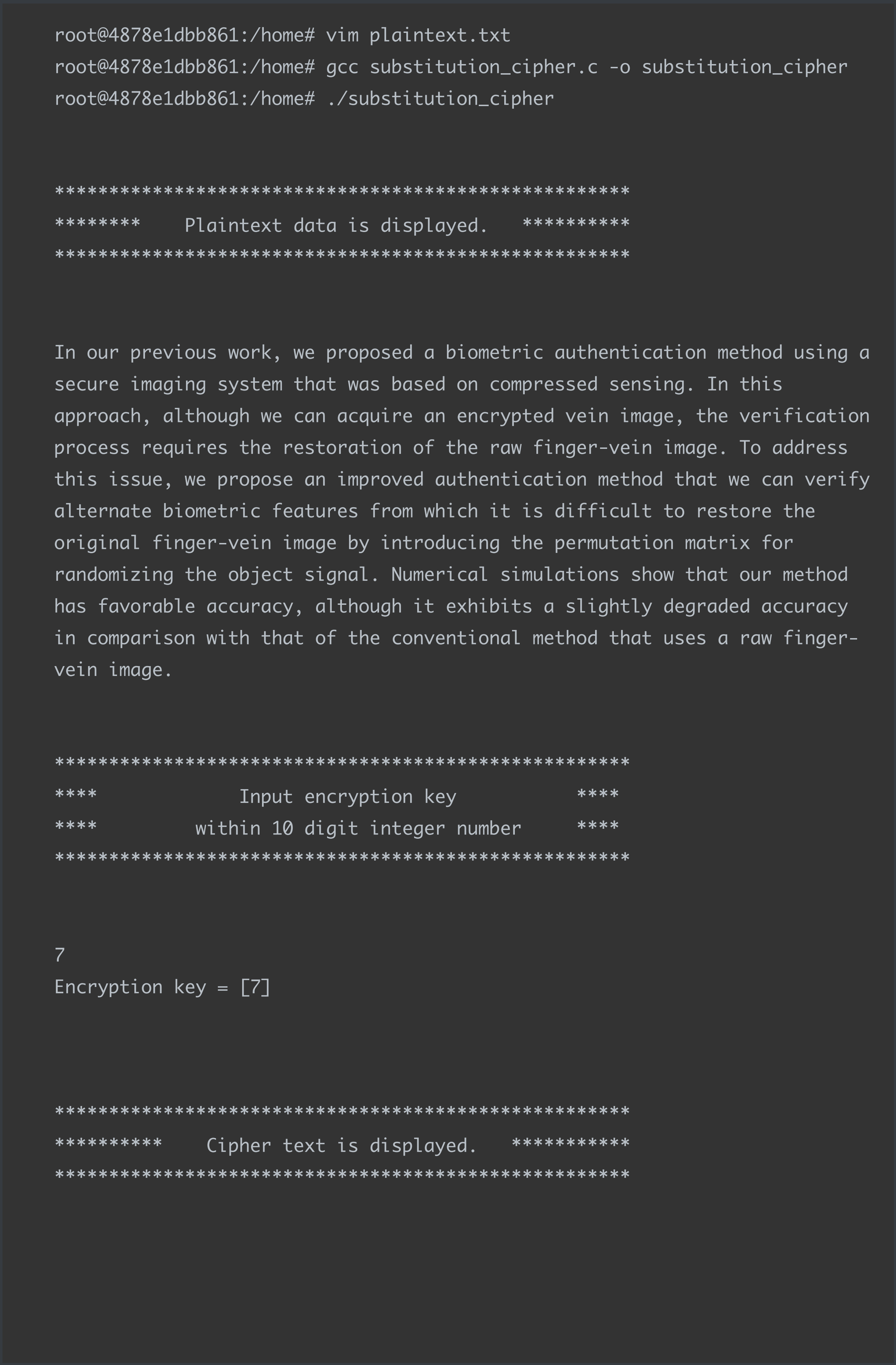
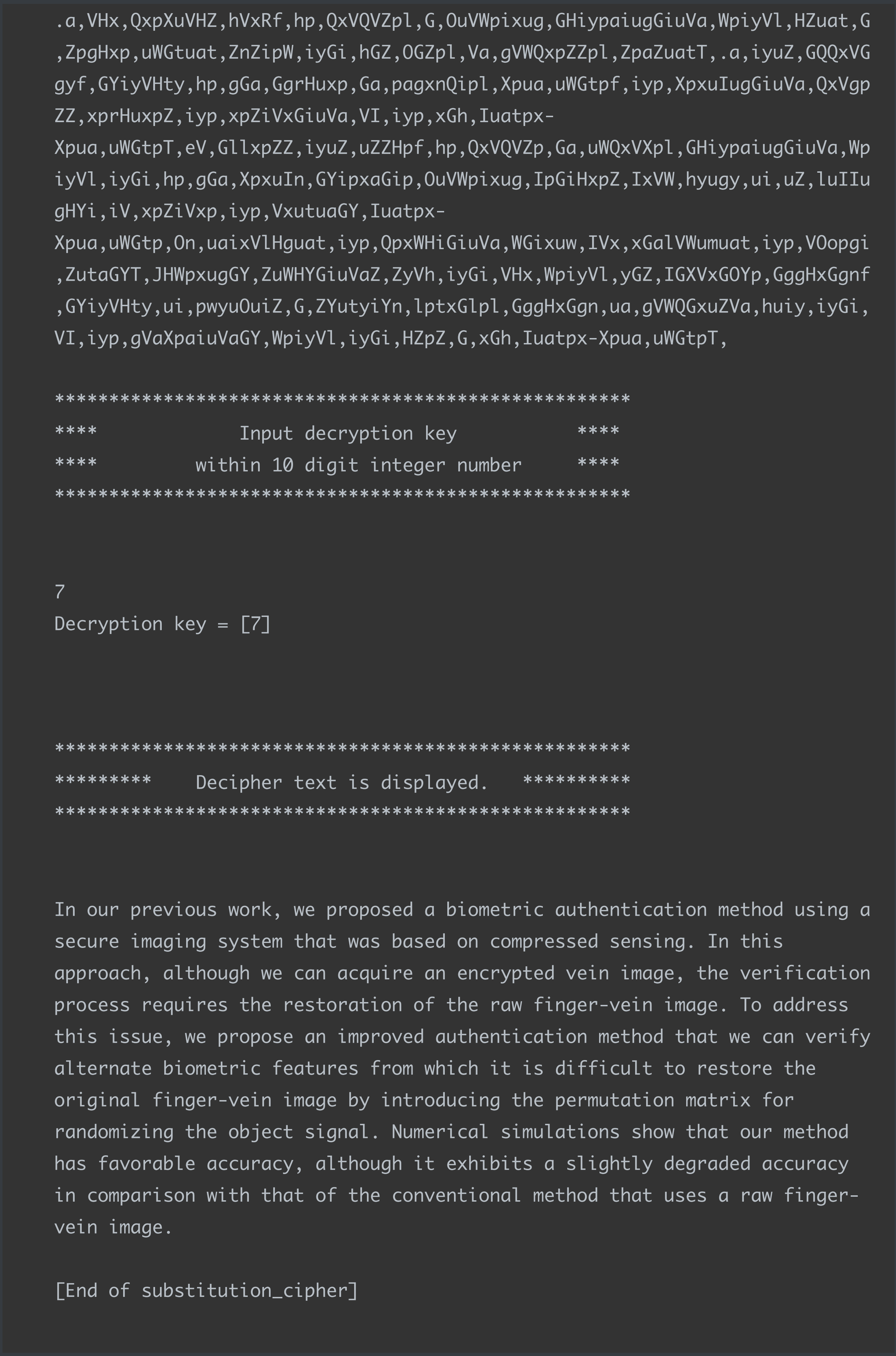
5-1

