#avoid using temp.txt temp0.txt temp1.txt temp2.txt as input since they will be used to store data

#temp.txt will store the value of p, q, d and other are used to store the three encrypted data during crack

Message:

Life’s but a walking shadow, a poor player that struts and frets his hour upon the stage and then is heard no more. It is a tale told by an idiot, full of sound and fury, signifying nothing.

Hex:

bash-4.1$ hexdump message.txt

0000000 feff 004c 0069 0066 0065 0027 0073 0020

0000010 0062 0075 0074 0020 0061 0020 0077 0061

0000020 006c 006b 0069 006e 0067 0020 0073 0068

0000030 0061 0064 006f 0077 002c 0020 0061 0020

0000040 0070 006f 006f 0072 0020 0070 006c 0061

0000050 0079 0065 0072 0020 0074 0068 0061 0074

0000060 0020 0073 0074 0072 0075 0074 0073 0020

0000070 0061 006e 0064 0020 0066 0072 0065 0074

0000080 0073 0020 0068 0069 0073 0020 0068 006f

0000090 0075 0072 0020 0075 0070 006f 006e 0020

00000a0 0074 0068 0065 0020 0073 0074 0061 0067

00000b0 0065 0020 0061 006e 0064 0020 0074 0068

00000c0 0065 006e 0020 0069 0073 0020 0068 0065

00000d0 0061 0072 0064 0020 006e 006f 0020 006d

00000e0 006f 0072 0065 002e 0020 0049 0074 0020

00000f0 0069 0073 0020 0061 0020 0074 0061 006c

0000100 0065 0020 0074 006f 006c 0064 0020 0062

0000110 0079 0020 0061 006e 0020 0069 0064 0069

0000120 006f 0074 002c 0020 0066 0075 006c 006c

0000130 0020 006f 0066 0020 0073 006f 0075 006e

0000140 0064 0020 0061 006e 0064 0020 0066 0075

0000150 0072 0079 002c 0020 0073 0069 0067 006e

0000160 0069 0066 0079 0069 006e 0067 0020 006e

0000170 006f 0074 0068 0069 006e 0067 002e feff

0000180 000a

P: 259175246047993254142035567388076122391

Q: 330949194243463255807127583411562258447

D: 78240472712185390244493913756672421868261530412312394285204738278320939186693

Encrypted:

