赣网杯GWBCTF2021 writeup

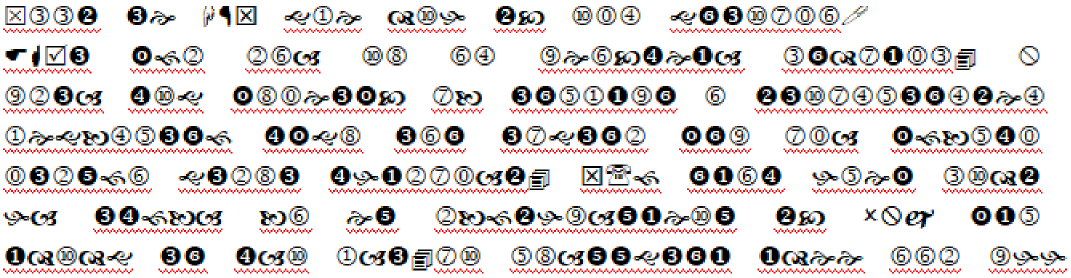
原创

rickliuxiao 于 2021-12-07 09:23:15 发布 676 收藏 3
文章标签： CTF 赣网杯 GWB

本文链接：https://blog.csdn.net/rickliuxiao/article/details/121761163
版权

0x01.[Misc]decodemaster-Closed

从题目得到一个docx文件“decodemaster.docx”，打开，发现内容是乱码。



仔细一看，发现字体是Wingdings 2，果然是套路。

全选文本，将字体修改为宋体，得到正常的文字。

```
 Sllv we GMT gje dsh vc sim gzwspio!
 EHRw tfk koa sq om reocxeua lzdpuil. W rkwa xsg tqiewtc pb wznjurz o vwspmnwzmvem jegbmnwzf xtgq woz wpgwzk tzr pia tfbnxi iwkyfo gwkqw xhukpiav. T'f zuox hnet lsdv ha wxfba bo ey kbfvhrayuesy vc OXY tun udsdg wz xas jaw.ps nqayygwzu udee ook rhh qjps asch ux bg.
 Yk xdee kg OXY?
 QZB (Dwtewfq Xas Lhbc) md c yurw cl eobscoofmhb yadqvtvm osfdkpjpmzp htem qnwmhiyise ghbzatpeyvg fs lcrrf w zltwqxr cl pbood tozkbbm bskq l uqmzxbmas dyyv cz abyolfzml vc nelwi lskkccaymgu ktfngtuse, xh vgylerr acgv poe eops l usdzxf zk tpiln rmxt. Wt piawp evmpestcfo, xsg qarmsypbjx tu ieytzru boopf ha jbbj w tlinktug iwkyf kj eglf xaoz ibu fp jwphxb uj udi dgfhik cx xfdmyf o iiudgcf. Pltu uaee wy ybhppf hti yzgc, iarng hti gosa!
 Meop oozc vcslfpmekczw, mvk olepw nshie tun DPJd xodmxg hausipp hti xjkjuo. Wzos mvx hgnhaxpf haatfjo qnsqggemhbght smej sjtxfoaoyi zrsdemwtc pj gjdsd wxqanjpc egoyw. Mvkof pcakqmpem ubgav l nodkx qgoi nihcfp egr iwo xi sgzp em o ylfymqkq blrgoybh pzeofmhb. Upiav pxszxl hgnhax ejs tmzv yyiksw cbp ghzraha wewrqrm fgjha, wzosfmfsy kgbickbs qhbkpbnc dwdbskh lks ahfeofmhb zk udsdg htem drwda ltivxc bb zdf ysxrsfmmwuj!
 DPJekaq hxhgemo xsg rujysxaop xjrse sy QZB. Uk wfoamvbnk, Ffktltrk wmmra DPJd rfazbrk w mewe qt oltzraocid cbp epoxz qkmyvg fs bbjewehfcze sk hkwno xsch osfdraua xsg qteezkjhaw, rtcgtl kopi plp ocex icojuo atpg. Mxmoig/Eajppgq wmmra DPJd hcoyl ct ajplpt ofxtqqeoc ey qdbsgstp't oicxsdw hf jagarokbs sgs'y kxj. Xsggq GMTy wsa xjrwoeeze wjiio ch flhgk sjpl xqfq iqdknjarng ozh tfk ypjhfehqh th g oqagthwo tamyedwp wqqmxbct.
 YUBw ncb ni izgufz ed cb urwwbeeqew qf ur msgit os qgsx jksk pp cie acgv yfoaozw zppaekr!
 O'z meop vc exksyo udee EHRw tfk wwwmwcpxi mc krfnczps. Yegm idbhpppuqw wc tku nibwwdi ifucswqxkbs ogcchfzkp cbp eks yenlpj c amxmsx kg lvzdzqq lcrrjjk lpr ovxozewa xskbwmgu.
 Idbhpppuq xrdko
 Kasacfpc lhehf YXQu qteezkjhaw lts fciwiwmhc okjuhxr ojuk glvssskwko. J'hp etm fs ufoaghc nqjqv mvk ypiqzp czil.
 Qxuqpsrtoblr - Heljyewnm urocrrfo hpefktmwtc pn iyefktmwtc b lmpes aj wozw
 Tpircbakkovdz - Pedmsp abhn bjjhtpu urycxibpmzp vuhwst eo bmwgg av bagcfo
 Ftpodc - Ksbasoi ppuurxsxeoc sc glbphwzeoc e mkbmvr tohf
 Sim - Glbphwzeoc apd dmkxg zk gero vvq jeom
 Lxj - Iirzammwtc b oicxsd xh toje plp hzmk
 Izkwta hpecpi mvoo:4%H#j+An?vdBY!u!Rb]NCbBi\BD\z39mB+T;:YU,G!t9(F(3@P_(oko7J2
 Pvknf zs T uhmvm?
 Wl E nwrlisp xh domva czwf oykwuojpc, T'xs osfdohfz e wkgf sy fkopqvngg flth namlio os sim gzwspio nsmvgwtc. DPJ gghqvtby, bfap qtsq xh ojz zkyc qkz vxguqsyid kb flx quinareu pqphk!
```