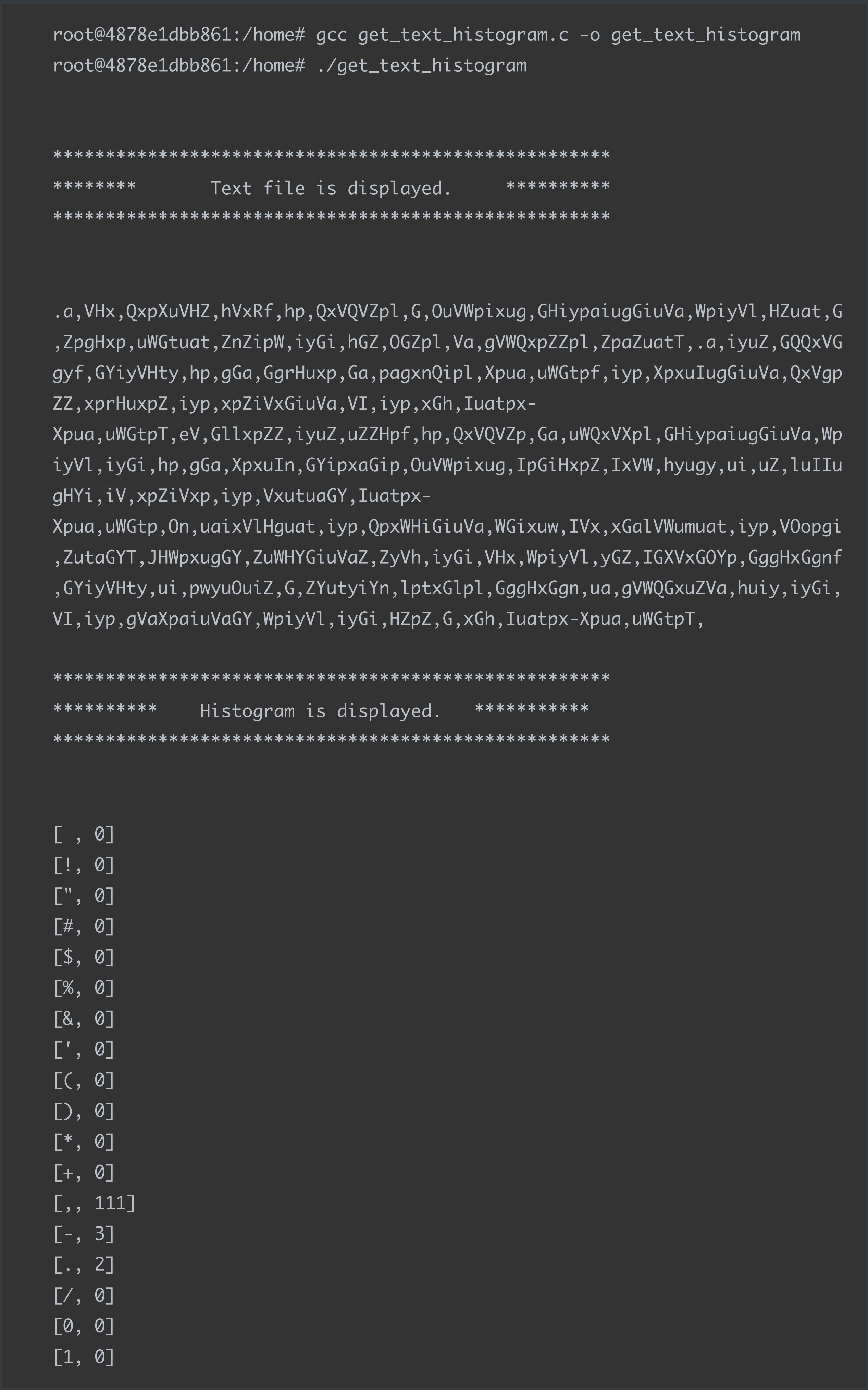


```
root@4878e1dbb861:/home# vim plaintext.txt
root@4878e1dbb861:/home# gcc substitution_cipher.c -o substitution_cipher
root@4878e1dbb861:/home# ./substitution_cipher


*****************************************************
********    Plaintext data is displayed.   **********
*****************************************************



In our previous work, we proposed a biometric authentication method using a
secure imaging system that was based on compressed sensing. In this
approach, although we can acquire an encrypted vein image, the verification
process requires the restoration of the raw finger-vein image. To address
this issue, we propose an improved authentication method that we can verify
alternate biometric features from which it is difficult to restore the
original finger-vein image by introducing the permutation matrix for
randomizing the object signal. Numerical simulations show that our method
has favorable accuracy, although it exhibits a slightly degraded accuracy
in comparison with that of the conventional method that uses a raw finger-
vein image.


*****************************************************
****             Input encryption key           ****
****         within 10 digit integer number     ****
*****************************************************



7
Encryption key = [7]




*****************************************************
**********    Cipher text is displayed.   ***********
*****************************************************
```



```
.a,VHx,QxpXuVHZ,hVxRf,hp,QxVQVZpl,G,OuVWpixug,GHiypaiugGiuVa,WpiyVl,HZuat,G
,ZpgHxp,uWGtuat,ZnZipW,iyGi,hGZ,OGZpl,Va,gVWQxpZZpl,ZpaZuatT,.a,iyuZ,GQQxVG
gyf,GYiyVHty,hp,gGa,GgrHuxp,Ga,pagxnQipl,Xpua,uWGtpf,iyp,XpxuIugGiuVa,QxVgp
ZZ,xprHuxpZ,iyp,xpZiVxGiuVa,VI,iyp,xGh,Iuatpx-
Xpua,uWGtpT,eV,GllxpZZ,iyuZ,uZZHpf,hp,QxVQVZp,Ga,uWQxVXpl,GHiypaiugGiuVa,Wp
iyVl,iyGi,hp,gGa,XpxuIn,GYipxaGip,OuVWpixug,IpGiHxpZ,IxVW,hyugy,ui,uZ,luIIu
gHYi,iV,xpZiVxp,iyp,VxutuaGY,Iuatpx-
Xpua,uWGtp,On,uaixVlHguat,iyp,QpxWHiGiuVa,WGixuw,IVx,xGalVWumuat,iyp,VOopgi
,ZutaGYT,JHWpxugGY,ZuWHYGiuVaZ,ZyVh,iyGi,VHx,WpiyVl,yGZ,IGXVxGOYp,GggHxGgnf
,GYiyVHty,ui,pwyuOuiZ,G,ZYutyiYn,lptxGlpl,GggHxGgn,ua,gVWQGxuZVa,huiy,iyGi,
VI,iyp,gVaXpaiuVaGY,WpiyVl,iyGi,HZpZ,G,xGh,Iuatpx-Xpua,uWGtpT,

*****************************************************
****             Input decryption key           ****
****         within 10 digit integer number     ****
*****************************************************



7
Decryption key = [7]




*****************************************************
*********    Decipher text is displayed.   **********
*****************************************************



In our previous work, we proposed a biometric authentication method using a
secure imaging system that was based on compressed sensing. In this
approach, although we can acquire an encrypted vein image, the verification
process requires the restoration of the raw finger-vein image. To address
this issue, we propose an improved authentication method that we can verify
alternate biometric features from which it is difficult to restore the
original finger-vein image by introducing the permutation matrix for
randomizing the object signal. Numerical simulations show that our method
has favorable accuracy, although it exhibits a slightly degraded accuracy
in comparison with that of the conventional method that uses a raw finger-
vein image.

[End of substitution_cipher]
```

5-2



```
root@4878e1dbb861:/home# gcc get_text_histogram.c -o get_text_histogram
root@4878e1dbb861:/home# ./get_text_histogram


*****************************************************
********       Text file is displayed.     **********
*****************************************************


.a,VHx,QxpXuVHZ,hVxRf,hp,QxVQVZpl,G,OuVWpixug,GHiypaiugGiuVa,WpiyVl,HZuat,G
,ZpgHxp,uWGtuat,ZnZipW,iyGi,hGZ,OGZpl,Va,gVWQxpZZpl,ZpaZuatT,.a,iyuZ,GQQxVG
gyf,GYiyVHty,hp,gGa,GgrHuxp,Ga,pagxnQipl,Xpua,uWGtpf,iyp,XpxuIugGiuVa,QxVgp
ZZ,xprHuxpZ,iyp,xpZiVxGiuVa,VI,iyp,xGh,Iuatpx-
Xpua,uWGtpT,eV,GllxpZZ,iyuZ,uZZHpf,hp,QxVQVZp,Ga,uWQxVXpl,GHiypaiugGiuVa,Wp
iyVl,iyGi,hp,gGa,XpxuIn,GYipxaGip,OuVWpixug,IpGiHxpZ,IxVW,hyugy,ui,uZ,luIIu
gHYi,iV,xpZiVxp,iyp,VxutuaGY,Iuatpx-
Xpua,uWGtp,On,uaixVlHguat,iyp,QpxWHiGiuVa,WGixuw,IVx,xGalVWumuat,iyp,VOopgi
,ZutaGYT,JHWpxugGY,ZuWHYGiuVaZ,ZyVh,iyGi,VHx,WpiyVl,yGZ,IGXVxGOYp,GggHxGgnf
,GYiyVHty,ui,pwyuOuiZ,G,ZYutyiYn,lptxGlpl,GggHxGgn,ua,gVWQGxuZVa,huiy,iyGi,
VI,iyp,gVaXpaiuVaGY,WpiyVl,iyGi,HZpZ,G,xGh,Iuatpx-Xpua,uWGtpT,

*****************************************************
**********    Histogram is displayed.   ***********
*****************************************************


[ , 0]
[!, 0]
[", 0]
[#, 0]
[$, 0]
[%, 0]
[&, 0]
[', 0]
[(, 0]
[), 0]
[*, 0]
[+, 0]
[,, 111]
[-, 3]
[., 2]
[/, 0]
[0, 0]
[1, 0]
```