bash-4.1$ hexdump output.txt

0000000 d47d a6eb 0c1f 04e7 976c b342 aeb7 ebf9

0000010 a641 275f c6c0 ac09 c27b 6ffa e02b aea3

0000020 d24b b301 1641 1429 7502 1728 ee6a 6ca8

0000030 7453 0ffb f4e8 49a1 3301 24eb 2618 6005

0000040 9a56 8ba1 280a ed6e aaf8 e9f5 1f87 21d8

0000050 2cac 2fff 3916 84bd 80a2 a647 c919 0b95

0000060 3662 4b58 01f4 174f 2fb7 8410 1b01 cc67

0000070 24e2 bcdb 592d 268f bc6d 0b3c 5019 fef5

0000080 4d9f 1dec d9f7 4ac5 23bf 822a 79b7 faf7

0000090 3b65 b073 b8bb 8143 8630 de20 f3f1 52d3

00000a0 a39e 0381 f5d6 5bef 7335 bf89 b104 1c5c

00000b0 496a da66 93ee ff85 b8bb e8c2 d058 1b55

00000c0 a0b7 8c62 ee87 9617 c087 ddc4 a831 b1f9

00000d0 f125 4aed a960 b035 3b28 bab7 e041 5aee

00000e0 5200 bf18 c42e 3741 55c4 8385 8b6d 446f

00000f0 7a93 7994 1215 40ca 3bbf 22e0 e7b2 8929

0000100 dd5d 2001 e3c9 e274 c56a 2efb 4977 7126

0000110 3714 4319 f309 40cb 7d56 68e9 53bb d7fc

0000120 0706 14d3 749e 1e2c 38d6 c304 a02a e894

0000130 8744 0603 ef73 3bb6 a23c e225 5a59 0f71

0000140 0797 aded c56d 9029 5fe5 eaea 6b64 31b0

0000150 0acb 1bc1 ae54 8eee b24f be1f cfc1 923d

0000160 4383 7c84 e553 c3bf a633 7265 9af1 5e31

0000170 7ee7 bb6c 7fa3 abf2 d480 bab7 61c4 263f

0000180 2c03 a89f 3fe8 6b7e fe9e 584c ef16 aeff

0000190 b76c f804 41fd d22e 7994 7b83 db7d 284d

00001a0 bd6b 217f b948 b6f9 b74f 4ab1 861b f946

00001b0 5d7d 689e 5a5b a857 0517 e1b9 b67f 4538

00001c0 417e 2d51 7a38 3108 7779 98a6 32dc d34f

00001d0 c613 cf10 3412 1cd3 d2dc 9ce5 cf31 9c2f

00001e0 9c67 fa2c f380 8786 de6a 76aa f3b0 5ef9

00001f0 8b98 7463 cf9e eac4 29e3 a314 fb5f a13f

0000200 40b8 eceb 4610 e9f0 fb21 56b3 0623 4dce

0000210 b811 b677 b66e 4f7b fff7 ba13 ee73 3102

0000220 2124 eb76 72c5 c1f6 94bb 3b34 8913 6fbf

0000230 23fb b369 dca9 9993 881e 2733 c915 0834

0000240 14a2 dc87 f93b bb0d acae 727d c333 9e62

0000250 abb6 701f 3a4e 01af cb06 e589 9eee bc15

0000260 647c 4a80 1edc 4a9f 9ea2 3515 25e9 acbd

0000270 2382 eb9e ab17 fe8e 5d4e 0a78 646d a7e5

0000280 5a1b 4399 938b 646c 6b06 e6c5 6f27 601c

0000290 83df 0760 8eb5 96a1 7df2 2e38 3fd3 e47b

00002a0 3315 6546 a42c 2c0e 5504 0464 b718 c801

00002b0 f298 8d51 0b6d 1d1f 0285 db73 6b58 6ae0

00002c0 ed6a 52fa ebdc cd9a 0061 a534 4448 d5a0

00002d0 546f 1386 cbda 2525 f69a 6a42 0f97 106f

00002e0 b00f 1775 fd19 819a a200 400c b68f d561

00002f0 c64a 6cb2 d3a9 514e 1635 4b86 fed1 6026

0000300 3a22 bbee 968e d195 6fd1 2b3d 2ab1 cece

0000310 f530 46ed 50be 6586 4bd7 27ef 6e3a 4c62

0000320

Decrypted:

Life’s but a walking shadow, a poor player that struts and frets his hour upon the stage and then is heard no more. It is a tale told by an idiot, full of sound and fury, signifying nothing.

bash-4.1$ hexdump output1.txt

0000000 feff 004c 0069 0066 0065 0027 0073 0020

0000010 0062 0075 0074 0020 0061 0020 0077 0061

0000020 006c 006b 0069 006e 0067 0020 0073 0068

0000030 0061 0064 006f 0077 002c 0020 0061 0020

0000040 0070 006f 006f 0072 0020 0070 006c 0061

0000050 0079 0065 0072 0020 0074 0068 0061 0074

0000060 0020 0073 0074 0072 0075 0074 0073 0020

0000070 0061 006e 0064 0020 0066 0072 0065 0074

0000080 0073 0020 0068 0069 0073 0020 0068 006f

0000090 0075 0072 0020 0075 0070 006f 006e 0020

00000a0 0074 0068 0065 0020 0073 0074 0061 0067

00000b0 0065 0020 0061 006e 0064 0020 0074 0068

00000c0 0065 006e 0020 0069 0073 0020 0068 0065

00000d0 0061 0072 0064 0020 006e 006f 0020 006d

00000e0 006f 0072 0065 002e 0020 0049 0074 0020

00000f0 0069 0073 0020 0061 0020 0074 0061 006c

0000100 0065 0020 0074 006f 006c 0064 0020 0062

0000110 0079 0020 0061 006e 0020 0069 0064 0069

0000120 006f 0074 002c 0020 0066 0075 006c 006c

0000130 0020 006f 0066 0020 0073 006f 0075 006e

0000140 0064 0020 0061 006e 0064 0020 0066 0075

0000150 0072 0079 002c 0020 0073 0069 0067 006e

0000160 0069 0066 0079 0069 006e 0067 0020 006e

0000170 006f 0074 0068 0069 006e 0067 002e feff

0000180 000a 0a0a 0a0a 0a0a 0a0a 0a0a 0a0a 0a0a

0000190

There is padding of new line character in the end.

Cracked:

Three different N and their encrypted file

N1: 89533425768699048071438521161493617585378577776773878325676980311087127766931

Encrypted:

7D381756CD184E43A430D767D6F25C72

2D4ABF1C1E8C3599691E580B77AEB5C5

19F0FA8690EDAEE0C59E0EA84B337C3E

67A9F80EBC24A3B591BAE1802305D4B4

56B7F8AA56D01E83EBA8A6BE6DDFA4AC

8B8C70D57CA7E2B9AB26BECB54C0DAE3

65487497AC3EADDE04B67BEA9FEA9284

7C0605578F92C04C9129AA5A6A5F0249

2D85B6FC51D4B89E9CE1491F7D5FE471

B21C027F6888527AED3C1F03FB51FC04

7C94B76EA0801EE307659A0397C3F935

64F760EF697D6AB5C3590FDA60BFB45F

8D3F302F33BF14C77548E5B490E37895

ED52E3DA056D3A362389448638E01AA1

0537AE1AB673BB38F5B78ED4EE2FC8A8

A0E00E88BB813CC29F1952E14825141F

469F17FD94E13AA35524B41B1D11F705

CDC95E0C0D8063EE3B982C63D55DA9FD

3092CFC5F6B2E0CB97756848D99BA366

3287452BBB73811438F340EF7720CB93

4548BEDE87EC14837ACC679CBF7331DD

922E2030C1A26ED08F6879CDF61B38F1

BF39FA43578C46B5A27742A4977BB52C

5E30DE89803E9FD67443137D777B1081

N2: 92162101813384876231932051907862811433926147661743041665344895511903913096019

Encrypted:

