Исходный код:

from Cryptodome.Util.number import inverse  
  
def CheckSignature(p, g, m, y, a, b):  
 if (pow(y, a, p) \* pow(a, b, p)) % p == pow(g, m, p):  
 print("Valid Signature")  
 else:  
 print("Invalid Signature")  
  
  
def GenerateSignature(p, q, g, m, x, k):  
 a = pow(g, k, p)  
 b = (m - x \* a) \* inverse(k, q) % q  
 print("Digital View:")  
 print("a/r: ", hex(a))  
 print("b/s: ", hex(b))  
  
  
print("Choose Task (Check signature or generate signature):\n1) Check Signature\n2) Generate Signature")  
choice = int(input())  
if choice == 1:  
 p = int(input("Enter p: "), 16)  
 q = int(input("Enter q: "), 16)  
 g = int(input("Enter g: "), 16)  
 m = int(input("Enter message: "), 16)  
 y = int(input("Enter public key: "), 16)  
 a = int(input("Enter a/r: "), 16)  
 b = int(input("Enter b/s: "), 16)  
 CheckSignature(p, g, m, y, a, b)  
elif choice == 2:  
 p = int(input("Enter p: "), 16)  
 q = int(input("Enter q: "), 16)  
 g = int(input("Enter g: "), 16)  
 m = int(input("Enter message: "), 16)  
 x = int(input("Enter secret key: "), 16)  
 k = int(input("Enter random number: "), 16)  
 GenerateSignature(p, q, g, m, x, k)

Результат работы генерации на данных из таблички:

P = 103fb179699c855326ebe3e03d8d0e930c9d8f089a7ff785e4a6c539968fd33cf4544ee3fe282b16a667ff9d3bfeed96b

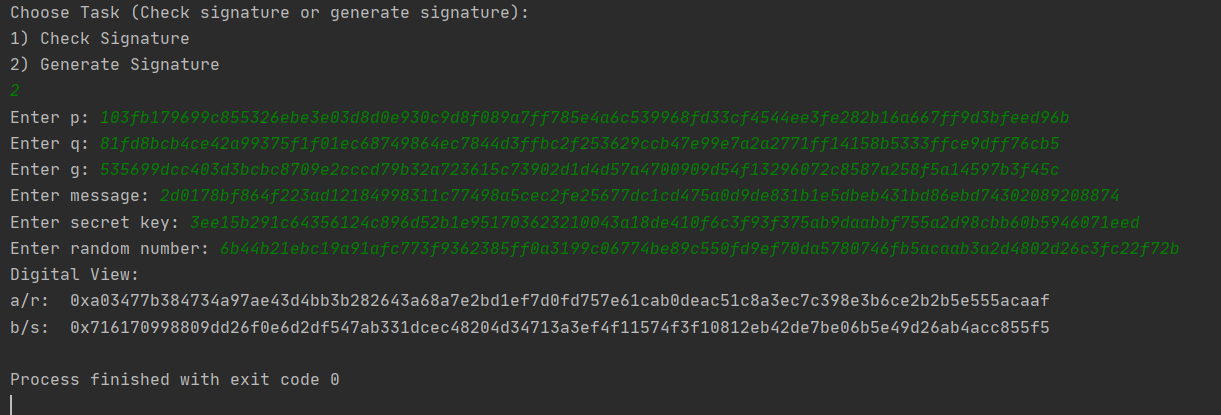
Q = 81fd8bcb4ce42a99375f1f01ec68749864ec7844d3ffbc2f253629ccb47e99e7a2a2771ff14158b5333ffce9dff76cb5

G = 535699dcc403d3bcbc8709e2cccd79b32a723615c73902d1d4d57a4700909d54f13296072c8587a258f5a14597b3f45c

M = 2d0178bf864f223ad12184998311c77498a5cec2fe25677dc1cd475a0d9de831b1e5dbeb431bd86ebd74302089208874

SecretKey = 3ee15b291c64356124c896d52b1e951703623210043a18de410f6c3f93f375ab9daabbf755a2d98cbb60b5946071eed