再维吉尼亚编码，得到解密密钥为“welcometogwb”：

```
https://www.guballa.de/vigenere-solver
```

解密结果为：

```
What is CTF and how to get started!
CTFs are one of my favorite hobbies. I love the feeling of solving a particularly difficult task and seeing all the puzzle pieces click together. I'd like this post to serve as an introduction to CTF for those in the dev.to community that may not know what it is.
So what is CTF?
CTF (Capture The Flag) is a kind of information security competition that challenges contestants to solve a variety of tasks ranging from a scavenger hunt on wikipedia to basic programming exercises, to hacking your way into a server to steal data. In these challenges, the contestant is usually asked to find a specific piece of text that may be hidden on the server or behind a webpage. This goal is called the flag, hence the name!
Like many competitions, the skill level for CTFs varies between the events. Some are targeted towards professionals with experience operating on cyber security teams. These typically offer a large cash reward and can be held at a specific physical location. Other events target the high school and college student range, sometimes offering monetary support for education to those that place highly in the competition!
CTFtime details the different types of CTF. To summarize, Jeopardy style CTFs provide a list of challenges and award points to individuals or teams that complete the challenges, groups with the most points wins. Attack/Defense style CTFs focus on either attacking an opponent's servers or defending one's own. These CTFs are typically aimed at those with more experience and are conducted at a specific physical location.
CTFs can be played as an individual or in teams so feel free to get your friends onboard!
I'd like to stress that CTFs are available to everyone. Many challenges do not require programming knowledge and are simply a matter of problem solving and creative thinking.
Challenge types
Jeopardy style CTFs challenges are typically divided into categories. I'll try to briefly cover the common ones.
Cryptography - Typically involves decrypting or encrypting a piece of data
Steganography - Tasked with finding information hidden in files or images
Binary - Reverse engineering or exploiting a binary file
Web - Exploiting web pages to find the flag
Pwn - Exploiting a server to find the flag
Please decode this:4%G#n+Wc?tpPU!b!Dv]RBfXx\ZP\n39iI+F;:SY,F!x9(B(3@E_(mwc7F2
Where do I start?
If I managed to pique your curiosity, I've compiled a list of resources that helped me get started learning. CTF veterans, feel free to add your own resources in the comments below!
```

需要对以下字符串进行解密：

```
4%G#n+Wc?tpPU!b!Dv]RBfXx\ZP\n39iI+F;:SY,F!x9(B(3@E_(mwc7F2
```

再BASE92解码，得到：

```
http://www.hiencode.com/base92.html
```

解码结果：

```
3KJ5e1uPn6D6ecMJWG8zkBSWHso39Qs9vfy8HB3VmmuEmVn
```

再BASE58解码：

```
flag{You_Are_Really_Decode_Master}
```

0x02.[Misc]I_Love_Math-Closed

```
参考由三星主办的 Hacker's Playground 2021的meLorean题目的wp。
https://a1eaiactaest.github.io/blog/writeups/mlwriteup.html
```