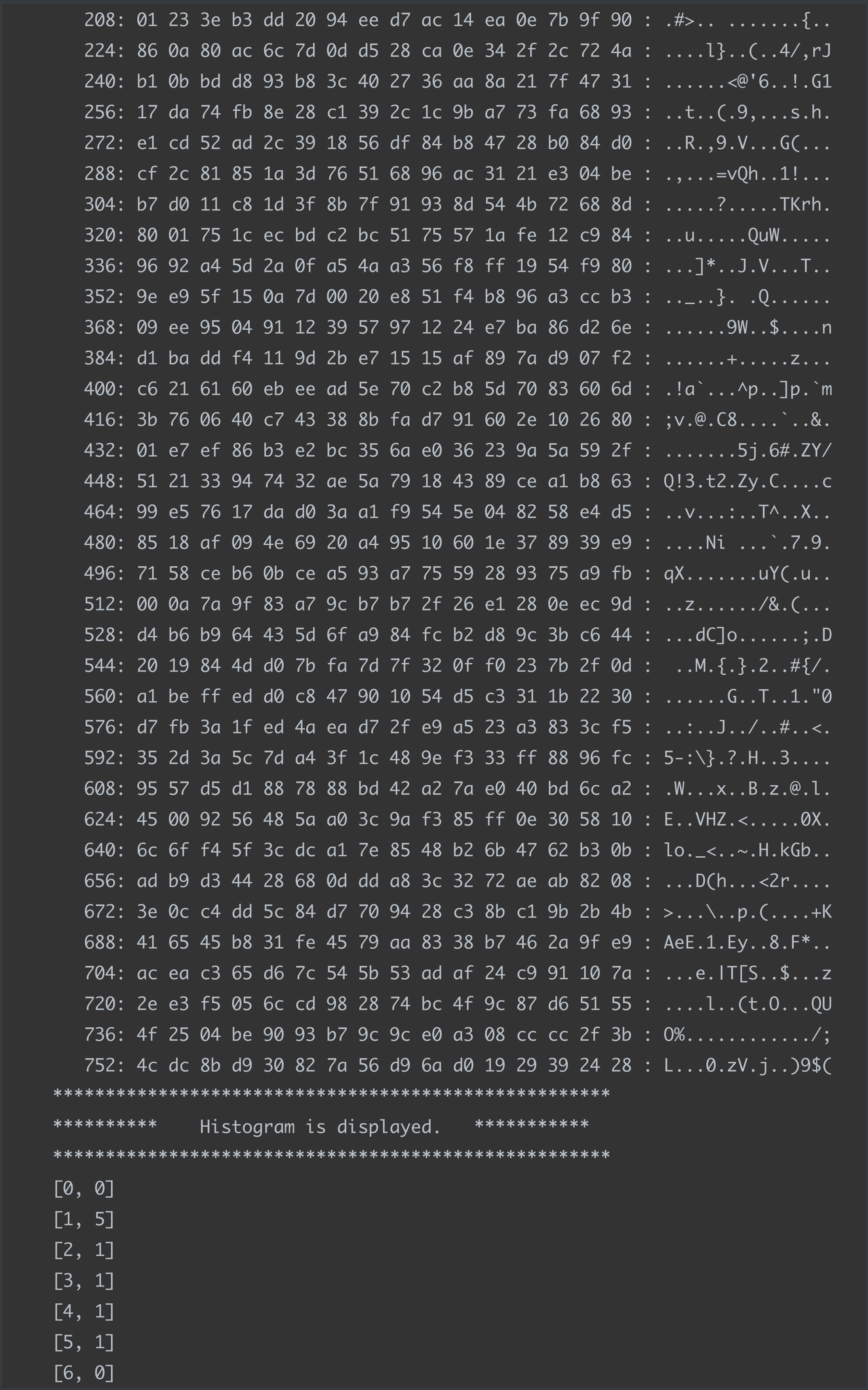
```
    [2, 0]
    [3, 0]
    [4, 0]
    [5, 0]
    [6, 0]
    [7, 0]
    [8, 0]
    [9, 0]
    [:, 0]
    [;, 0]
    [<, 0]
    [=, 0]
    [>, 0]
    [?, 0]
    [@, 0]
    [A, 0]
    [B, 0]
    [C, 0]
    [D, 0]
    [E, 0]
    [F, 0]
    [G, 54]
    [H, 21]
    [I, 13]
    [J, 1]
    [K, 0]
    [L, 0]
    [M, 0]
    [N, 0]
    [O, 7]
    [P, 0]
    [Q, 13]
    [R, 1]
    [S, 0]
    [T, 4]
    [U, 0]
    [V, 45]
    [W, 21]
    [X, 10]
    [Y, 12]
    [Z, 36]
    [[, 0]
    [\, 0]
    [], 0]
    [^, 0]
    [_, 0]
    [`, 0]
    [a, 39]
    [b, 0]
    [c, 0]
    [d, 0]
    [e, 1]
    [f, 5]
    [g, 26]
    [h, 11]
    [i, 56]
    [j, 0]
    [k, 0]
    [l, 17]
    [m, 1]
    [n, 7]
    [o, 1]
    [p, 67]
    [q, 0]
    [r, 2]
    [s, 0]
    [t, 19]
    [u, 60]
    [v, 0]
    [w, 2]
    [x, 44]
    [y, 32]
    [z, 0]
    [{, 0]
    [|, 0]
    [}, 0]
    [~, 0]
    [, 0]
```

5-3

```
Tokyo Institute of Technology is a national research university located in
Greater Tokyo Area, Japan. Tokyo Tech is the largest institution for
higher education in Japan dedicated to science and technology, and is
generally considered to be one of the most prestigious universities in
Japan. Tokyo Techs main campus is located at Ookayama on the boundary of
Meguro and Ota, with its main entrance facing the Ookayama Station. Other
campuses are located in Suzukakedai and Tamachi. Tokyo Tech is organized
into six schools, within which there are over forty departments and
research centers. Tokyo Tech enrolled four thousands seven hundreds thirty
three undergraduates and one thousand four hundreds sixty four graduate
students for two thousands fifteen to two thousand sixteen. It employs
around one thousand and one hundred faculty members. The university has
been ranked second in two thousands eleven in the field of Engineering by
Scorenavi. In another ranking, Japanese prep school Kawaijuku ranked Tokyo
Tech as the fourth best, second or third best in former semester and first
in latter semester university in Japan. According to QS World University
Lankings, Tokyo Tech was ranked third in Japan and internationally ranked
twentieth in the field of Engineering and Technology, and fifty first in
Natural science in two thousands eleven. The university was ranked thirty
first worldwide according to Global University ranking and
fifty seventh in two thousands eleven according to QS World University
Lankings. It was also ranked thirty first worldwide according to the Global
University Lanking in two thousands eleven.
```

