Task 3

3(a)

For this task we asked for finding the PIN with the given information according to this formula c = (PIN)e mod N). Also we know that the PIN format is changed to binary number and concatenated with 2048 of ones which gave us the **c_prime** in the result.
For calculating this, need a **("for") Loop** in a range of (0 , 2**16) and then, we should say we have the Binary number and which concatenated with 2048 "1" at the end of it. After that we need to put the power_mod formula in the "if" condition which is a reverse code to calculate the missing part. By doing that when the number is matched as PIN, it will be print out as Hexadecimal.

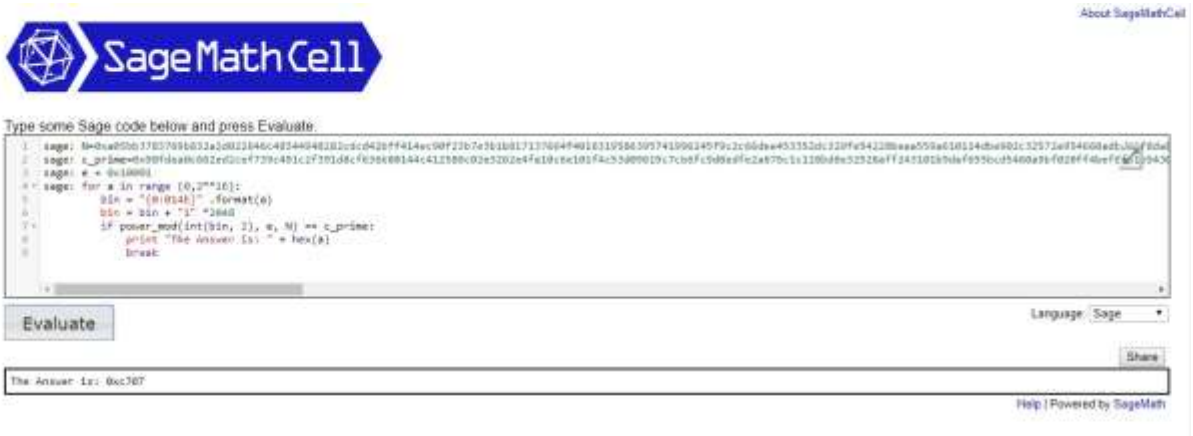
```
sage:
N=0xa05bb3783769b832a2d022646c48344948282cdcd42bff414ec90f23b7e3b1b81713766
4f40163195863957419962 45f9c2c66dee453352dc329fe54228beaa559a610114dbe902c32
572e954660adbd06f8da8c770c33bb5ad15f506073ea0c50ff4e9906e16ee70d1311e0ad8189
6f4807282361f5b2116488de06966b571cdb15da536226378bc1fba8a3476c5809b5a274a01
17b5de3e52278d39fdfa62de29f338b0453ac3af61a30dcb2975949a3d0ec2d2b7f0d2c4d2e3
ef6ddefa8caad21bc16972dcecfcd5f9332373a759632f7f02c52dd424b83985eaa673ce67023
366e85899729fc1d1fede02fa9c53aa01328c9108a3c5145f47ef988688f3076d49821314210d
1f4db88fa836d41f3dc3960499eb46b28261aaa1515e0fb6d7481ae051b607683cbfdc18d6b6
92f93d6facf4002d6fa835aac4d61911b66859a81043763e1d0ef6e47f1a7a4c8d57993b0fb67
b5758ed3aca9540d39e150935cdd0c320d166da65612ae78322f96853885e6a44add306a89
9fab2f87cf2a1d

Sage:
c_prime=0x90fdea0c662ed2cef739c491c2f391d8cf636b80144c412580c02e3262e4fa10c6
e
101f4c53d09619c7cb6fc9d8edfe2a676c1c128bd8e32528aff243101b9daf655bcd5460a9bf0
20ff4bef0f61b94304b142b6b18830b8b4d5574e8b54903de67df71f39234fdf9f66723ab1bf42
6d1c0a95fabae8485e9edf7f4c868ca2816398b1f46ffda2a84b5d52ff36bad829ddc2e123f86c
b266256824f047fb6f6a1c7593eaf4ae5c47c6f5e633370d832345fde53324d02687a9b21e60f
cefb5e2e2eb1ace969fe72afca67847acad093dec8976336ace5f135257f740f625851a325885
4775a3f4f123eae1a6253b2740de37d112bca596f36e4c0d4cfc50b05643b8ec0b52619ae7d0
ae990e041ba01bc149ac4a510c81e3aef3f4f2843a50f15c637e274e714c6a768e0c7d96e28a
5365b64aee0315623794724573648516ebc9b0f5135a180ac3141a98f2ef0f005f6980781036
c9b1c7975774708d1929d1935ae782de80722124220a9dd3fadc457d8bdb8be762b0158187
ee619142637d

sage: e = 0x10001

sage: for a in range (0,2**16):          bin =
"{0:014b}" .format(a)          bin = bin + "1" *2048
if power_mod(int(bin, 2), e, N) == c_prime:
print "The answer is: " + hex(a)              break
```