数据集为：

```
 [(376, 38462.085), (485, 49579.895), (28, 2964.377), (390, 39888.567), (222, 22753.108), (388, 39685.235),
(24, 2556.346), (204, 20916.088), (45, 4698.592), (9, 1026.251), (428, 43765.177), (334, 34176.356), (205,
21018.683), (218, 22344.21), (69, 7146.245), (347, 35503.166), (479, 48967.208), (213, 21834.244), (227,
23262.95), (460, 47029.989), (118, 12144.819), (491, 50192.035), (44, 4596.27), (241, 24690.668), (476,
48661.456), (18, 1944.416), (427, 43664.197), (214, 21936.838), (274, 28056.588), (272, 27853.2)],
 [(85, 8348.621), (346, 33665.322), (101, 9900.75), (286, 27845.358), (490, 47634.336), (256, 24935.159),
(499, 48507.783), (384, 37352.466), (314, 30561.655), (47, 4662.515), (279, 27166.774), (449, 43656.702),
(415, 40358.941), (335, 32598.173), (445, 43269.738), (257, 25033.479), (56, 5535.53), (484, 47053.0), (24,
2431.123), (447, 43463.332), (252, 24547.35), (269, 26197.073), (375, 36478.885), (467, 45404.153), (299,
29106.661), (410, 39874.781), (111, 10870.232), (162, 15817.212), (473, 45985.348), (428, 41620.527)],
 [(482, 59363.599), (493, 60717.612), (242, 29842.836), (403, 49645.494), (257, 31687.884), (418,
51490.659), (382, 47062.795), (172, 21232.594), (409, 50383.537), (37, 4627.411), (113, 13975.622), (283,
34886.502), (62, 7702.363), (438, 53951.295), (95, 11761.148), (164, 20248.214), (270, 33287.123), (60,
7456.365), (89, 11023.68), (165, 20371.405), (222, 27382.086), (416, 51244.099), (433, 53335.646), (422,
51983.683), (29, 3643.292), (466, 57395.086), (109, 13483.208), (200, 24677.075), (371, 45710.712), (325,
40052.51)],
 [(214, 10596.501), (338, 16672.817), (383, 18878.996), (198, 9813.117), (149, 7411.18), (439, 21621.139),
(12, 698.274), (30, 1580.109), (425, 20935.333), (372, 18338.869), (52, 2658.353), (282, 13928.514), (421,
20740.908), (242, 11968.381), (223, 11037.519), (46, 2364.361), (314, 15497.448), (225, 11135.62), (210,
10400.927), (168, 8342.544), (104, 5206.607), (175, 8685.26), (437, 21523.478), (55, 2805.311), (419,
20642.936), (79, 3981.11), (473, 23287.359), (207, 10253.953), (379, 18682.114), (498, 24512.699)],
 [(444, 22697.484), (201, 10303.965), (442, 22594.985), (268, 13720.463), (215, 11018.358), (64, 3316.136),
(99, 5101.527), (117, 6019.476), (42, 2194.3), (235, 12037.331), (447, 22850.954), (491, 25093.206), (400,
20452.699), (409, 20911.527), (303, 15505.555), (430, 21983.053), (166, 8518.432), (91, 4693.31), (197,
10099.772), (147, 7549.539), (115, 5917.528), (390, 19942.57), (396, 20250.15), (386, 19739.285), (144,
7396.758), (185, 9488.074), (308, 15761.079), (299, 15301.183), (453, 23156.869), (326, 16678.433)],
 [(157, 17994.029), (466, 53219.713), (298, 34067.876), (336, 38400.176), (404, 46152.114), (35, 4085.249),
(370, 42277.13), (74, 8531.099), (38, 4427.459), (356, 40680.902), (461, 52649.548), (103, 11837.351), (287,
32814.011), (153, 17537.147), (105, 12065.227), (165, 18905.831), (383, 43758.064), (14, 1691.277), (149,
17081.899), (48, 5567.135), (60, 6935.317), (183, 20958.053), (425, 48546.553), (124, 14231.309), (154,
17651.315), (305, 34865.077), (225, 25745.798), (22, 2603.436), (260, 29735.779), (268, 30648.491)],
 [(35, 2921.193), (74, 6119.615), (366, 30063.851), (84, 6939.611), (445, 36541.644), (266, 21864.537), (44,
3659.23), (21, 1773.203), (281, 23094.394), (446, 36625.1), (134, 11039.599), (224, 18419.597), (125,
10301.272), (187, 15386.092), (27, 2265.144), (384, 31540.715), (312, 25636.875), (81, 6693.404), (256,
21043.915), (272, 22355.386), (413, 33917.33), (466, 38263.262), (10, 871.15), (322, 26455.254), (491,
40314.018), (285, 23422.235), (299, 24569.304), (314, 25799.903), (472, 38756.921), (207, 17025.119)],
 [(18, 1909.09), (423, 43626.197), (443, 45686.428), (434, 44759.148), (227, 23436.716), (129, 13342.914),
(6, 673.051), (30, 3145.382), (182, 18801.909), (53, 5514.395), (38, 3969.362), (306, 31573.971), (449,
46303.27), (342, 35281.657), (208, 21479.106), (58, 6029.494), (426, 43933.203), (31, 3248.286), (455,
46921.265), (46, 4793.37), (67, 6956.534), (436, 44964.671), (352, 36311.115), (39, 4072.332), (482,
49703.378), (36, 3763.208), (490, 50525.775), (404, 41667.513), (411, 42389.72), (87, 9016.124)],
 [(466, 47119.357), (238, 24091.99), (378, 38231.425), (397, 40151.664), (62, 6315.361), (16, 1669.443),
(495, 50048.255), (248, 25101.314), (97, 9850.418), (496, 50149.486), (250, 25303.773), (254, 25708.162),
(151, 15304.476), (298, 30151.49), (39, 3992.359), (301, 30455.131), (487, 49240.674), (137, 13890.614),
(170, 17223.704), (12, 1265.129), (306, 30959.984), (324, 32777.275), (354, 35808.118), (259, 26213.599),
(61, 6214.064), (315, 31869.574), (419, 42373.779), (36, 3689.172), (56, 5709.441), (347, 35101.57)],