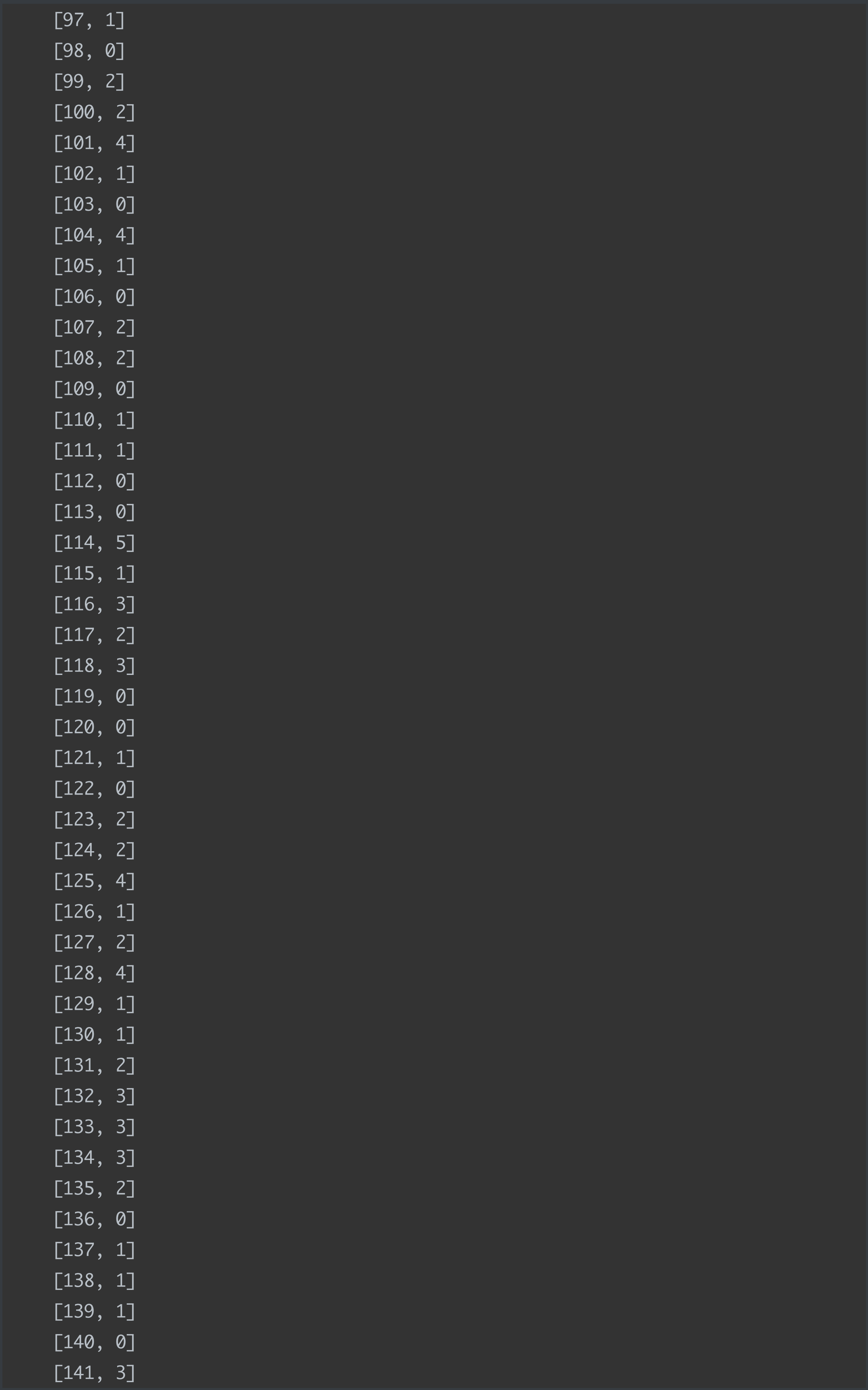
5-4

```
*****************************************************
********       Binary file is dumped.      **********
*****************************************************
     0: 53 61 6c 74 65 64 5f 5f 79 99 99 7b e2 b4 e3 46 : Salted__y..{...F
    16: e1 a8 3a e9 72 ac d1 b0 83 41 68 ee 72 03 d7 9e : ..:.r....Ah.r...
    32: f6 86 46 05 e8 a4 47 34 12 8d ac bb d0 7c a9 85 : ..F...G4.....|..
    48: 01 e4 99 7d af 4b c9 97 0d 5f 3f 1d 48 c0 59 53 : ...}.K..._?.H.YS
    64: 42 ee bc d4 a2 aa 5f f3 57 85 1c 18 6b c3 ea ce : B....._.W...k...
    80: 13 30 3e f5 15 1a 4d c9 69 51 dc 7c 0d 74 af 2d : .0>...M.iQ.|.t.-
    96: 6f 66 d0 09 c0 d3 1f ab fb 2f 26 41 65 97 3c 21 : of......./&Ae.<!
   112: 80 cd 9d 64 45 ea 47 01 10 f0 e6 26 02 c2 bc d4 : ...dE.G....&....
   128: 63 40 32 f1 19 3f 2c 65 63 50 bf a5 2a 1b fb f0 : c@2..?,ecP..*...
   144: 9c 4e c3 ba 18 f6 1a 87 65 ab 94 59 ba a6 24 de : .N......e..Y..$.
   160: 2b cc 52 4c a5 eb d8 76 c2 96 76 b0 11 7e 82 99 : +.RL...v..v..~..
   176: 89 96 9a db 1b 5b 6e bc 56 9f bb 87 5a 19 55 83 : .....[n.V...Z.U.
   192: f3 86 01 1a 7d 6b 94 72 c5 a4 b8 5c f0 d8 31 c7 : ....}k.r...\..1.
```



```
   208: 01 23 3e b3 dd 20 94 ee d7 ac 14 ea 0e 7b 9f 90 : .#>.. .......{..
   224: 86 0a 80 ac 6c 7d 0d d5 28 ca 0e 34 2f 2c 72 4a : ....l}..(..4/,rJ
   240: b1 0b bd d8 93 b8 3c 40 27 36 aa 8a 21 7f 47 31 : ......<@'6..!.G1
   256: 17 da 74 fb 8e 28 c1 39 2c 1c 9b a7 73 fa 68 93 : ..t..(.9,...s.h.
   272: e1 cd 52 ad 2c 39 18 56 df 84 b8 47 28 b0 84 d0 : ..R.,9.V...G(...
   288: cf 2c 81 85 1a 3d 76 51 68 96 ac 31 21 e3 04 be : .,...=vQh..1!...
   304: b7 d0 11 c8 1d 3f 8b 7f 91 93 8d 54 4b 72 68 8d : .....?.....TKrh.
   320: 80 01 75 1c ec bd c2 bc 51 75 57 1a fe 12 c9 84 : ..u.....QuW.....
   336: 96 92 a4 5d 2a 0f a5 4a a3 56 f8 ff 19 54 f9 80 : ...]*..J.V...T..
   352: 9e e9 5f 15 0a 7d 00 20 e8 51 f4 b8 96 a3 cc b3 : .._..}. .Q......
   368: 09 ee 95 04 91 12 39 57 97 12 24 e7 ba 86 d2 6e : ......9W..$....n
   384: d1 ba dd f4 11 9d 2b e7 15 15 af 89 7a d9 07 f2 : ......+.....z...
   400: c6 21 61 60 eb ee ad 5e 70 c2 b8 5d 70 83 60 6d : .!a`...^p..]p.`m
   416: 3b 76 06 40 c7 43 38 8b fa d7 91 60 2e 10 26 80 : ;v.@.C8....`..&.
   432: 01 e7 ef 86 b3 e2 bc 35 6a e0 36 23 9a 5a 59 2f : .......5j.6#.ZY/
   448: 51 21 33 94 74 32 ae 5a 79 18 43 89 ce a1 b8 63 : Q!3.t2.Zy.C....c
   464: 99 e5 76 17 da d0 3a a1 f9 54 5e 04 82 58 e4 d5 : ..v...:..T^..X..
   480: 85 18 af 09 4e 69 20 a4 95 10 60 1e 37 89 39 e9 : ....Ni ...`.7.9.
   496: 71 58 ce b6 0b ce a5 93 a7 75 59 28 93 75 a9 fb : qX.......uY(.u..
   512: 00 0a 7a 9f 83 a7 9c b7 b7 2f 26 e1 28 0e ec 9d : ..z....../&.(...
   528: d4 b6 b9 64 43 5d 6f a9 84 fc b2 d8 9c 3b c6 44 : ...dC]o......;.D
   544: 20 19 84 4d d0 7b fa 7d 7f 32 0f f0 23 7b 2f 0d :  ..M.{.}.2..#{/.
   560: a1 be ff ed d0 c8 47 90 10 54 d5 c3 31 1b 22 30 : ......G..T..1."0
   576: d7 fb 3a 1f ed 4a ea d7 2f e9 a5 23 a3 83 3c f5 : ..:..J../..#..<.
   592: 35 2d 3a 5c 7d a4 3f 1c 48 9e f3 33 ff 88 96 fc : 5-:\}.?.H..3....
   608: 95 57 d5 d1 88 78 88 bd 42 a2 7a e0 40 bd 6c a2 : .W...x..B.z.@.l.
   624: 45 00 92 56 48 5a a0 3c 9a f3 85 ff 0e 30 58 10 : E..VHZ.<.....0X.
   640: 6c 6f f4 5f 3c dc a1 7e 85 48 b2 6b 47 62 b3 0b : lo._<..~.H.kGb..
   656: ad b9 d3 44 28 68 0d dd a8 3c 32 72 ae ab 82 08 : ...D(h...<2r....
   672: 3e 0c c4 dd 5c 84 d7 70 94 28 c3 8b c1 9b 2b 4b : >...\..p.(....+K
   688: 41 65 45 b8 31 fe 45 79 aa 83 38 b7 46 2a 9f e9 : AeE.1.Ey..8.F*..
   704: ac ea c3 65 d6 7c 54 5b 53 ad af 24 c9 91 10 7a : ...e.|T[S..$...z
   720: 2e e3 f5 05 6c cd 98 28 74 bc 4f 9c 87 d6 51 55 : ....l..(t.O...QU
   736: 4f 25 04 be 90 93 b7 9c 9c e0 a3 08 cc cc 2f 3b : O%............/;
   752: 4c dc 8b d9 30 82 7a 56 d9 6a d0 19 29 39 24 28 : L...0.zV.j..)9$(
******************************************************
**********    Histogram is displayed.   ***********
******************************************************
[0, 0]
[1, 5]
[2, 1]
[3, 1]
[4, 1]
[5, 1]
[6, 0]
```

