赛题数据中题目$i(1\leq i\leq 12)$相关符号说明如下：

(1)RSA 密码的公开密钥为(e_i,N_i),用户秘密保管的私钥为d_i,其中$N_i=p_i\times q_i$是两个 512 比特素数的乘积,私钥d_i满足$d_i\times e_i\equiv 1\mathrm{mod}((p_i-1)\times(q_i-1))$;

(2)密文数据$c_i\equiv {m_i}^{e_i}\mathrm{mod}N_i$，这里$m_i$是明文消息字符串$M_i$经编码后的整数值并且满足$1\leq m_i\leq N_i$;，即$m_i$的取值范围为[1,$N_i$];

(3)为降低赛题求解难度,用户的私钥d_i特定比特位置的密钥信息发生泄漏，即本赛题每组数据均额外已知部分密钥信息;

(4)记 MSBs 为最高数位比特 (Most Significant Bits), LSBs 为最低数位比特 (Least Significant Bits). 以整数$e=65537$=0b10000000000000001 为例,其比特长度为 17, 其中最高 10 位比特 MSBs 的二进制形式为 0b1000000000=512，最低 7 位比特 LSBs 为"0000001",其二进制形式为 0b1=1,满足关系：$65537=1+512\times 2^7$.

题目 1：25 分

N_1=0xa4d80845630d3b332f74f667ec8a0e49aba15b6f0c4f4006161d62c91b78cf6811421cc76609d2d9dba2c43be9d8ecdc6a0dff64a8041dcde52c7f92820b0a38fc91419e8ec9a5c69d47edc6e347934b4d87f97c5759886dac6c1143ff55b8eb11acfaa6cc70956a8ec7796e1a063b123bc2e467e30937c5a69c7ab5f8ed17e1;

e_1=0x3458c2e97adef45f741c7db11ece6c0814aa5b6fad9144242cdaa16a6b4f3622477935f98a41765b92892b4de22a391cf08767447df113f5151c86edd109b97f9b045fd8ad5d7a51084684d4e2353db6c0e474d5d79f399a2bf4fd867ec85b7960845ab5497f705914912f797804c06dcff57139e040596d22b141e54835e0d3;

c_1=0x91b097a5b1f6b12accdbda15cd2247384e1b3ed8311085a0f3e0dbb5fffce650a355600a02674189d1b7f4075df079c70354a08646e85ecf31dd150220cd1d4ce22d55a946500f4bd8def74fb0acea3e8d2e7bb1d27ebf2ca2e80fc28c3f0d88a041d4a556a18147f66b88c65f19c99b4b94c3f78d468b8accb4da7e7ce31b29;

已知信息: 私钥 d_1 的取值范围为[2^{249},2^{250}]。

题目 2： 30 分

N_2=0xd231f2c194d3971821984dec9cf1ef58d538975f189045ef8a706f6165aab4929096f61a3eb7dd8021bf3fdc41fe3b3b0e4ecc579b4b5e7e035ffcc383436c9656533949881dca67c26d0e770e4bf62a09718dbabc2b40f2938f16327e347f187485aa48b044432e82f5371c08f6e0bbde46c713859aec715e2a2ca66574f3eb;

e_2=0x5b5961921a49e3089262761e89629ab6dff2da1504a0e5eba1bb7b20d63c785a013fd6d9e021c01baf1b23830954d488041b92bca2fe2c92e3373dedd7e625da11275f6f18ee4aef336d0637505545f70f805902ddbacb21bb8276d34a0f6dfe37ede87dd95bb1494dbb5763639ba3984240f1178e32aa36ee3c5fcc8115dde5;

c_2=0x6a88a8fa2b8f28d96284298bab2061efeb35e3a086370e19523c15c429f5d783b9d4f32e31a402916f45ad4f2760ab30e77177335af44756bfbeef0f168b5e0dc8c3ddf75d141c358969cca0e7c2b8ab99ef8e33b031be1cbccd95b687682ac7b0dcc0d56f5651ee671d6358128d2e0801f247a6af4fe0dc5e8fb199eba0780f;