09574D5AEFF5A38B1488B56F11C824B1

C3A6042FC426ECE61A8212EE44604E70

7B73E1684191BC9FDC85151AED5BE5ED

BD8FC946AD7417DC77CE4705FF39F394

942970FC5CEC97F6DF1CC8B743850E78

51B19C669EA27563C0E845A831B154D9

5F65C8A04572A96EDED9EE1AB6E7AFD2

3B12A8497EEBC495CBE0A98FDBB0EEA8

593E7D4924198347169A6CFDEC173F31

43EECC0490F63005AACB36D903A08E00

B9A8259523977571D75C30D28880EA76

D61703D57F602D531D713C4DF95D9133

8DA46BF471172E537C4DB83E0DCC8E54

1CE442248311A7015602F4169930B1B2

25FDC1B4F9E0C354BDCE76D6F02A25EE

A5484E067752C30F6277B95201724916

9B45A6F8A5F247B04C84139E9EFACCD9

01CD2FD74B37CF3514E32B0914B200FF

0A5D7E716E4F8D15DDBCEC615B9FC149

4AB7D9F7D679B8F538C129C8F1EF49F3

943B24968D654175DF85A9EF8EBA3A17

95716DDFC4D6AEDFD309A7E5CDAFFBFD

A324C01803E168257837F14CE9244DF8

FC2BFF765A9EA9F6B54451382CDBEC0C

N3: 79153338251961140082087369418019797208704981389107155359590624572702820380453

Encrypted:

7D17CA1C518456E5C7739AACC79D9D47

F5A6D16385C6AEACF47A2B72EB2E4EBE

0F3F7EE153732C99E8C0BBDEC64F1155

55E761922827FCA663E3B9E42EC407C9

20B2ACFE5AB2411D003CEDA42690D1FB

76DBB0E397EA8729D0864BC5C7553E4F

56FE28205E57D58609CB67A7C0813189

6909CED0079FA57C0031DA31DDAA9683

6C4333FE81F60A3710A54AC5D8A5AE65

E5E0C62AD3D8DC52B2288DD30B841B29

7AA18C5BE1B721C91AD086E6BF130563

CADFCF94670AF63E24AB93D494CBE813

531DDAA5A1D2C999A103E1637AB262CE

3CD9015A3ABEFFFA84CC606D7BF5DAE4

A2E336A7212B7AF24ACD8F850D336892

08C9DF96AA3B79FD5C6CEB7691DDEE33

232FA06469FB508E89FDF5B72FF7BD24

44B0CA6AC92DF0B3247C061F78E07B0C

9F20DDE4587E685E7E0F6AFAE751DDAA

977DB6B353E77FCC73C46209B1273434

0F8DD01FBF9E030FF8E48CAB84AF086A

249A9298D0A81C478222283DB4F45BD7

97EE71A2D85A453AF1FDECAD175285C6

C5DCBE5FF392D8C69A3C2EADC7682098

Cracked:

Life’s but a walking shadow, a poor player that struts and frets his hour upon the stage and then is heard no more. It is a tale told by an idiot, full of sound and fury, signifying nothing.

Hex:

0000000 feff 004c 0069 0066 0065 0027 0073 0020

0000010 0062 0075 0074 0020 0061 0020 0077 0061

0000020 006c 006b 0069 006e 0067 0020 0073 0068

0000030 0061 0064 006f 0077 002c 0020 0061 0020

0000040 0070 006f 006f 0072 0020 0070 006c 0061

0000050 0079 0065 0072 0020 0074 0068 0061 0074

0000060 0020 0073 0074 0072 0075 0074 0073 0020

0000070 0061 006e 0064 0020 0066 0072 0065 0074

0000080 0073 0020 0068 0069 0073 0020 0068 006f

0000090 0075 0072 0020 0075 0070 006f 006e 0020

00000a0 0074 0068 0065 0020 0073 0074 0061 0067

00000b0 0065 0020 0061 006e 0064 0020 0074 0068

00000c0 0065 006e 0020 0069 0073 0020 0068 0065

00000d0 0061 0072 0064 0020 006e 006f 0020 006d

00000e0 006f 0072 0065 002e 0020 0049 0074 0020

00000f0 0069 0073 0020 0061 0020 0074 0061 006c

0000100 0065 0020 0074 006f 006c 0064 0020 0062

0000110 0079 0020 0061 006e 0020 0069 0064 0069

0000120 006f 0074 002c 0020 0066 0075 006c 006c

0000130 0020 006f 0066 0020 0073 006f 0075 006e

0000140 0064 0020 0061 006e 0064 0020 0066 0075

0000150 0072 0079 002c 0020 0073 0069 0067 006e

0000160 0069 0066 0079 0069 006e 0067 0020 006e

0000170 006f 0074 0068 0069 006e 0067 002e feff

0000180 000a 0a0a 0a0a 0a0a 0a0a 0a0a 0a0a 0a0a

0000190