bef49bba86e31fe5148153f13
Encryption time: 584 us
sshsv192:Prob2 s1260066[178]$ ./tempsha1 ./data/test_32768.txt
File containes 32768 bytes
sha1 = 72fa141ace53668bef49bba86e31fe5148153f13
Encryption time: 515 us
sshsv192:Prob2 s1260066[179]$ ./tempsha1 ./data/test_32768.txt
File containes 32768 bytes
sha1 = 72fa141ace53668bef49bba86e31fe5148153f13
Encryption time: 852 us
```

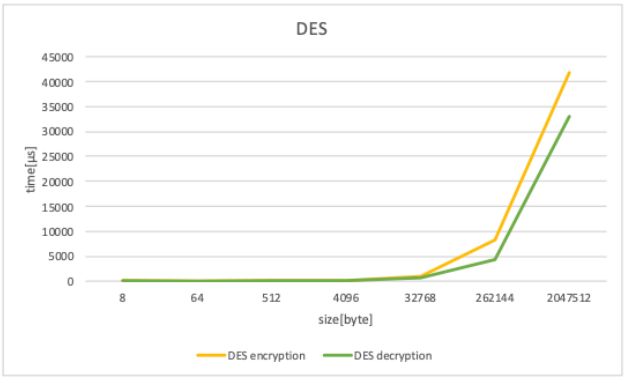
```
sshsv192:Prob2 s1260066[180]$ ./tempsha1 ./data/test_262144.txt
File containes 262144 bytes
sha1 = d355b8e3c4da926638e060a42f2c1a7e053a12b0
Encryption time: 1415 us
sshsv192:Prob2 s1260066[181]$ ./tempsha1 ./data/test_262144.txt
File containes 262144 bytes
sha1 = d355b8e3c4da926638e060a42f2c1a7e053a12b0
Encryption time: 1408 us
sshsv192:Prob2 s1260066[182]$ ./tempsha1 ./data/test_262144.txt
File containes 262144 bytes
sha1 = d355b8e3c4da926638e060a42f2c1a7e053a12b0
Encryption time: 1505 us
sshsv192:Prob2 s1260066[183]$ ./tempsha1 ./data/test_262144.txt
File containes 262144 bytes
sha1 = d355b8e3c4da926638e060a42f2c1a7e053a12b0
Encryption time: 867 us
sshsv192:Prob2 s1260066[184]$ ./tempsha1 ./data/test_262144.txt
File containes 262144 bytes
sha1 = d355b8e3c4da926638e060a42f2c1a7e053a12b0
Encryption time: 1402 us
```

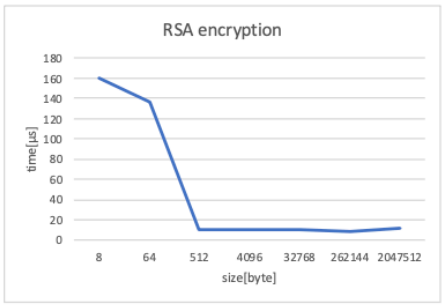
```
sshsv192:Prob2 s1260066[185]$ ./tempsha1 ./data/test_2047512.txt
File containes 2047512 bytes
sha1 = 35ad7334c481e36dc14bfa21bfbc9b9cd7a606f8
Encryption time: 3579 us
sshsv192:Prob2 s1260066[186]$ ./tempsha1 ./data/test_2047512.txt
File containes 2047512 bytes
sha1 = 35ad7334c481e36dc14bfa21bfbc9b9cd7a606f8
Encryption time: 3866 us
sshsv192:Prob2 s1260066[187]$ ./tempsha1 ./data/test_2047512.txt
File containes 2047512 bytes
sha1 = 35ad7334c481e36dc14bfa21bfbc9b9cd7a606f8
Encryption time: 3571 us
sshsv192:Prob2 s1260066[188]$ ./tempsha1 ./data/test_2047512.txt
File containes 2047512 bytes
sha1 = 35ad7334c481e36dc14bfa21bfbc9b9cd7a606f8
Encryption time: 7478 us
sshsv192:Prob2 s1260066[189]$ ./tempsha1 ./data/test_2047512.txt
File containes 2047512 bytes
sha1 = 35ad7334c481e36dc14bfa21bfbc9b9cd7a606f8
Encryption time: 7443 us
```

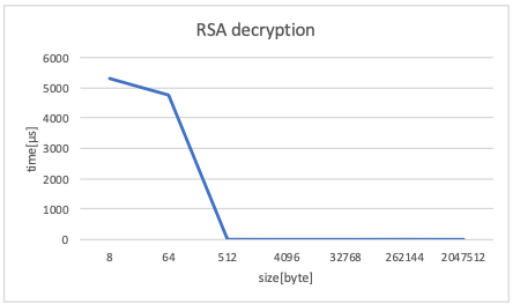
(2) Q&A

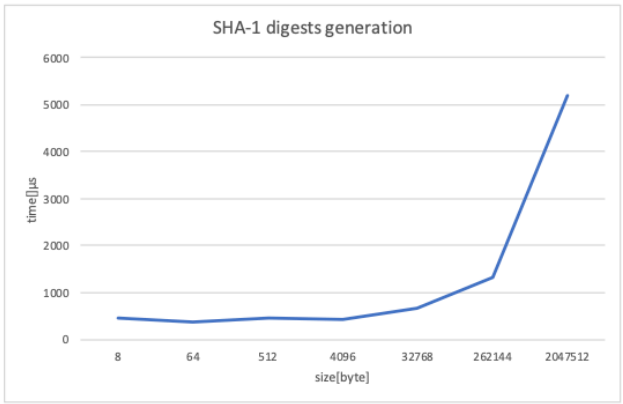
1. (a)-(d)

Result	8	64	512	4096	32768	262144	2047512
DES encryption	29.6	23.8	49	171.8	925.6	8307	41801
DES decryption	3.2	3	17.4	129.6	784.8	4212.8	33015.8
RSA encryption	160	136.2	10.2	10.8	9.8	8.4	11
RSA decryption	5306.8	4749.2	8	8.6	17.2	8	11.2
SHA-1 digests g	451.2	380.2	468.6	444.8	669	1319.4	5187.4









2.(e)-(g)

(e) Compare DES encryption and RSA encryption. Explain your observations. (10 points)

With DES, the encryption process takes longer as the number of bytes increases. With a small number of bytes, RSA takes longer to decrypt, but less time to encrypt.

(f) Compare DES encryption and SHA-1 digest generation. Explain your observations.

SHA-1 can encrypt and encrypt plain text, but not decrypt. DES can be encrypted and decrypted.

Also, DES contains symbols, but SHA-1 contains non-symbol alphabets and numbers.

(g) CompareRSAencryptionanddecryptiontimes.Canyouexplainyourobservations?

The execution time of RSA encryption and the execution time of decryption are relatively the same. The smaller the number of bytes for encryption / decryption, the longer the decryption time.