已知信息: 私钥 d_2 的取值范围为[2^{285},2^{286}]。

题目 3：40 分

N_3=0xf4c548636db62ffcc7ac4a0797952bea9a65bd426175af2435f72657e67ec8194667bfa94ce23c6f1e5baf3201867ab41701f6b8768e71009c41a3d5e9e7c109455341d549c7611f9f52851a2f017

906aa9ccbedb95d238468e2c8577d30ecc4f158e3811fd5e2a6051443d468e3506bbc39bba710e3
4a604ac9e85d0feef8b3;

e_3=0x16f4b438ba14e05afa944f7da9904f8c78ea52e4ca0be7fa2b5f84e22ddd7b0578a3477b19b7
bb4a7f825acc45da2dd10e62dbd94a3386b97d92ee817b0c66c1507514a7860b9139bc2ac3a4e0f
e304199214da00a4ca82bfcb7b18253e7e6144828e584dac2dfb9a03fabaf2376ce7c269923fbb60f
c68325b9f6443e1f896f;

c_3=0x26b1823cf836b226e2f5c90fdcd8420dbfcd02765b26e52ef3e5c0ab494c2f4650e475e280b0
b5fff0d5016621186420b09e4706a5866e4a3319f23ef09d92c4e36acba39a0f6213fbe5ee1a736ce
383e6e12351e6cbfd43f10a96b7fe34bdbaf948f2fb075d9063723c9f747fe6247ae9209e5d417faf2
e37e6fee2eb863556;

已知信息：私钥 d_3 的取值范围为$[2^{299},2^{300}]$。

题目 4：40 分

N_4=0xd46dd141810786e451320ca452b379024fd263501ae767760f3dcf34b79806b85e36b0fee53
8dac61a5872c37d051a8a026384d09f12b7e1adae7eb15c4d75878007ee0043c2186cf8999c59eb
66f689f55baf190bd80e70bf47b553be76bd4efffc782a51b43314d54b83fc19461e1beb6021164f6
4723b505e5a619cb62335；

e_4=0x92fbeeef2d40eb125234cfe4c063c4607f12aec7e3014b32fb4600e58c4eac1ec485192a1b03
745632f2966311ad68bd1e49dd9d08b2bff67f58e214c8d7bae0142559994c24e347ff7555c86aa3
0ccd03cf794e6f00eead7f15e24f33da61fae11ec81e4e09bcc76c1a0ed5ca8c2f512856cdb42470be
ee7111a2410188697d；

c_4=0x8c5e9db89f96d769f6514836407755caf71b7bc6f5db2246200b0f824dac7ea3be5ba022c0e1
91d76c69b7d20c7cad5c49e381479c7cbe7ba055ce8aec2cad1a19d42aa5c4b8c07c67e22c702898
91d53c3d55dff50e506ec7fb480df44f9b3219f8c73e0702d8072e9f6aabed8bb5d35f583bea30ce8
50b154d4fd8c39e4fb8；

已知信息：私钥 d_4 的取值范围为$[2^{399},2^{400}]$,此外已知 d_4 的汉明重量较轻，其最高 310 位比特（MSBs）汉明重量不超过 5，剩余 90 位比特较为随机.

题目 5：30 分

N_5=0x94eab94581f4931a5ea6aabcfe0598600fa3e0a06573887aed69e274f14484472dc3feaf50d4
ef384e502f747f5605c1d2a4c8172b6ef134b7e96d6c383a9cb967ccbbd8b3647848d34928982a27
4999c2df00bd7dd11bf25acd61411e3395637e85dd84ecf785ff1027eed91f3976c8186e2e940edcb
5fed8d759a5028b47a1;

e_5=0x124c552642ef2467aaecde51b0f3e1bee2ebe87bae39a956ad56cf7eec669cdc7b9664ea435
b4c3492b8e610e0a182e1a76c7af443ca2962672b4e703c4f359cf8d88a67db77be2491b74bcdae5
8691b69e6ea06d067815b26fc0d669d8c06f11a728154dc8cdf983a056633fecadc417df4304625c3
e6f91ec3d655a91a29e9;

c_5=0x63e09028c774513b5420236f8405f970c8d97c8347697c44f50b23e5cc964c921413b5e6742
bb5ba7ef49f032e372f502babc0040f9c7cc2c9f4e27d18aefff0e764529ba70f6a7b22d525d0aaeb1
d21432817b6b148b8143c80a6401a5c9adfecf0c033181bb076a2192a4866c5355c9e401fba78d5f
22b9c1661c0065a1a28;