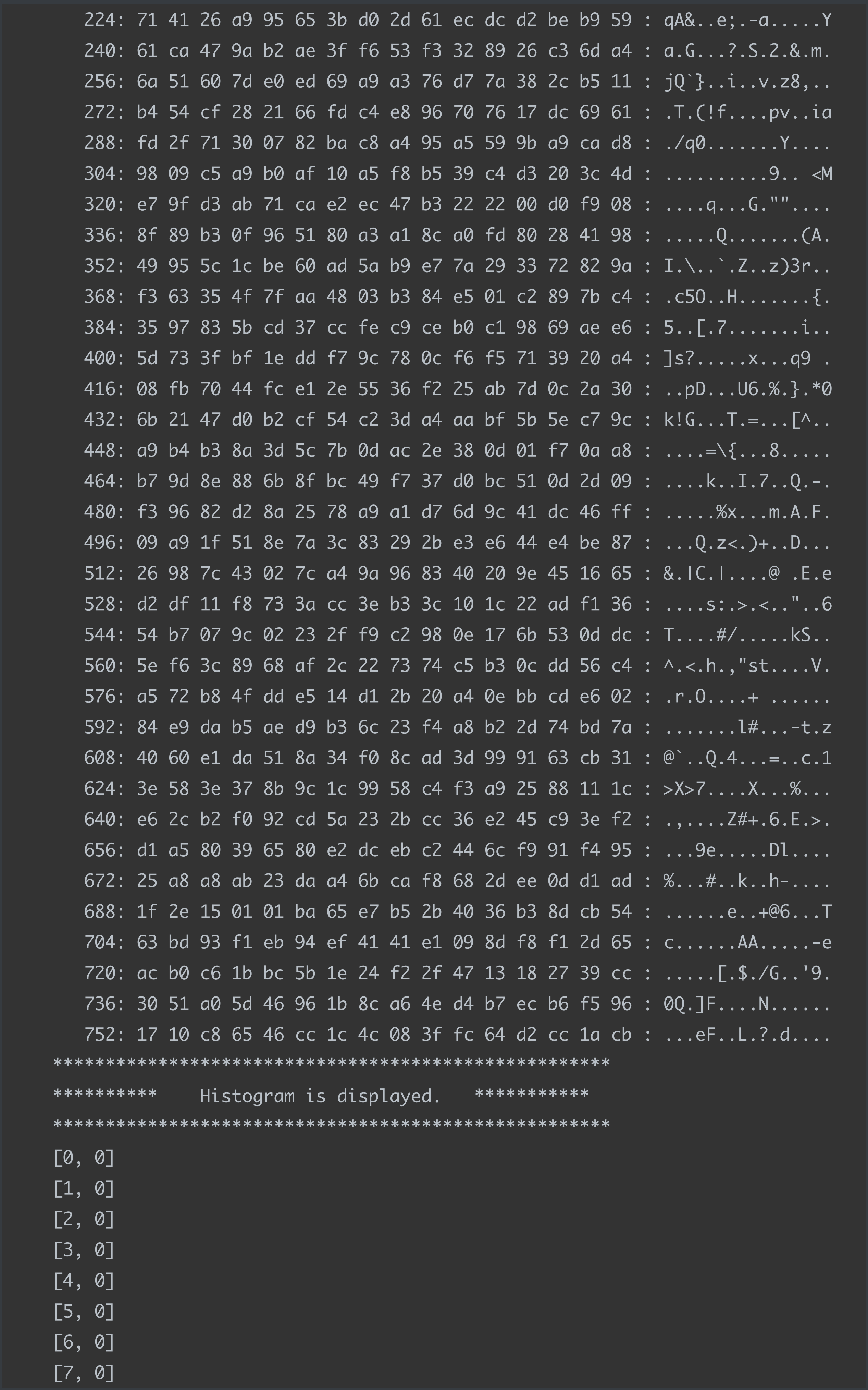
```
    [7, 0]
    [8, 0]
    [9, 1]
    [10, 2]
    [11, 1]
    [12, 0]
    [13, 3]
    [14, 2]
    [15, 1]
    [16, 1]
    [17, 2]
    [18, 2]
    [19, 1]
    [20, 1]
    [21, 2]
    [22, 0]
    [23, 1]
    [24, 3]
    [25, 3]
    [26, 5]
    [27, 2]
    [28, 3]
    [29, 2]
    [30, 0]
    [31, 1]
    [32, 1]
    [33, 3]
    [34, 0]
    [35, 1]
    [36, 1]
    [37, 0]
    [38, 2]
    [39, 1]
    [40, 3]
    [41, 0]
    [42, 2]
    [43, 1]
    [44, 5]
    [45, 1]
    [46, 0]
    [47, 2]
    [48, 1]
    [49, 3]
    [50, 1]
    [51, 0]
    [52, 2]
    [53, 0]
    [54, 1]
    [55, 0]
    [56, 0]
    [57, 2]
    [58, 1]
    [59, 0]
    [60, 2]
    [61, 1]
    [62, 2]
    [63, 3]
    [64, 2]
    [65, 2]
    [66, 1]
    [67, 0]
    [68, 0]
    [69, 1]
    [70, 2]
    [71, 4]
    [72, 1]
    [73, 0]
    [74, 2]
    [75, 2]
    [76, 1]
    [77, 1]
    [78, 1]
    [79, 0]
    [80, 1]
    [81, 3]
    [82, 2]
    [83, 2]
    [84, 2]
    [85, 1]
    [86, 3]
    [87, 2]
    [88, 0]
    [89, 2]
    [90, 1]
    [91, 1]
    [92, 1]
    [93, 1]
    [94, 0]
    [95, 5]
    [96, 0]
```



```
    [97, 1]
    [98, 0]
    [99, 2]
    [100, 2]
    [101, 4]
    [102, 1]
    [103, 0]
    [104, 4]
    [105, 1]
    [106, 0]
    [107, 2]
    [108, 2]
    [109, 0]
    [110, 1]
    [111, 1]
    [112, 0]
    [113, 0]
    [114, 5]
    [115, 1]
    [116, 3]
    [117, 2]
    [118, 3]
    [119, 0]
    [120, 0]
    [121, 1]
    [122, 0]
    [123, 2]
    [124, 2]
    [125, 4]
    [126, 1]
    [127, 2]
    [128, 4]
    [129, 1]
    [130, 1]
    [131, 2]
    [132, 3]
    [133, 3]
    [134, 3]
    [135, 2]
    [136, 0]
    [137, 1]
    [138, 1]
    [139, 1]
    [140, 0]
    [141, 3]
    [142, 1]
    [143, 0]
    [144, 1]
    [145, 1]
    [146, 1]
    [147, 3]
    [148, 3]
    [149, 0]
    [150, 4]
    [151, 2]
    [152, 0]
    [153, 4]
    [154, 1]
    [155, 1]
    [156, 1]
    [157, 1]
    [158, 2]
    [159, 2]
    [160, 0]
    [161, 0]
    [162, 1]
    [163, 1]
    [164, 3]
    [165, 3]
    [166, 1]
    [167, 1]
    [168, 1]
    [169, 1]
    [170, 2]
    [171, 2]
    [172, 5]
    [173, 1]
    [174, 0]
    [175, 2]
    [176, 3]
    [177, 1]
    [178, 0]
    [179, 1]
    [180, 1]
    [181, 0]
    [182, 0]
    [183, 1]
    [184, 3]
    [185, 0]
    [186, 2]
    [187, 2]
    [188, 4]
    [189, 2]
    [190, 1]
    [191, 1]
    [192, 2]
    [193, 1]
    [194, 3]
    [195, 2]
    [196, 0]
    [197, 1]
    [198, 0]
    [199, 1]
    [200, 1]
    [201, 3]
    [202, 1]
    [203, 0]
    [204, 1]
    [205, 2]
    [206, 1]
    [207, 1]
    [208, 4]
    [209, 1]
    [210, 0]
    [211, 1]
    [212, 2]
    [213, 1]
    [214, 0]
    [215, 2]
    [216, 3]
    [217, 0]
    [218, 1]
    [219, 1]
    [220, 1]
    [221, 1]
    [222, 1]
    [223, 1]
    [224, 0]
    [225, 2]
    [226, 1]
    [227, 2]
    [228, 1]
    [229, 0]
    [230, 1]
    [231, 0]
```

```
[232, 1]
[233, 2]
[234, 3]
[235, 1]
[236, 1]
[237, 0]
[238, 3]
[239, 0]
[240, 3]
[241, 1]
[242, 0]
[243, 2]
[244, 0]
[245, 1]
[246, 2]
[247, 0]
[248, 1]
[249, 1]
[250, 1]
[251, 3]
[252, 0]
[253, 0]
[254, 1]
[255, 1]
```

```
******************************************************
********       Binary file is dumped.       **********
******************************************************
     0: 53 61 6c 74 65 64 5f 5f 57 db 60 c5 e2 b4 16 27 : Salted__W.`....'
    16: cc 8b b4 21 27 8b 76 19 5b 5b 69 ac 2b d0 24 98 : ...!'.v.[[i.+.$.
    32: 78 b4 65 75 0f 71 78 ae a3 5e 26 2c af 2f 60 f4 : x.eu.qx..^&,./`.
    48: 53 47 a3 63 ec f0 bd 4f b2 c4 77 48 70 c5 09 b6 : SG.c...O..wHp...
    64: 53 c9 4b 5f 27 aa 5c 0e 9e 7d c6 00 f9 ff 2b a3 : S.K_'.\..}....+.
    80: 4f 01 74 e9 42 52 1e 1f ee 2c 78 50 e6 dd 3b 76 : O.t.BR...,xP..;v
    96: a4 e3 3a 0c f8 30 40 dc f4 a6 d9 9f 8b 07 3c 68 : ..:..0@.......<h
   112: 4f a2 fb 73 f4 c1 1a db 70 86 b5 d4 16 9f b7 c2 : O..s....p.......
   128: 1b 97 e9 4f d1 ae bd c8 e3 90 e5 73 7d 50 03 c0 : ...O.......s}P..
   144: 9c 5b 6f 91 d8 ef 32 8e da df 26 64 0c 72 fa 89 : .[o...2...&d.r..
   160: f8 43 0c 88 0e b3 51 3d 39 36 2b e8 b8 02 f4 15 : .C....Q=96+.....
   176: a5 5d ac 1d e2 6e 71 53 7c 77 c6 b9 b8 73 4a 1f : .]...nqS|w...sJ.
   192: 56 3e 02 5f b7 7e 32 28 df 03 9e 24 10 58 09 e0 : V>._.~2(...$.X..
   208: 3a 66 fc 4b d0 cf 88 0e 25 ab 26 e0 cc 9a c3 1d : :f.K....%.&.....
```



```
   224: 71 41 26 a9 95 65 3b d0 2d 61 ec dc d2 be b9 59 : qA&..e;.-a.....Y
   240: 61 ca 47 9a b2 ae 3f f6 53 f3 32 89 26 c3 6d a4 : a.G...?.S.2.&.m.
   256: 6a 51 60 7d e0 ed 69 a9 a3 76 d7 7a 38 2c b5 11 : jQ`}..i..v.z8,..
   272: b4 54 cf 28 21 66 fd c4 e8 96 70 76 17 dc 69 61 : .T.(!f....pv..ia
   288: fd 2f 71 30 07 82 ba c8 a4 95 a5 59 9b a9 ca d8 : ./q0.......Y....
   304: 98 09 c5 a9 b0 af 10 a5 f8 b5 39 c4 d3 20 3c 4d : ..........9.. <M
   320: e7 9f d3 ab 71 ca e2 ec 47 b3 22 22 00 d0 f9 08 : ....q...G.""....
   336: 8f 89 b3 0f 96 51 80 a3 a1 8c a0 fd 80 28 41 98 : .....Q.......(A.
   352: 49 95 5c 1c be 60 ad 5a b9 e7 7a 29 33 72 82 9a : I.\..`.Z..z)3r..
   368: f3 63 35 4f 7f aa 48 03 b3 84 e5 01 c2 89 7b c4 : .c5O..H.......{.
   384: 35 97 83 5b cd 37 cc fe c9 ce b0 c1 98 69 ae e6 : 5..[.7.......i..
   400: 5d 73 3f bf 1e dd f7 9c 78 0c f6 f5 71 39 20 a4 : ]s?.....x...q9 .
   416: 08 fb 70 44 fc e1 2e 55 36 f2 25 ab 7d 0c 2a 30 : ..pD...U6.%.}.*0
   432: 6b 21 47 d0 b2 cf 54 c2 3d a4 aa bf 5b 5e c7 9c : k!G...T.=...[^..
   448: a9 b4 b3 8a 3d 5c 7b 0d ac 2e 38 0d 01 f7 0a a8 : ....=\{...8.....
   464: b7 9d 8e 88 6b 8f bc 49 f7 37 d0 bc 51 0d 2d 09 : ....k..I.7..Q.-.
   480: f3 96 82 d2 8a 25 78 a9 a1 d7 6d 9c 41 dc 46 ff : .....%x...m.A.F.
   496: 09 a9 1f 51 8e 7a 3c 83 29 2b e3 e6 44 e4 be 87 : ...Q.z<.)+..D...
   512: 26 98 7c 43 02 7c a4 9a 96 83 40 20 9e 45 16 65 : &.|C.|....@ .E.e
   528: d2 df 11 f8 73 3a cc 3e b3 3c 10 1c 22 ad f1 36 : ....s:.>.<..".. 6
   544: 54 b7 07 9c 02 23 2f f9 c2 98 0e 17 6b 53 0d dc : T....#/.....kS..
   560: 5e f6 3c 89 68 af 2c 22 73 74 c5 b3 0c dd 56 c4 : ^.<.h.,"st....V.
   576: a5 72 b8 4f dd e5 14 d1 2b 20 a4 0e bb cd e6 02 : .r.O....+ ......
   592: 84 e9 da b5 ae d9 b3 6c 23 f4 a8 b2 2d 74 bd 7a : .......l#...-t.z
   608: 40 60 e1 da 51 8a 34 f0 8c ad 3d 99 91 63 cb 31 : @`..Q.4...=..c.1
   624: 3e 58 3e 37 8b 9c 1c 99 58 c4 f3 a9 25 88 11 1c : >X>7....X...%...
   640: e6 2c b2 f0 92 cd 5a 23 2b cc 36 e2 45 c9 3e f2 : .,....Z#+.6.E.>.
   656: d1 a5 80 39 65 80 e2 dc eb c2 44 6c f9 91 f4 95 : ...9e.....Dl....
   672: 25 a8 a8 ab 23 da a4 6b ca f8 68 2d ee 0d d1 ad : %...#..k..h-....
   688: 1f 2e 15 01 01 ba 65 e7 b5 2b 40 36 b3 8d cb 54 : ......e..+@6...T
   704: 63 bd 93 f1 eb 94 ef 41 41 e1 09 8d f8 f1 2d 65 : c......AA.....-e
   720: ac b0 c6 1b bc 5b 1e 24 f2 2f 47 13 18 27 39 cc : .....[.$./G..'9.
   736: 30 51 a0 5d 46 96 1b 8c a6 4e d4 b7 ec b6 f5 96 : 0Q.]F....N......
   752: 17 10 c8 65 46 cc 1c 4c 08 3f fc 64 d2 cc 1a cb : ...eF..L.?.d....
*****************************************************
**********    Histogram is displayed.   ***********
*****************************************************
[0, 0]
[1, 0]
[2, 0]
[3, 0]
[4, 0]
[5, 0]
[6, 0]
[7, 0]
```

```
    [8, 0]
    [9, 1]
    [10, 0]
    [11, 0]
    [12, 0]
    [13, 0]
    [14, 1]
    [15, 1]
    [16, 0]
    [17, 0]
    [18, 0]
    [19, 0]
    [20, 0]
    [21, 0]
    [22, 1]
    [23, 0]
    [24, 0]
    [25, 1]
    [26, 0]
    [27, 0]
    [28, 0]
    [29, 0]
    [30, 0]
    [31, 0]
    [32, 0]
    [33, 1]
    [34, 0]
    [35, 0]
    [36, 1]
    [37, 0]
    [38, 1]
    [39, 3]
    [40, 0]
    [41, 0]
    [42, 0]
    [43, 1]
    [44, 1]
    [45, 0]
    [46, 0]
    [47, 1]
    [48, 0]
    [49, 0]
    [50, 0]
    [51, 0]
    [52, 0]
    [53, 0]
    [54, 0]
    [55, 0]
    [56, 0]
    [57, 0]
    [58, 0]
    [59, 0]
    [60, 0]
    [61, 0]
    [62, 0]
    [63, 0]
    [64, 0]
    [65, 0]
    [66, 0]
    [67, 0]
    [68, 0]
    [69, 0]
    [70, 0]
    [71, 1]
    [72, 1]
    [73, 0]
    [74, 0]
    [75, 1]
    [76, 0]
    [77, 0]
    [78, 0]
    [79, 1]
    [80, 0]
    [81, 0]
    [82, 0]
    [83, 3]
    [84, 0]
    [85, 0]
    [86, 0]
    [87, 1]
    [88, 0]
    [89, 0]
    [90, 0]
    [91, 2]
    [92, 1]
    [93, 0]
    [94, 1]
    [95, 3]
    [96, 2]
    [97, 1]
    [98, 0]
    [99, 1]
    [100, 1]
    [101, 2]
    [102, 0]
    [103, 0]
    [104, 0]
    [105, 1]
    [106, 0]
    [107, 0]
    [108, 1]
    [109, 0]
    [110, 0]
    [111, 0]
    [112, 1]
    [113, 1]
    [114, 0]
    [115, 0]
    [116, 1]
    [117, 1]
    [118, 1]
    [119, 1]
    [120, 2]
    [121, 0]
    [122, 0]
    [123, 0]
    [124, 0]
    [125, 1]
    [126, 0]
    [127, 0]
    [128, 0]
    [129, 0]
    [130, 0]
    [131, 0]
    [132, 0]
    [133, 0]
    [134, 0]
    [135, 0]
    [136, 0]
    [137, 0]
    [138, 0]
    [139, 2]
    [140, 0]
    [141, 0]
    [142, 0]
    [143, 0]
    [144, 0]
    [145, 0]
    [146, 0]
    [147, 0]
    [148, 0]
    [149, 0]
    [150, 0]
    [151, 0]
    [152, 1]
    [153, 0]
    [154, 0]
    [155, 0]
    [156, 0]
    [157, 0]
    [158, 1]
    [159, 0]
    [160, 0]
    [161, 0]
    [162, 0]
    [163, 2]
    [164, 0]
    [165, 0]
    [166, 0]
    [167, 0]
    [168, 0]
    [169, 0]
    [170, 1]
    [171, 0]
    [172, 1]
    [173, 0]
    [174, 1]
    [175, 1]
    [176, 0]
    [177, 0]
    [178, 1]
    [179, 0]
    [180, 3]
    [181, 0]
    [182, 1]
    [183, 0]
    [184, 0]
    [185, 0]
    [186, 0]
    [187, 0]
    [188, 0]
    [189, 1]
    [190, 0]
    [191, 0]
    [192, 0]
    [193, 0]
    [194, 0]
    [195, 0]
    [196, 1]
    [197, 2]
    [198, 1]
    [199, 0]
    [200, 0]
    [201, 1]
    [202, 0]
    [203, 0]
    [204, 1]
    [205, 0]
    [206, 0]
    [207, 0]
    [208, 1]
    [209, 0]
    [210, 0]
    [211, 0]
    [212, 0]
    [213, 0]
    [214, 0]
    [215, 0]
    [216, 0]
    [217, 0]
    [218, 0]
    [219, 1]
    [220, 0]
    [221, 0]
    [222, 0]
    [223, 0]
    [224, 0]
    [225, 0]
    [226, 1]
    [227, 0]
    [228, 0]
    [229, 0]
    [230, 0]
    [231, 0]
    [232, 0]
```

```
[233, 0]
[234, 0]
[235, 0]
[236, 1]
[237, 0]
[238, 0]
[239, 0]
[240, 1]
[241, 0]
[242, 0]
[243, 0]
[244, 1]
[245, 0]
[246, 0]
[247, 0]
[248, 0]
[249, 0]
[250, 0]
[251, 0]
[252, 0]
[253, 0]
[254, 0]
[255, 0]
```