 [(128, 10673.706), (410, 34080.113), (400, 33250.109), (495, 41134.303), (102, 8515.216), (388, 32253.575),
(421, 34992.384), (126, 10507.612), (448, 37233.402), (230, 19139.667), (432, 35905.656), (343, 28519.819),
(224, 18641.439), (16, 1377.078), (70, 5859.254), (188, 15653.68), (41, 3452.216), (262, 21795.981), (452,
37565.629), (496, 41218.974), (48, 4033.309), (19, 1626.453), (179, 14906.658), (490, 40720.602), (293,
24368.848), (17, 1460.317), (315, 26195.299), (351, 29182.612), (219, 18226.844), (192, 15985.401)],
 [(366, 17679.993), (311, 15039.672), (144, 7022.587), (56, 2798.177), (40, 2030.32), (86, 4238.677), (393,
18974.814), (409, 19742.828), (266, 12878.464), (53, 2654.169), (356, 17199.18), (233, 11294.64), (70,
3470.511), (89, 4382.363), (80, 3950.705), (378, 18255.237), (139, 6782.707), (120, 5870.596), (31,
1598.134), (492, 23728.638), (453, 21856.637), (210, 10190.151), (47, 2366.403), (306, 14798.785), (235,
11390.721), (22, 1166.112), (471, 22719.415), (108, 5294.502), (413, 19936.025), (329, 15903.103)],
 [(400, 38065.613), (406, 38635.921), (426, 40536.452), (228, 21725.303), (484, 46046.395), (297,
28280.548), (176, 16786.046), (316, 30085.821), (35, 3390.384), (315, 29990.94), (421, 40060.658), (448,
42627.029), (396, 37685.191), (458, 43575.818), (366, 34836.594), (474, 45095.324), (476, 45287.017), (36,
3485.245), (473, 45000.45), (22, 2155.411), (409, 38920.804), (362, 34455.627), (196, 18685.953), (450,
42816.42), (86, 8235.263), (266, 25335.452), (427, 40631.459), (423, 40252.254), (115, 10990.549), (180,
17165.868)],
 [(399, 37977.029), (141, 13467.056), (491, 46716.435), (236, 22491.873), (415, 39497.438), (239,
22776.126), (378, 35981.953), (404, 38452.185), (20, 1971.333), (392, 37312.171), (348, 33131.705), (68,
6531.521), (116, 11091.687), (24, 2351.378), (377, 35886.753), (352, 33511.265), (186, 17741.408), (64,
6151.27), (238, 22681.308), (156, 14891.645), (77, 7386.51), (264, 25151.192), (311, 29616.833), (481,
45766.877), (229, 21826.112), (124, 11851.454), (204, 19452.046), (74, 7101.408), (101, 9666.573), (23,
2256.442)],
 [(462, 22255.567), (404, 19472.985), (148, 7183.731), (116, 5647.385), (54, 2671.354), (129, 6271.643),
(396, 19089.092), (104, 5071.365), (351, 16928.509), (263, 12704.488), (231, 11167.616), (203, 9824.242),
(433, 20865.24), (380, 18319.847), (19, 991.333), (170, 8239.438), (61, 3007.183), (77, 3775.341), (193,
9343.796), (160, 7759.819), (113, 5503.85), (459, 22113.195), (472, 22735.985), (497, 23937.354), (121,
5887.589), (346, 16687.957), (332, 16016.091), (461, 22207.374), (145, 7039.67), (101, 4927.526)],
 [(356, 35695.781), (323, 32396.312), (99, 9995.636), (274, 27495.776), (284, 28495.424), (37, 3795.292),
(114, 11495.772), (381, 38195.254), (415, 41595.773), (45, 4595.278), (205, 20596.234), (418, 41896.749),
(282, 28296.166), (228, 22896.214), (338, 33896.127), (84, 8495.355), (237, 23795.222), (414, 41495.335),
(247, 24795.385), (133, 13395.59), (177, 17795.921), (481, 48195.587), (399, 39995.328), (435, 43595.973),
(476, 47696.302), (347, 34797.091), (75, 7595.72), (224, 22495.502), (402, 40296.272), (139, 13995.28)],
 [(334, 28161.025), (74, 6320.272), (244, 20600.842), (94, 8000.706), (174, 14720.587), (99, 8420.104),
(484, 40761.531), (493, 41517.869), (447, 37652.765), (49, 4220.412), (499, 42021.241), (298, 25137.81),
(79, 6740.362), (169, 14301.015), (439, 36981.933), (216, 18249.141), (476, 40090.247), (462, 38913.015),
(413, 34798.204), (480, 40424.342), (491, 41349.055), (150, 12704.648), (433, 36477.326), (13, 1196.272),
(400, 33705.346), (114, 9680.556), (127, 10772.474), (62, 5312.143), (295, 24884.463), (230, 19425.274)],
 [(95, 4765.293), (138, 6872.432), (433, 21328.028), (432, 21280.189), (418, 20592.642), (344, 16967.601),
(6, 404.037), (280, 13830.566), (175, 8685.604), (107, 5353.385), (487, 23975.472), (311, 15349.847), (473,
23288.902), (137, 6823.531), (427, 21033.375), (181, 8980.196), (453, 22308.892), (411, 20249.344), (328,
16183.891), (462, 22750.113), (407, 20054.791), (480, 23630.328), (31, 1629.26), (26, 1384.165), (170,
8440.836), (160, 7950.83), (58, 2952.176), (451, 22210.281), (43, 2217.416), (258, 12752.142)],
 [(353, 36485.204), (305, 31540.781), (117, 12176.054), (130, 13515.348), (25, 2700.292), (120, 12485.819),
(436, 45035.347), (254, 26287.979), (168, 17429.391), (484, 49979.295), (283, 29274.878), (112, 11661.515),
(285, 29480.534), (173, 17944.669), (188, 19489.607), (371, 38339.416), (110, 11455.441), (49, 5172.438),
(176, 18253.645), (72, 7541.458), (23, 2494.27), (262, 27111.683), (95, 9910.366), (175, 18150.397), (185,
19180.361), (133, 13824.115), (229, 23712.332), (27, 2906.355), (129, 13412.875), (381, 39369.318)]
```