已知信息：私钥 d_5 的取值范围为$[2^{511},2^{512}]$,此外 d_5 的最高 256 位比特 MSBs(记为 dm)及最低 176 位比特 LSBs(记为 dl)取值均已知，但是中间 80 位比特(记为 dx)取值未知，即满足如下关系：d_5= dl+dx*2^{176} +dm*2^{256}，具体取值如下：

dl=0x2b26d177dc20ceea15de6e3c5a03207fb326a42d53a9；

dm=0xacfad4bbb97a99b6bbc82c8b44a5260bcfe9c4a0acf437186ff4d5d1594cc5c1。

题目 6：40 分

N_6=0x94e4c83c67c6d6e33d83cc2953df899e8c4b33894f653d5bbc84d7dd9058e6949221897f6e5b7b8bd9013f495c906862e401436e77be585474066f6c220751dd9b2b8be66f07ad7f090547a6e759e482ba263b941b32c27c62c4b558d96dda168b28c52e550b7d7ff145a5996c0b398714cf5ee8f0ea1a3d5b17c592f1c15275;

e_6=0x949b2e72766be1e83ee278a56bc86a2d3268b719507068ac62c6d249a810284edaac39335e8d699630887c13864f4cdf1c0c423b2f7ae88ccc60a827332e6c410800c7c7a1677918c28aa51086991d1290fc64b8e1b0f14b482f35d86139bb3491a59e2ad99dcd35bd129a44c3b8e2667e405dc2d307a5bb5a1504d7ded3bda3;

c_6=0x6fd6fae8ab4e95e622e5dad2921c6f12e911df08768abf2d10d212ad9a26e4c5ec71640d7a6b3488064fd424224bc2c762b956af95a3212de37a57d74c0299936f48ae3d8b8803e644e8d1306ab735c94fd815fe8c77982b32d51e9b6f3b3d4f3753810b61fb528c3e9eb774dabd93a3c5c9919ae3fb90e8e998ed3e7f949738;

已知信息：私钥 d_6 的取值范围为[2^{559},2^{560}],此外 d_6 的最高 123 位比特 MSBs(记为 dm)取值未知，但其剩余 437 位比特(记为 dl)取值已知，即满足如下关系：d_6= dl +dm*2^{437}，dl 具体取值如下: dl=0x6da211f0d34b。

题目 7：30 分

N_7=0xaeb75bb97217271bf312a7897da81a544fe469ba0f1cf75304f2a5629717e1e3d0a9a28e71135443cc19f78c60dd3f7ea4ea28ae64657d5ac3b46e9755020de73cb5c4f89a682e0193916221bc8f4abb595f2c058bbb99e199a66144a9a9b258a74db847b2460107233280c94e854394595043f62bf77cd96c9ed3eca71b726d;

e_7=0x42b63e1113b4a84d0b037006a9bb729b52db495fa6b475bb64129a855a4ed6511792d0df946c5d7e22085d0db07bce5e408454a61c0cea51cf6d25e2455a2c6dc092e4b09bf4efb2157ffc1d1db3e969499479d721330ec4ac864e656318bc7bb9831a0dccf582406c87ae5d3ab9ffec351271dbb5481a0b6ed75a760b4f7e0d;

c_7=0xe1f90d9f115f9ba0b65ea8826ffec785bbe1b195fbb6f93c6ea28940f0d9b571930addb3e2714999ba5a19d17af22f1bc8da49f8b515ab03b6d276140b69fedf980d1aef78d0f3c0f6effdf2e92ce9195866f856720375370211 78f8c65989b57f29de2c4c9306fe3e13aef29f962f86b8d5216907e85f28260b9f41cfe2651;