5-6

松浦寛和 18B14101

```
I like nice clothes.  I love them.
```

```
  0: 53 61 6c 74 65 64 5f 5f 1d 5f 8d 44 56 f0 71 13 : Salted__._.DV.q.
    16: 9f e6 01 95 50 50 69 e5 a7 93 7d b8 3c 6f 79 da : ....PPi...}.<oy.
    32: 7d e8 ce ff 80 8b ca 53 2a 1b 45 94 c8 f5 7a ee : }......S*.E...z.
    48: 00 85 6a ba 3c 87 9c 6d 20 81 13 86 2e 65 b6 28 : ..j.<..m ....e.(
```

渡辺将任　18B16985

```
can’t love things that I used to love any more.
```

```
 0: 53 61 6c 74 65 64 5f 5f 8d 6e a5 d5 6a 46 e1 2f : Salted__.n..jF./
   16: 4e db f9 a2 24 2d da 78 f6 72 93 a5 ba 32 e6 8b : N...$-.x.r...2..
   32: 81 95 ae 54 38 01 54 75 54 d5 f3 b6 97 47 a1 2f : ...T8.TuT....G./
   48: b1 77 0d 16 b2 1e a9 f4 03 57 10 77 64 14 60 73 : .w.......W.wd.`s
   64: 0f 69 7c c5 fd 64 2b f9 35 00 d3 90 95 6a da b2 : .il..d+.5....j..
```

木村優孝 18B05007

```
I love baseball and I have a girlfriend.  She is very cute.
```

```
0: 53 61 6c 74 65 64 5f 5f bb 48 9f 0f bd 4a be bc : Salted__.H...J..
   16: 9a 94 cf 1d 54 61 09 2d ce b0 a1 30 2c 19 34 7d : ....Ta.-...0,.4}
   32: 75 3d 7d 66 da 01 53 d8 6a a4 d7 aa 7a ef fa f9 : u=}f..S.j...z...
   48: f4 bd 57 bd 3d 03 a4 68 9d 6b 76 b4 26 35 c6 06 : ..W.=..h.kv.&5..
   64: 40 9b a4 76 99 5d 15 8e 76 ae af 54 7b 2c de 75 : @..v.]..v..T{,.u
```