Solution: 0xc707



SageMathCell
About SageMathCell
Type some Sage code below and press Evaluate.
Evaluate
Language: Sage
Share
Help | Powered by SageMath

```
sage: N=0xa05bb3783769b832a2d022646c48344948282cdcd42bff414ec90f23b7e3b1b817137664f40163195863957419962 45f9c2c66dee453352dc329fe54228beaa559a610114dbe902c32572e954660adbd06f8da
sage: c_prime=0x90fdea8c002ed2cef739c481c2f381d8cf698800144c412580c02e5202e4fa10c6e101f4c53d00019c7cb6fc5d8edfe2a670c1c1100dde52526aff243101b9daf655bcd5460a9bfd20ff4befe81b9430
sage: e = 0x10001
sage: for a in range (0,2**16):
          bin = "{0:016b}" .format(a)
          bin = bin + "1" *2048
          if power_mod(int(bin, 2), e, N) == c_prime:
              print "The Answer Is: " + hex(a)
              break
```

```
The Answer is: 0xc707
```

3(b)

In this question we need to demonstrate how Marvin can factorise N. “**N**” is given to us and we know that **N = p * q** and also we know **phi(N) = (p-1) * (q-1).** So we need write the formula based on **N** & **q** completely and ignore **p,** so we can find **q** first and then calculate.

According to this formula : ax^2 + bx + c = 0

$$X = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

And then finally print out the answer in the Hexadecimal.

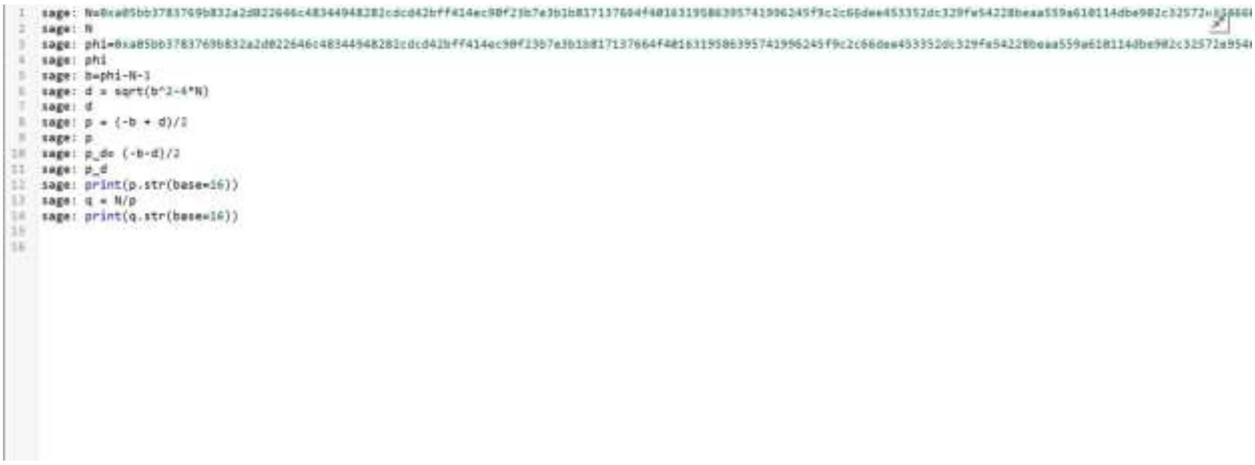
1. sage: phi
2. b=phi-N-1
3. d = sqrt(b^2-4*N)
4. p = (-b + d)/2 or p’ = (-b - d)/2
5. P
6. print(p.str(base=16))
7. q = N/p
8. print(q.str(base=16))