已知信息：私钥 d_7 与 phi_7=(p_7-1)*(q_7-1)很接近,据估计,phi_7-d_7 的取值范围为[2^{267},2^{268}] 。

题目 8：30 分

N_8=0xf12eac2099c4190a6f586bea0b4fc3f9dff4f23f0cb8e42cbeff950aa1df8a373c49df7974fb33b4b6619eadb2d6c01f80da1b433295b199df11b323114c439884eb31fa568bd747ae37079e885e2490c3b5a56d61b9d10533983ff78fe85e07876fe2ae07ae7ea1c71f0f9c2d6beccdcd8baf046a58549aec19d45d48d7d92d;

e_8=0xb8906f5097658f27cc448d98974d9e7ccd4e8a8f25a80007826c341dcb2ac42420f899e5a89045fbefd9163bc94e6f98b4953546203be4bec249031587a27dbf;

c_8=0x162a6dee8bcbe24698b9249137c2a157890910fa74a56e7d2792b5b4f29112aba03448995ff32ed24bec5118f7433212196d3f99e1c794b61395d8183e4658c9dc05953a87c069c9390773c7f885907840ebd29676afac7bf3374d54c81c4e404f09716b9885d243c41dc48db561f8291b88826cae3

2bfd575a472e523f455c4;

已知信息：私钥 d_8 的最低 900 位比特 LSBs(记为 dl)取值已知，剩余约 124 位比特(记为 dm)取值未知，即满足如下关系：

d_8= dl +dm*2^{900}，dl 具体取值如下:

dl=0x4cbec287edc86c5b2a9e1975d64d2a24d3930075f0d445163c7b1ceec9ee0319fe1166af348b49004d2420b83bcb82d4879e93dba01ee76c5ca1b7141490465e824bdb5e91d04016c6bbbaa41c4470747ee8163f710b2d8adb8ab2168dcc996b5ab5f85a2269dc459379fb68848cec487

题目 9：30 分

e_9=65537

N_9=0xcc5b706f373a79c680cec9527aac573fd435129cf16c23334085bf97832e5a6c78b633c2f244b12a62f87ec5295dd89fcf3c808c39e45a9afdbda2f8d2d0b50d61b685c0fe9eb41a7018a40f98892f96d738e2a4e740d4e507bcbd07f68c1ecb2ca10bd780ce65265a7e4da00f1031a5db9d038878a29a5ffefcaf2119720005;

c_9=0x20bac8a7d73a74c9913377846c13c3d2bd9f47e6df118d1486a96ed184ca9910e0f250500065cfb44105a41dff655364cabc3067ef3cd3d7d983e75c9303b786ac97507cfe803b788b12e582232028ca9772d05004aef194076ec442e3ee55e17fbb4a57f332b4393ac056c024141cc2b82f9dbc6d3c77f6eff20cd0ecc9cbab;

已知信息:

私钥 d_9 的最低 530 位比特 LSBs 取值(记为 dl)已知，剩余高位比特(记为 dm)取值未知，即满足如下关系：

d_9= dl +dm*2^{530}，dl 具体取值如下:

dl=0x20142ae2802b877eb4dfa8a462e7d017c4d348181c367fd1a661ec9b6bbcca9dcb6601ccb6c10416b7f3c20129527346bbc136ee60f9945125cba03a9bba3720f7411

题目 10：25 分

e_{10}=65537

N_{10}=0x8d0df1ce526c39f9b057de462778a61ceda2049c7e32ee99d40baa4b22b7fd438e9ca1dfd7467684625add252095ee97c698199f4c5991279f6d3e74d4c14d01d137d42722df0d4565ff2a5275f9cac66dc4dfdf3304f85cbdc3d18eda1e32ac5d03675141a722ceefe0ea0533b53d7e50ed7eda1a1bbce47ed0ecb966f8678d

c_{10}=0x3b42fa3dc9089a21e9dabfe18297df47272f7e0ff59bf9bf16bc55e7fa70504c03fed56ca5ae93ac028f60ce5da3c145c6d181c5bd3c267288ec4765a19ca6b957b4535a1a185bd1b87d2e39b30e2430ed648175c29fdc1fde3787c426783dd66ba17f98b42ba13a7b3532970d0aa31b5ffa5f3eae243337a1668bae456bfbfb