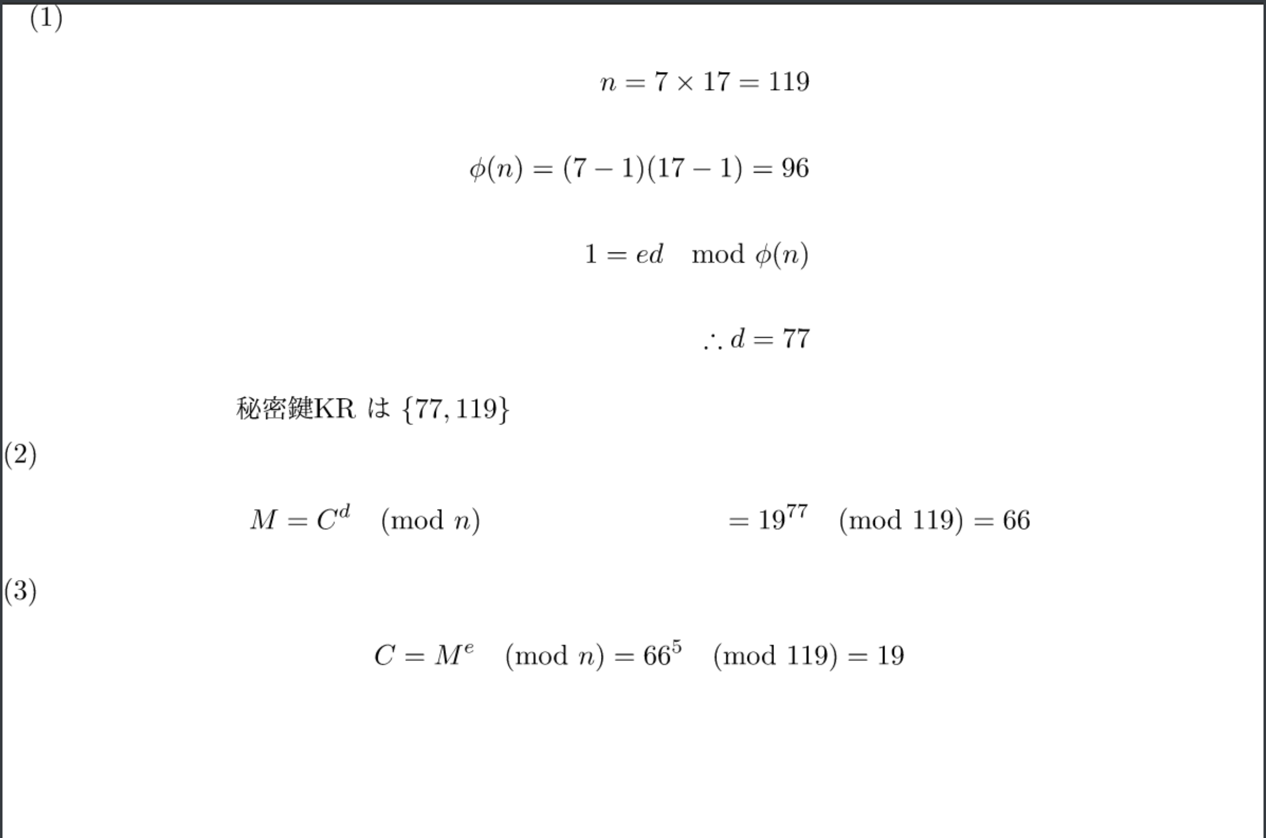
6-1

512bit
なぜなら、平文の可能性として2^512通りしかないため全ての数を表現するには512bit以下でないと全ての数を表現できない。

また、割られる数を2^512-1以下の数を、割る数を512ビットの数の中で最大の数(2^512)にすれば商は0で余りは絶対に重ならない(0以上2^512-1以下の2^512種類)

つまり、512bitの時には成り立つので、
最大値は512bit

6-2



(1)

$$n = 7 \times 17 = 119$$

$$\phi(n) = (7-1)(17-1) = 96$$

$$1 = ed \mod \phi(n)$$

$$\therefore d = 77$$

秘密鍵KR は $\{77, 119\}$

(2)

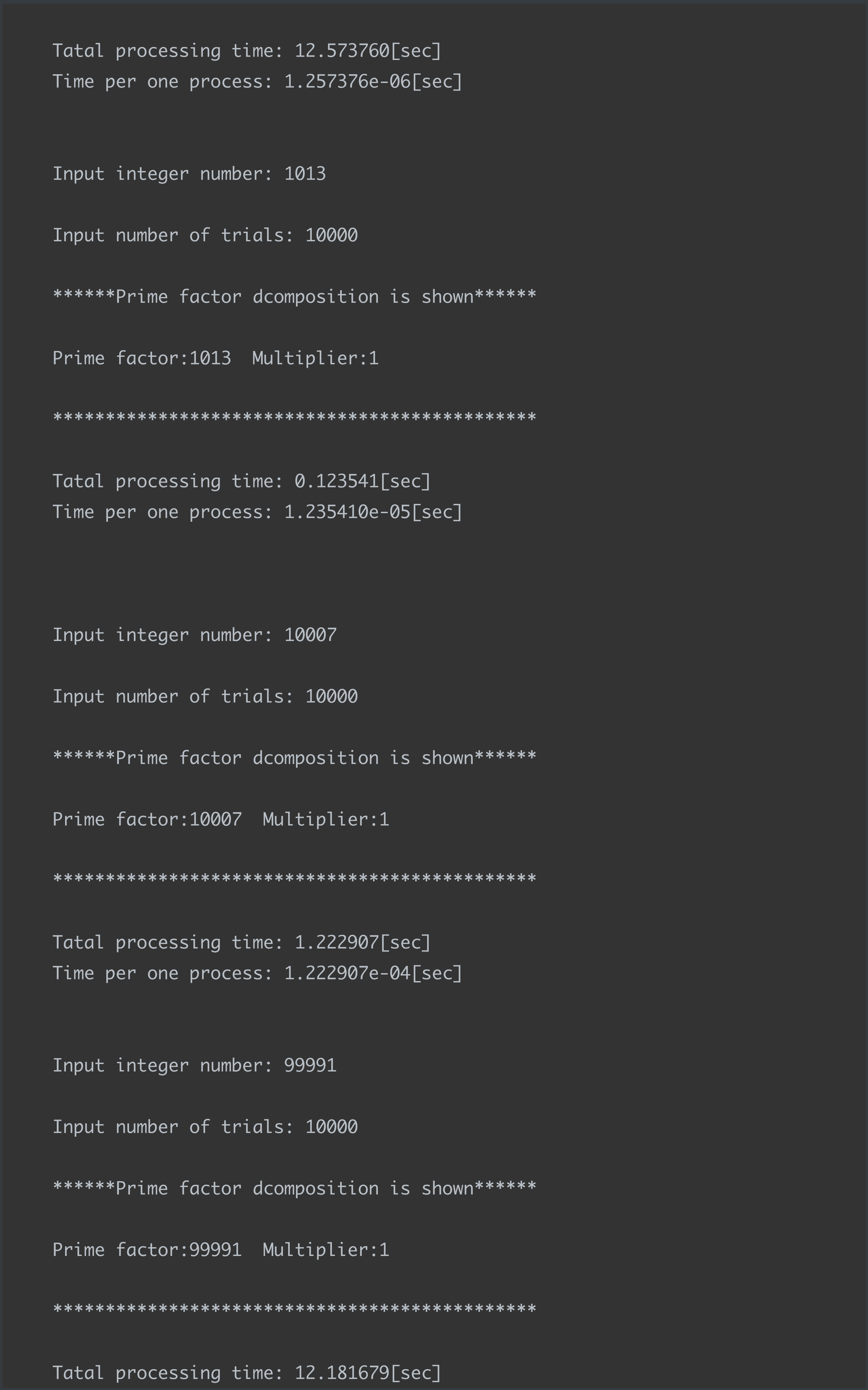
$$M = C^d \pmod{n} \qquad = 19^{77} \pmod{119} = 66$$

(3)

$$C = M^e \pmod{n} = 66^5 \pmod{119} = 19$$

6-3

```
Input integer number: 11

Input number of trials: 10000000

******Prime factor dcomposition is shown******

Prime factor:11  Multiplier:1

**********************************************

Tatal processing time: 1.435461[sec]
Time per one process: 1.435461e-07[sec]

Input integer number: 101

Input number of trials: 10000000

******Prime factor dcomposition is shown******

Prime factor:101  Multiplier:1

**********************************************
```



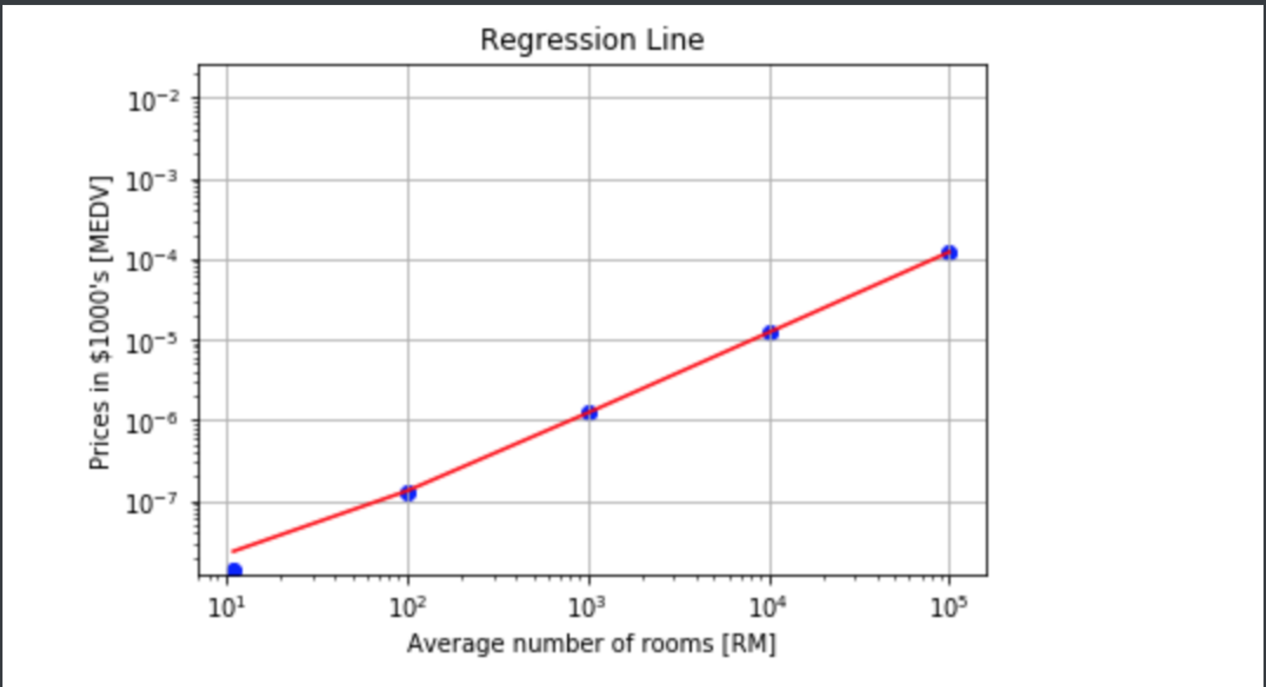
```
Tatal processing time: 12.573760[sec]
Time per one process: 1.257376e-06[sec]


Input integer number: 1013

Input number of trials: 10000

******Prime factor dcomposition is shown******

Prime factor:1013  Multiplier:1

*********************************************

Tatal processing time: 0.123541[sec]
Time per one process: 1.235410e-05[sec]



Input integer number: 10007

Input number of trials: 10000

******Prime factor dcomposition is shown******

Prime factor:10007  Multiplier:1

*********************************************

Tatal processing time: 1.222907[sec]
Time per one process: 1.222907e-04[sec]


Input integer number: 99991

Input number of trials: 10000

******Prime factor dcomposition is shown******

Prime factor:99991  Multiplier:1

*********************************************

Tatal processing time: 12.181679[sec]
```

```
Time per one process: 1.218168e-03[sec]
```