共18个列表，每个列表中30个元组。第一个想法是为所有 18个列表的每个 x 和 y 创建一个图。

图 (1) 为数据集中的第一个列表

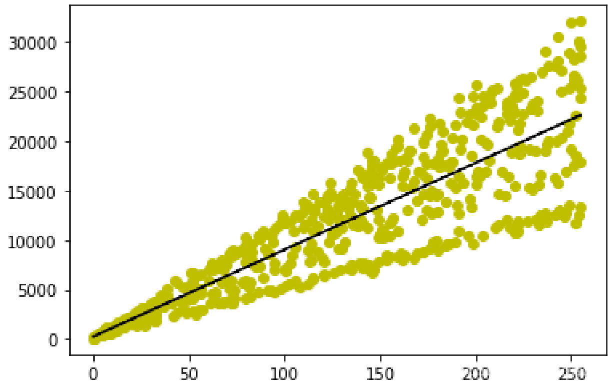


图 (2) 来自数据集中所有列表的数据组合

看到这个图让我想起了一些东西并想到了【线性回归】

一个数据集中有 30 个元素。让我们假设每个列表都对应于flag中的一个字符。

直接套用大佬中的脚本。*smol_sqr(x,y)*函数设计如下：

该函数接受两个参数X 和 是它们应该是包含来自数据集中 25 个列表之一的所有 xs 和 ys 的数组。 让我们计算算术平均值X 和 是 数组。

有了它我们可以计算 出 a 和 b 的近似值。

然后，将每个 a 和 b 的近似值，求出对应的ASCII值，得到flag。

```
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt
import ast
from math import sqrt



dataset = [[(376, 38462.085), (485, 49579.895), (28, 2964.377), (390, 39888.567), (222, 22753.108), (388, 39685.235), (24, 2556.346), (204, 20916.088), (45, 4698.592), (9, 1026.251), (428, 43765.177), (334, 34176.356), (205, 21018.683), (218, 22344.21), (69, 7146.245), (347, 35503.166), (479, 48967.208), (213, 21834.244), (227, 23262.95), (460, 47029.989), (118, 12144.819), (491, 50192.035), (44, 4596.27), (241, 24690.668), (476, 48661.456), (18, 1944.416), (427, 43664.197), (214, 21936.838), (274, 28056.588), (272, 27853.2)],
 [(85, 8348.621), (346, 33665.322), (101, 9900.75), (286, 27845.358), (490, 47634.336), (256, 24935.159), (499, 48507.783), (384, 37352.466), (314, 30561.655), (47, 4662.515), (279, 27166.774), (449, 43656.702), (415, 40358.941), (335, 32598.173), (445, 43269.738), (257, 25033.479), (56, 5535.53), (484, 47053.0), (24, 2431.123), (447, 43463.332), (252, 24547.35), (269, 26197.073), (375, 36478.885), (467, 45404.153), (299, 29106.661), (410, 39874.781), (111, 10870.232), (162, 15817.212), (473, 45985.348), (428, 41620.527)],
 [(482, 59363.599), (493, 60717.612), (242, 29842.836), (403, 49645.494), (257, 31687.884), (418, 51490.659), (382, 47062.795), (172, 21232.594), (409, 50383.537), (37, 4627.411), (113, 13975.622), (283, 34886.502), (62, 7702.363), (438, 53951.295), (95, 11761.148), (164, 20248.214), (270, 33287.123), (60, 7456.365), (89, 11023.68), (165, 20371.405), (222, 27382.086), (416, 51244.099), (433, 53335.646), (422, 51983.683), (29, 3643.292), (466, 57395.086), (109, 13483.208), (200, 24677.075), (371, 45710.712), (325, 40052.51)],
 [(214, 10596.501), (338, 16672.817), (383, 18878.996), (198, 9813.117), (149, 7411.18), (439, 21621.139), (12, 698.274), (30, 1580.109), (425, 20935.333), (372, 18338.869), (52, 2658.353), (282, 13928.514), (421, 20740.908), (242, 11968.381), (223, 11037.519), (46, 2364.361), (314, 15497.448), (225, 11135.62), (210, 10400.927), (168, 8342.544), (104, 5206.607), (175, 8685.26), (437, 21523.478), (55, 2805.311), (419, 20642.936), (79, 3981.11), (473, 23287.359), (207, 10253.953), (379, 18682.114), (498, 24512.699)],
 [(444, 22697.484), (201, 10303.965), (442, 22594.985), (268, 13720.463), (215, 11018.358), (64, 3316.136), (99, 5101.527), (117, 6019.476), (42, 2194.3), (235, 12037.331), (447, 22850.954), (491, 25093.206), (400, 20452.699), (409, 20911.527), (303, 15505.555), (430, 21983.053), (166, 8518.432), (91, 4693.31), (197, 10099.772), (147, 7549.539), (115, 5917.528), (390, 19942.57), (396, 20250.15), (386, 19739.285), (144, 7396.758), (185, 9488.074), (308, 15761.079), (299, 15301.183), (453, 23156.869), (326, 16678.433)],
 [(157, 17994.029), (466, 53219.713), (298, 34067.876), (336, 38400.176), (404, 46152.114), (35, 4085.249), (370, 42277.13), (74, 8531.099), (38, 4427.459), (356, 40680.902), (461, 52649.548), (103, 11837.351), (287, 32814.011), (153, 17537.147), (105, 12065.227), (165, 18905.831), (383, 43758.064), (14, 1691.277), (149, 17081.899), (48, 5567.135), (60, 6935.317), (183, 20958.053), (425, 48546.553), (124, 14231.309), (154, 17651.315), (305, 34865.077), (225, 25745.798), (22, 2603.436), (260, 29735.779), (268, 30648.491)],
 [(35, 2921.193), (74, 6119.615), (366, 30063.851), (84, 6939.611), (445, 36541.644), (266, 21864.537), (44, 3659.23), (21, 1773.203), (281, 23094.394), (446, 36625.1), (134, 11039.599), (224, 18419.597), (125, 10301.272), (187, 15386.092), (27, 2265.144), (384, 31540.715), (312, 25636.875), (81, 6693.404), (256, 21043.915), (272, 22355.386), (413, 33917.33), (466, 38263.262), (10, 871.15), (322, 26455.254), (491, 40314.018), (285, 23422.235), (299, 24569.304), (314, 25799.903), (472, 38756.921), (207, 17025.119)],
 [(18, 1909.09), (423, 43626.197), (443, 45686.428), (434, 44759.148), (227, 23436.716), (129, 13342.914), (6, 673.051), (30, 3145.382), (182, 18801.909), (53, 5514.395), (38, 3969.362), (306, 31573.971), (449, 46303.27), (342, 35281.657), (208, 21479.106), (58, 6029.494), (426, 43933.203), (31, 3248.286), (455, 46921.265), (46, 4793.37), (67, 6956.534), (436, 44964.671), (352, 36311.115), (39, 4072.332), (482, 49703.378), (36, 3763.308), (490, 50525.775), (404, 41667.513), (411, 42389.72), (87, 9016.124)]
49703.378), (36, 3763.208), (490, 50525.775), (404, 41667.513), (411, 42389.72), (87, 9016.124)],
 [(466, 47119.357), (238, 24091.99), (378, 38231.425), (397, 40151.664), (62, 6315.361), (16, 1669.443),
(495, 50048.255), (248, 25101.314), (97, 9850.418), (496, 50149.486), (250, 25303.773), (254, 25708.162),
(151, 15304.476), (298, 30151.49), (39, 3992.359), (301, 30455.131), (487, 49240.674), (137, 13890.614),
(170, 17223.704), (12, 1265.129), (306, 30959.984), (324, 32777.275), (354, 35808.118), (259, 26213.599),
(61, 6214.064), (315, 31869.574), (419, 42373.779), (36, 3689.172), (56, 5709.441), (347, 35101.57)],
 [(128, 10673.706), (410, 34080.113), (400, 33250.109), (495, 41134.303), (102, 8515.216), (388, 32253.575),