***** sage:
N=0xa05bb3783769b832a2d022646c48344948282cdcd42bff414ec90f23b7e3b1b81713766
4f40163195863957419962 45f9c2c66dee453352dc329fe54228beaa559a610114dbe902c32
572e954660adbd06f8da8c770c33bb5ad15f506073ea0c50ff4e9906e16ee70d1311e0ad8189
6f4807282361f5b2116488de06966b571cdb15da536226378bc1fba8a3476c5809b5a274a01
17b5de3e52278d39fdfa62de29f338b0453ac3af61a30dcb2975949a3d0ec2d2b7f0d2c4d2e3

ef6ddefa8caad21bc16972dcecfcd5f9332373a759632f7f02c52dd424b83985eaa673ce67023366e85899729fc1d1fede02fa9c53aa01328c9108a3c5145f47ef988688f3076d49821314210d1f4db88fa836d41f3dc3960499eb46b28261aaa1515e0fb6d7481ae051b607683cbfdc18d6b692f93d6facf4002d6fa835aac4d61911b66859a81043763e1d0ef6e47f1a7a4c8d57993b0fb67b5758ed3aca9540d39e150935cdd0c320d166da65612ae78322f96853885e6a44add306a899fab2f87cf2a1d

sage: N

sage:
phi=0xa05bb3783769b832a2d022646c48344948282cdcd42bff414ec90f23b7e3b1b817137664f4016319586395741996245f9c2c66dee453352dc329fe54228beaa559a610114dbe902c32572e954660adbd06f8da8c770c33bb5ad15f506073ea0c50ff4e9906e16ee70d1311e0ad81896f4807282361f5b2116488de06966b571cdb15da536226378bc1fba8a3476c5809b5a274a0117b5de3e52278d39fdfa62de29f338b0453ac3af61a30dcb2975949a3d0ec2d2b7f0d2c4d2e3ef6ddefa8c915dbdc153c25b847c313f96c30a78950106adcc70eef014d1340f26f0fd36a90d6a5e1c369a70658dfbb20feccf4efd255d477924a95ae093387182cf946b4dae80d6b434fcb11f2a8e9265b23e7dd076733f268d8cacf0ba15aeee50b7fc577c7db1269f54436c8c9ade14d23f27097e128a4a312eb9c9e7cd9fc5c40efe18a6b3b56947761243265d6a3ccd7bc9027e6e4ecc267765ea293574502e955349b0d866ad5a16f92bf6e96273d24dd25807554de152e65fa7273818bb3f013a73c



```
sage: N=0xa05bb3783769b832a2d022646c48344948282cdcd42bff414ec90f23b7e3b1b817137664f4016319586395741996245f9c2c66dee453352dc329fe54228beaa559a610114dbe902c32572e
sage: N
sage: phi=0xa05bb3783769b832a2d022646c48344948282cdcd42bff414ec90f23b7e3b1b817137664f4016319586395741996245f9c2c66dee453352dc329fe54228beaa559a610114dbe902c32572e954
sage: phi
sage: b=phi-N-1
sage: d = sqrt(b^2-4*N)
sage: d
sage: p = (-b + d)/2
sage: p
sage: p_d= (-b-d)/2
sage: p_d
sage: print(p.str(base=16))
sage: q = N/p
sage: print(q.str(base=16))
```

The two factors p and q:

p=0xe0090a82f4665efc3dee6cce9ee457a00ada319e3818283b86587313464c22b9b30db4da7562b2ead09f900058e9581798d7dbc84ee4fccb5972fe37a7999062c03837f97db2b60e03887f235033264a6f9d18b88b640026d99b17a99f921a99b5b87169a2ff5334e2da36672b3eeeb087451768dc403155ce52ea414226ea96afd455fc7e08d72fd1a672febccaaa2f1ff0135cf59b00b80c251692bbc0bcf92f0994f57c2fd28c6fa971a7df81161bbcc508efde052fbbc6222287ba6b19a3

q=0xb73cd57e66a1b78bcc5d2cf767ae94a617b2e1c70bd618c2e9fef928111d59259982d7e7aa8d70b86cc53ce109cb7d50b166d56e770f917cb8fa6894e78849f2ce8ef4e463c448d14869e37c0f523ea2056855283a859bf5ab24a3866acf1b5bf6ee2a31831cec861f75a9d91c37d04b6e8d133413ab2c8f0f7f66c40e049a647f7157a66e77d58d36cadadc10419b228cdbfb4858642f790d2cf87794cb5eff204d0c66ef77085a77d315932dd15ae9066bff9f3e72063c4ffbfcf3dd50693f