この結果をscikit-learnの線形回帰を用いて、尤もらしい直線を求めます。
また、その結果をmatplotlibを使って可視化していきます。

```
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
%matplotlib inline
from sklearn.linear_model import LinearRegression

df = pd.read_csv("time.csv")
lr = LinearRegression()

X = df[["number"]].values
Y = df[[" time"]].values

lr.fit(X, Y)

# グラフの描画
plt.scatter(X, Y, color = 'blue')
plt.plot(X, lr.predict(X), color = 'red')
plt.yscale('log')
plt.xscale('log')
plt.title('time of prime factorization')
plt.xlabel('numbers')
plt.ylabel("time [sec]")
plt.grid()

plt.show()

print('coefficient = ', lr.coef_[0]) # 説明変数の係数を出力
print('intercept = ', lr.intercept_) # 切片を出力

coefficient =  [1.21820299e-09]
intercept =  [1.02002747e-08]
```

matplotlibを使って結果を可視化する。



かなり精度高く求められていることがわかるので、この回帰結果を用いて、一年かかるところをこのモデルを用いて推測する。

これのyが一年である31536000になるのは、
xが25000000000000000程度の時であることがわかる。
ただし、xが素数の時には非常に時間がかかるが、そうでないときはそうとはかからないので、
あくまでもxが25000000000000000前後の素数の時には一年程度の計算時間を要することがわかった。

２つの素数pqの積の計算にかかる時間は、
pの計算時間+qの計算時間なので、
それぞれ半年の時の時におおよそ一年になると考えられる。

よって、
pqの計算時間のオーダーは、
1.5625e+32
と考えられる。

6-4

```
ryota@instance-1:~/security_homework$ ./rsa_keygenerate
Private-Key: (512 bit)
modulus:
    00:e1:99:57:78:72:be:4a:95:2b:73:7b:6d:8e:71:
    b8:f1:f6:49:98:c8:23:e0:36:1b:5f:7b:cf:ee:de:
    6e:99:f0:3b:20:02:fc:28:8c:86:3f:52:88:2a:9c:
    a2:6f:48:f1:9a:c3:90:65:e2:39:6f:a8:14:0a:03:
    83:78:f3:70:49
publicExponent: 65537 (0x10001)
privateExponent:
    04:e8:a3:40:99:ae:8e:4c:e4:9f:24:a6:63:9d:11:
    db:21:f2:c4:02:46:d5:90:17:d4:62:0b:4a:35:48:
    ce:cc:a2:e7:27:9c:2a:85:a7:0c:74:a7:01:51:f6:
    c5:78:cf:86:83:0a:12:19:ec:ca:c2:50:63:c3:11:
    15:12:2f:01
prime1:
    00:f3:9b:94:7a:ef:a3:4e:39:19:fd:0a:10:d2:1e:
    e1:38:cd:af:07:64:29:c3:28:a3:b9:e1:98:4a:ea:
    f8:12:11
prime2:
    00:ed:13:3d:6f:f6:e1:09:b0:1a:7a:f9:98:5d:29:
    58:1a:95:53:9f:6b:ff:c0:7a:29:7c:9c:d8:f0:00:
    a6:42:b9
exponent1:
    75:54:90:ce:29:4f:61:64:95:44:cf:ad:4c:56:bd:
    29:4b:bf:aa:72:ae:be:a5:7b:3e:13:0e:f3:be:7a:
    1e:d1
exponent2:
    42:fa:f0:9c:b5:8f:97:01:1e:3a:28:52:97:df:9a:
    78:c8:3f:bc:06:f3:57:1a:2c:a6:7c:59:fe:54:f0:
    a4:61
coefficient:
    0a:22:54:dd:4e:5b:23:b3:3f:e6:47:1e:4a:19:9c:
    5a:76:99:03:b0:2b:6e:96:62:30:c6:98:33:4a:2b:
    7f:5b
```

6-5

素数の非再現性の実現は，仮に同じ鍵が生成され，そのことが判明すれば，機密の確保，情報の改ざんの防止などが不可能になる(暗号鍵から推測できる)ため、実装されている。

今回の課題では、主にパディングを用いて素数鍵を作っているとかんがえられる。
パディングの仕様は RFC8017 で定義されており、 RSAES-PKCS1-v1_5 と RSAES-OAEP の２つがある。
これは非再現性を実現しており、確率理論的に毎回違う鍵が生成される。

##6-6
電子署名:My name is Ryota.
SHA256 digest:
0x6B 0xF9 0x09 0xC6 0xA9 0xA3 0xE9 0x14 0xE4 0xD5 0x6C 0xC2 0x67 0xA0 0x88 0x0E 0xE6 0x67 0xF5 0x9E 0xE6 0xD7 0x47 0x66 0xC5 0xA6 0x99 0xB0 0xA6 0x5D 0x79 0xBC
署名成功
署名文:
0x4A 0x2F 0x24 0x1C 0xA8 0xED 0xB9 0x71 0xB2 0x3E 0x73 0x6B 0x86 0xCA 0xBB 0x0C 0x7B 0x9E 0xAD 0x5D 0xBD 0xA6 0x58 0x9B 0x1F 0xF1 0xB2 0x21 0x97 0x48 0x7C 0xFF 0xD4 0x6F 0x15 0xEA 0x03 0x39 0x16 0xAF 0xBB 0xBD 0x41 0xA5 0x9C 0x4F 0x87 0xBC 0x50 0x45 0xB9 0xFE 0xAB 0x1C 0x0E 0x1F 0x7F 0x4A 0xEE 0x4A 0xEE 0x35 0x03 0x88
復号文(HEX):
0x30 0x31 0x30 0x0D 0x06 0x09 0x60 0x86 0x48 0x01 0x65 0x03 0x04 0x02 0x01 0x05 0x04 0x20 0x6B 0xF9 0x09 0xC6 0xA9 0xA3 0xE9 0x14 0xE4 0xD5 0x6C 0xC2 0x67 0xA0 0x88 0x0E 0xE6 0x67 0xF5 0x9E 0xE6 0xD7 0x47 0x66 0xC5 0xA6 0x99 0xB0 0xA6 0x5D 0x79 0xBC
署名検証成功

6-7

６−５にあるように、鍵にはパディングを持たせて、非再現性を実現している。
この課題では、パディング部分が一致していないために
鍵が一致していないように見えるのであって、実際の暗号文部分は一致している。

6-8

Program1 674820
Program2 17

6-9

```
セキュリティ鍵長 80bit
RSA 1024bit 暗号化（100,000回）CPU使用時間：1.32 秒
RSA 1024bit 復号（100,000回）CPU使用時間：11.51 秒
Segmentation fault
```

6-10

```
学生名:西原夏輝
平文:Hi I'm Ryota Yamada.

送った暗号文:
0000000 a3 c0 77 2b 1a be cc 5e 43 ea d1 76 38 0c ce 83
0000010 ec 7f 0f fd 66 8c e4 08 ee e9 2d e7 bd 7f 5a 5c
```

```
0000020 ef 5f 4f 99 8c e7 51 5e 0a d2 85 75 d2 19 2b 10
0000030 92 d1 cd 2f 2e 0a 9f f3 fa e1 94 72 2f c5 2a 90
0000040 3f 95 e2 be 6d a7 04 8e f2 c6 ef 34 57 89 69 e7
0000050 84 5e f9 2e 21 8f 54 c4 35 a1 dc a3 25 65 a7 f2
0000060 ba 8d 30 ec 1c b7 d2 26 1b eb 1e da 33 cc 5f 66
0000070 f8 47 56 fa 9e f3 0d ed f0 8f f0 f9 73 6f 8a 6b
0000080
受け取った暗号文(HEX):
0000000 60 0a 89 a8 09 7e 3b 64 be 1d dd e3 e4 15 2b 64
0000010 2e 99 a2 f6 8b 30 16 8a b0 5d 37 88 96 23 af 8f
0000020 75 33 f1 13 e0 11 a9 35 7b c4 d4 4a 18 b9 05 52
0000030 c2 8a b3 59 cf 18 43 b5 f8 c8 4d 43 89 6f 06 e6
0000040 11 07 fd 17 3c bc 12 4a a1 17 7a 3c 72 c2 95 2d
0000050 91 44 41 2a fb 09 b6 33 8c 53 28 93 a4 4d 28 72
0000060 b1 04 2a 0a b6 a8 30 a2 40 5d 4f 34 4c ab 4c ec
0000070 cc 66 cf 36 7d b6 2b 73 43 ce a4 2f bf ff ea 1d
0000080

復号文:

Hi, I am BISCO.
Nice to meet you.
I enjoy 6-10.
```