(421, 34992.384), (126, 10507.612), (448, 37233.402), (230, 19139.667), (432, 35905.656), (343, 28519.819),
(224, 18641.439), (16, 1377.078), (70, 5859.254), (188, 15653.68), (41, 3452.216), (262, 21795.981), (452,
37565.629), (496, 41218.974), (48, 4033.309), (19, 1626.453), (179, 14906.658), (490, 40720.602), (293,
24368.848), (17, 1460.317), (315, 26195.299), (351, 29182.612), (219, 18226.844), (192, 15985.401)],
 [(366, 17679.993), (311, 15039.672), (144, 7022.587), (56, 2798.177), (40, 2030.32), (86, 4238.677), (393,
18974.814), (409, 19742.828), (266, 12878.464), (53, 2654.169), (356, 17199.18), (233, 11294.64), (70,
3470.511), (89, 4382.363), (80, 3950.705), (378, 18255.237), (139, 6782.707), (120, 5870.596), (31,
1598.134), (492, 23728.638), (453, 21856.637), (210, 10190.151), (47, 2366.403), (306, 14798.785), (235,
11390.721), (22, 1166.112), (471, 22719.415), (108, 5294.502), (413, 19936.025), (329, 15903.103)],
 [(400, 38065.613), (406, 38635.921), (426, 40536.452), (228, 21725.303), (484, 46046.395), (297,
28280.548), (176, 16786.046), (316, 30085.821), (35, 3390.384), (315, 29990.94), (421, 40060.658), (448,
42627.029), (396, 37685.191), (458, 43575.818), (366, 34836.594), (474, 45095.324), (476, 45287.017), (36,
3485.245), (473, 45000.45), (22, 2155.411), (409, 38920.804), (362, 34455.627), (196, 18685.953), (450,
42816.42), (86, 8235.263), (266, 25335.452), (427, 40631.459), (423, 40252.254), (115, 10990.549), (180,
17165.868)],
 [(399, 37977.029), (141, 13467.056), (491, 46716.435), (236, 22491.873), (415, 39497.438), (239,
22776.126), (378, 35981.953), (404, 38452.185), (20, 1971.333), (392, 37312.171), (348, 33131.705), (68,
6531.521), (116, 11091.687), (24, 2351.378), (377, 35886.753), (352, 33511.265), (186, 17741.408), (64,
6151.27), (238, 22681.308), (156, 14891.645), (77, 7386.51), (264, 25151.192), (311, 29616.833), (481,
45766.877), (229, 21826.112), (124, 11851.454), (204, 19452.046), (74, 7101.408), (101, 9666.573), (23,
2256.442)],
 [(462, 22255.567), (404, 19472.985), (148, 7183.731), (116, 5647.385), (54, 2671.354), (129, 6271.643),
(396, 19089.092), (104, 5071.365), (351, 16928.509), (263, 12704.488), (231, 11167.616), (203, 9824.242),
(433, 20865.24), (380, 18319.847), (19, 991.333), (170, 8239.438), (61, 3007.183), (77, 3775.341), (193,
9343.796), (160, 7759.819), (113, 5503.85), (459, 22113.195), (472, 22735.985), (497, 23937.354), (121,
5887.589), (346, 16687.957), (332, 16016.091), (461, 22207.374), (145, 7039.67), (101, 4927.526)],
 [(356, 35695.781), (323, 32396.312), (99, 9995.636), (274, 27495.776), (284, 28495.424), (37, 3795.292),
(114, 11495.772), (381, 38195.254), (415, 41595.773), (45, 4595.278), (205, 20596.234), (418, 41896.749),
(282, 28296.166), (228, 22896.214), (338, 33896.127), (84, 8495.355), (237, 23795.222), (414, 41495.335),
(247, 24795.385), (133, 13395.59), (177, 17795.921), (481, 48195.587), (399, 39995.328), (435, 43595.973),
(476, 47696.302), (347, 34797.091), (75, 7595.72), (224, 22495.502), (402, 40296.272), (139, 13995.28)],
 [(334, 28161.025), (74, 6320.272), (244, 20600.842), (94, 8000.706), (174, 14720.587), (99, 8420.104),
(484, 40761.531), (493, 41517.869), (447, 37652.765), (49, 4220.412), (499, 42021.241), (298, 25137.81),
(79, 6740.362), (169, 14301.015), (439, 36981.933), (216, 18249.141), (476, 40090.247), (462, 38913.015),
(413, 34798.204), (480, 40424.342), (491, 41349.055), (150, 12704.648), (433, 36477.326), (13, 1196.272),
(400, 33705.346), (114, 9680.556), (127, 10772.474), (62, 5312.143), (295, 24884.463), (230, 19425.274)],
 [(95, 4765.293), (138, 6872.432), (433, 21328.028), (432, 21280.189), (418, 20592.642), (344, 16967.601),
(6, 404.037), (280, 13830.566), (175, 8685.604), (107, 5353.385), (487, 23975.472), (311, 15349.847), (473,
23288.902), (137, 6823.531), (427, 21033.375), (181, 8980.196), (453, 22308.892), (411, 20249.344), (328,
16183.891), (462, 22750.113), (407, 20054.791), (480, 23630.328), (31, 1629.26), (26, 1384.165), (170,
8440.836), (160, 7950.83), (58, 2952.176), (451, 22210.281), (43, 2217.416), (258, 12752.142)],
 [(353, 36485.204), (305, 31540.781), (117, 12176.054), (130, 13515.348), (25, 2700.292), (120, 12485.819),
(436, 45035.347), (254, 26287.979), (168, 17429.391), (484, 49979.295), (283, 29274.878), (112, 11661.515),
(285, 29480.534), (173, 17944.669), (188, 19489.607), (371, 38339.416), (110, 11455.441), (49, 5172.438),
(176, 18253.645), (72, 7541.458), (23, 2494.27), (262, 27111.683), (95, 9910.366), (175, 18150.397), (185,
19180.361), (133, 13824.115), (229, 23712.332), (27, 2906.355), (129, 13412.875), (381, 39369.318)]]

 def smol_sqr(x,y):
     n = len(x)
     x_mean = sum(x)/len(x) # x with a dash
     y_mean = sum(y)/len(y) # y with a dash
     a_hat = [0,0]
     for i in range(n):
         sub_mean = x[i] - x_mean
         y_sub_mean = y[i] * sub_mean
         sub_mean_sqr = sub_mean**2
         a_hat[0] += y_sub_mean
         a_hat[1] += sub_mean_sqr
         #print('x: %d, y: %.2f, %.2f, %.2f, %.2f' % (x[i],y[i],sub_mean,y_sub_mean,sub_mean_sqr))

     a_hat = a_hat[0]/a_hat[1]
     b_hat = y_mean - x_mean * a_hat
     # print('a-hat: %.10f, b-hat: %.10f' % (a_hat, b_hat))
     return a_hat, b_hat

 for i in range(len(dataset)):
     data = dataset[i]
     x,y = [], []
     for d in data:
         x.append(d[0])
         y.append(d[1])

     ret, _ = smol_sqr(x,y)
     print(chr(round(ret))+chr(round(_)), end='')
 # flag{L1n34r_R3g7e5S10n_A_G0Od_Th1ng}
```