已知信息：私钥 d_{10} 的取值范围为[a,b],a 和 b 的具体取值如下

a=0x19ffe8024fcf0320b3107f380f2e7deff71d561c4266c0f439d1aca20cd43d2aa6aed8679a16b2e1d3ff4ba3fc4da69cf34e35ead6f7eb79923960b9c83d9923e591b07b65275bf67f0b3d424cd7e6e6dd88ea39a5cfa27ecee61caaacc93e751dbb2a4c196f0ce0c36d44c35d6658d71b6c48b7b29400ab9161a0000000000

b=0x19ffe8024fcf0320b3107f380f2e7deff71d561c4266c0f439d1aca20cd43d2aa6aed8679a16b2e1d3ff4ba3fc4da69cf34e35ead6f7eb79923960b9c83d9923e591b07b65275bf67f0b3d424cd7e6e6dd88ea39a5cfa27ecee61caaacc93e751dbb2a4c196f0ce0c36d44c35d6658d71b6c48b7b29400ab9161affffffffff

题目 11：40 分

e_{11}=65537

N_{11}=0xcb5645c59c402b0edcf96cbd6a7308b64aac2f37a3c6f96be7c421c4b7f0a4adbdecd88cbea1128352fb21baae583fe4ceb3fc93c4905803ad3e9214ada050d5c0ff785a13a5c9157c3154ad8d7015a2d239fe13ef836d3279c5cd5dc96013ac40f372a9c9226d2f5fe73f312c56e11d9cdfbf9fb0db627ac1a752f5f0bd2b29

c_{11}=0x84e4aa0be481e9c4bbd4c71dba5235cccd8312759de35c326c7e4cdda494196d1c0cae298240942af3082fac215965999c908a79bf07e093ee0c402e727a09a1c1f13831875d66ebbc3f89507163de90339af055bcd7d778574775214accfbd8ae20001f27bc196b974cb3ac215fea3debb7b17a21a8ebb1a9880a671539ef21

已知信息：私钥 d_{11} 的取值范围为[a,b],a 和 b 的具体取值如下

a=0x4f77b72b04e6fb2d02e5a43edef4784a2e22df0d42bfc7c9093a58ec35eb21a11962103be960b0088d0cc2e0dfb473bc2ba0a22cea1c73997442c8fab5e4bad22cd131055b0382eb9264ad40ec8257abaff11b33b173ffd0168039bf40dc203eb325d884d2845fd2b5a37f41a0f64183db0c256c244500000000000000000000

b=0x4f77b72b04e6fb2d02e5a43edef4784a2e22df0d42bfc7c9093a58ec35eb21a11962103be960b0088d0cc2e0dfb473bc2ba0a22cea1c73997442c8fab5e4bad22cd131055b0382eb9264ad40ec8257abaff11b33b173ffd0168039bf40dc203eb325d884d2845fd2b5a37f41a0f64183db0c256c2445fffffffffffffffffff

题目 12：40 分

e_{12}=65537

N_{12}=0x9fac422a93f6e486e3ddae088bb5f5d06dec183ab81290042a9c98c53352961a00db3e9def7adff842381a395cedf1d06294f0b63457133e4e44cabb7633c562dcbfffdffe541d66c46ddf6a28b686c478300bcf31945f2a6495f140e64f78fa5cd47d1885233f175f28e38f1bfc422a6853ca19a7dd47a291a9e7de78a67bf1

c_{12}=0x35476c9d0e5ad9d364ea31d8f6628b92a4f6307b1fef754e49286bc7f53ea8cd013a7ebf2a21b2327af44498d267e19526c2051a02f22cca9cab567f7ceefe5003137e396c23742370e14ec2c6a90943ca848908e87420f560d34eae4635475effa867722276710c6f4b6cb9b295777d62f3f03c57603ac815072864aadbf041

已知信息:素因子 q_{12} 是模数 $N_{12} = p_{12}*q_{12}$ 与整数 N 的部分近似公因子，即 $N=k*q_{12}+r$,其中 $2^{511}<k<2^{512}$ 和 2^^{255}$<r<2^{256}$ 均为正整数且 N 的具体取值如下：

N=0x8199f8d487909988daf7d692ce8b1ffb4c37aa8010c8ca337ae4398c521383dc51007645cb6a1743c9b52ec5808e9e0e6f54d5fbb143cf81651240beab342dfb4622f073c4f8ab968dd5c8d4be3b7dd55c2cb9ef9c06294cd87e5fa29e38279c850f03687dc8c83c68104dca88e3a5c8559a01c040e7d5107e4a9f2385429f90