0x03.[Misc]-

0x04.[Crypto]signin-Closed

```
 ZnJvbSBzZWNyZXQgaW1wb3J0IGZsYWcKZnJvbSBDcnlwdG8uVXRpbC5udW1iZXIgaW1wb3J0ICoKCm0gPSBieXRlc190b19sb25nKGZsYWc
pCgplMSA9IDY2NzQzMDEwNDg2NTI4OQplMiA9IDUzNzQwOTkzMDUyMzQyMQpwID0gZ2V0UHJpbWUoNTEyKQpxID0gZ2V0UHJpbWUoNTEyKQp
uID0gcCpxCmMxID0gcG93KG0sIGUxLCBuKQpjMiA9IHBvdyhtLCBlMiwgbikKCnByaW50KGYnYzEgPSB7YzF9JykKcHJpbnQoZidjMiA9IHt
jMn0nKQpwcmludChmJ24gPSB7bn0nKQoiIiIKYzEgPSA2NTkwMjY3ODU3MjcyNzcyNDE3OTE3NjQ5NjU3Mzk2ODk5NzE4MjcxMjA2MzMxNzA
4MjI4OTEyMDQ1MzA5NDA2ODE5OTMyNTQxOTk4OTY4ODM4MjE3NzgwODUyOTA0MjMyMjIxNzg4NzMzNDAwNTA4NDUwNDc5NjM5NzIyMDgwNDg
1NjE2NzI1NTE3NjQxNTY5MDIxNzM0ODI1MjEyNjA5NzgwOTEzMDE5NTIwODAyMDY5NDAyNjI1MDE5NDA0NzQ2MDU4MTE2NTAyNDE3ODM1ODQ
zNDMwNTQ5NTM2NDk4MzgzMDc1NjU1MjM3OTMzNTk4NTM5OTg3NjUyODkyMjA3NjAzMDU5NTIzMjY3OTA0Njk0MTMxMDc4NjYzNzI2MDc2NDk
5MjQ5OTM3NTQyMTQ2NDUyOQpjMiA9IDg1ODA5NDAzNjc4MjUwMTUwMTUzMjkxNDcxMTg1OTk5ODA1ODcwODU4MTIzMDAxMjczMDM0MjEyNTg
yODQ3NzMxODI1Mjk2ODkxMDE2ODEwODcxMzk3NTQ2MTM0MTE3MDEyMTk3NTk5NjUxNzI5NDAxNTkwOTgwMDIwMDI4MzgyODg0MDY4NTEzMjA
xNzU4OTI2NDE2MTkyMjExODIxOTIyNTkzNjg2MjMyNDc1OTY3ODA4OTY0MDA2Nzg2MDc2NDYwMTYwNDI4NjM5MzUzMTUzNjU4MzIzMjA4MTE
5NDUzMDU1MDcwMTk5MjQzMjk1MzMwNTIyODA0OTc0ODQ5MzMwOTI2NTAxMDkxNDMwNDE5Nzc1MTU1NjcwMjY0MzA2MjIyOTYyNDEzMjg5NjE
2OTU3NTE5Cm4gPSA5MzAxMjM3OTk0OTU5NjY3OTg3NDAxMDgzNjUyMDk3MjQ2MzQzODE1NTE3NTk2MTI4MzI3Nzc0MzUxNDIwMzg3MTExNDM
yOTAwODA0NDczNTUwMDcyNjQ0MDAxMjQ2NDAyOTE0NDIwNDgxMzQxMzkwOTMyMjM4OTU4NTk2NjMxMzQyNjYxMTQ4ODkyNzI5Mjg3NDMxOTY
yODA2MzUyNjAwOTQwNTE0NDQzNjYwNTk5NjM4OTk4NTk3NzM0MDI4MDk4MzQ2OTgwMzQxMjExOTQ1ODE4NTA0NzQ3NTI1MzA1OTYzNjEyNjU
1NTQ1MTU1NzM0ODE2OTUxNDk3NTI0OTcxMDkwMTg5OTUyNjk3NDI0NjEzOTU1OTczMDQ2MTU0MDY2MDk5MDM3NTAzNDY2OTA0Mjk1OQoiIiI
=
```

BASE64解码，得到密码学的代码：

```
from secret import flag
from Crypto.Util.number import *

m = bytes_to_long(flag)

e1 = 667430104865289
e2 = 537409930523421
p = getPrime(512)
q = getPrime(512)
n = p*q
c1 = pow(m, e1, n)
c2 = pow(m, e2, n)

print(f'c1 = {c1}')
print(f'c2 = {c2}')
print(f'n = {n}')
"""
c1 =
6590267857272772417917649657396899718271206331708228912045309406819932541998968838217780852904232221788733400508450479639722080485616725517641569021734825212609780913019520802069402625019404746058116502417835843430549536498383075655237933598539987652892207603059523267904694131078663726076499249937542146452 9
c2 =
8580940367825015015329147118599980587085812300127303421258284773182529689101681087139754613411701219759965172940159098002002838288406851320175892641619221182192259368623247596780896400678607646016042863935315365832320811945305507019924329533052280497484933092650109143041977515567026430622296241328961695751 9
n =
9301237994959667987401083652097246343815517596128327774351420387111432900804473550072644001246402914420481341390932238958596631342661148892729287431962806352600940514443660599638998597734028098346980341211945818504747525305963612655545155734816951497524971090189952697424613955973046154066099037503466904295 9
"""
```

很明显是共模攻击的变形。这里的e1, e2加密指数不互质，存在共同的公约数3。

```
from Crypto.Util.number import *
from factordb.factordb import FactorDB


e1 = 667430104865289
e2 = 537409930523421
f = FactorDB(e1)
f.connect()
print(f.get_factor_list())
f = FactorDB(e2)
f.connect()
print(f.get_factor_list())
```

执行上面的脚本，得到：

```
[3, 222476701621763]
[3, 179136643507807]
```

直接套用[共模攻击的变形]脚本：

```
 import  gmpy2
 import  libnum

 n=930123799495966798740108365209724634381551759612832777435142038711143290080447355007264400124640291442048
134139093223895859663134266114889272928743196280635260094051444366059963899859773402809834698034121194581850
47475253059636126555451557348169514975249710901899526974246139559730461540660990375034669042959
 c1=65902678572727724179176496573968997182712063317082289120453094068199325419989688382177808529042322217887
334005084504796397220804856167255176415690217348252126097809130195208020694026250194047460581165024178358434
305495364983830756552379335985399876528922076030595232679046941310786637260764992499375421464529
 c2=85809403678250150153291471185999805870858123001273034212582847731825296891016810871397546134117012197599
651729401590980020028382884068513201758926416192211821922593686232475967808964006786076460160428639353153658
323208119453055070199243295330522804974849330926501091430419775155670264306222962413289616957519

 e1 = 667430104865289
 e2 = 537409930523421
 e1e2 = e1*e2

 def rsa_gong_N_def(e1,e2,c1,c2,n):
     e1, e2, c1, c2, n=int(e1),int(e2),int(c1),int(c2),int(n)
     s = gmpy2.gcdext(e1, e2)
     s1 = s[1]
     s2 = s[2]
     if s1 < 0:
         s1 = - s1
         c1 = gmpy2.invert(c1, n)
     elif s2 < 0:
         s2 = - s2
         c2 = gmpy2.invert(c2, n)
     m = (pow(c1,s1,n) * pow(c2 ,s2 ,n)) % n
     return int(m)

 def de(c, e, n):
     k = 0
     while k<1000:
         mm = c + n*k
         result, flag = gmpy2.iroot(mm, e)
         if True == flag:
             return result
         k += 1

 c=rsa_gong_N_def(e1, e2, c1, c2, n)
 e=gmpy2.gcd(e1,e2)
 m1=de(c,e,n)
 if m1:
     flag=libnum.n2s(int(m1))
     if "flag" in flag:
         print(flag)
 # flag{e6e5722e-4b9a-11ec-b784-00155d9a1603}
```

0x05.[Crypto]-

0x06.[Web]Ser-Closed