RandomNumber = 6b44b21ebc19a91afc773f9362385ff0a3199c06774be89c550fd9ef70da5780746fb5acaab3a2d4802d26c3fc22f72b



a/r = a03477b384734a97ae43d4bb3b282643a68a7e2bd1ef7d0fd757e61cab0deac51c8a3ec7c398e3b6ce2b2b5e555acaaf

b/s = 0x716170998809dd26f0e6d2df547ab331dcec48204d34713a3ef4f11574f3f10812eb42de7be06b5e49d26ab4acc855f5

Общие итоги из таблички:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| вариант | F\*\_p | q|p-1 | g \in F\*\_p, ordg=q | message | public key |  |  | secret key | random number | |
|  | p | q | g | m | y | r | s | x | k | correct or no |
| 2 | 3ef0a4d2070c2133466e71ff0762d9fc5ff01a105e45611aefb1cd052e2ee7a6dd7ec6f245ad9319b01960efb64d9e46321ebea3ba8e51dad9b303e03ae6eb7f341d2e494031c4246dbcb82eb97efb8f51303d154b8d1c52f4951d8b51910a2d14fc6c4055d17b531c1887c309ec3e237ec78b3f3917af73aa21232f668311b0680b7c8dee86c5c332ba44ae05771eb7dd0d308d701ab5d22ca0c3bbebe929c1f33f4ed9 | c81e8636445fe9144026266d5e3d817398a4f97afb10cb271fc6c3c5378f51e4e5c54747be85cb97860c65f40a530d6f | 336c165dd8ee434681f7588fb49279249ad2952404b29acd5099645d2062a8325a9910e5dcaec0a10912f788c7a9b191eb03bc82d593b229ff9223b681c6b9589c836fc6dc65005aa6e9ac6a016dc39f257205759b796e3cabbeab16eb1d7abab6a2397e967bc0ff399fb9e54eb3f9a6147dff0139fcedaceabc3850cfed7e4babe4c33a2d174e5c41bb1e17055f4fedd5991d0892b94902868200c1ddb62ae7b3fc30db | 1732589c35524ec90b10de684d1acca1b4ebb64225c6c4f | 31893b3747e71d26e49e5fc64dcd11eb46315496b3b2def925cec5997da75ab12f01faff7150158d60e68aebb0b6d520b84bc1c3d7855e5e12306e2a1a0c83c5ff7511f9f427184cfc1697bd4b02cbb4b799ca68b9a820955f160e731a5881016e3b2a8921fd906a5b76556feb74b271512065f8d807e8fbe5a8e90982c1f69d2a9fbf18ef74cff55a5ecd3f5b962b93971ebd7051fe3c2933898f0c29bf938eaa1da41 | 2e7f94a20e9c1c0129b3d9cda136e465954aed260e71a0fe96ac40a121cdaf741983ad44c4ceb230df8b206cf99c4393f4d17e9136496efa4deede8862d7869de476f111b3beb5d1b604467cb18ee3d3f601f3fcfe621ea5880b2b0e5b2b9af9e43885f93c7590c41f5ca0c384637e8f530b3d338de98b69a0297161b608fa1abaa7727d16ddd201f7da032f4634a4eb5c863ebb57694d7aadc8e648ef4f59647334d402 | 1334cc144f45da091a5109d7dc37c1f4d33b682c6c73fd8ab | \_ | \_ | correct |
| 2 | 22a21276441c098a029870bbc9fbe465902ceee35d57bfc1fc6305cc4b924607eeb6003f840c28e0ef657a1327066a7a4817df5042f240d800298ad7ddadad758ef8cc27542649c222dc01c9f6dab07fa41ea840289866481c4683f7bda14065493aac1f1c0ff08f213f15df0171d86b40031caba2bf36c649bb5c4d8f868d502420acc909ec65ef5213918ad2f24e9902ff5810ad75fae5c761b77086fad983a683d5cf | 43c4362fa0fca765e0f6fc7f7a8e86cb1bddf908c67850501 | 502a1b73ad853be0ac4c3f10e35884596bc79f337f336f0672b3bdc82674bbe452ccbb7b0241dc742f9eb5c95b6c20aa347e0bbdec1b2888231fd34be8b3a2cb8d3523f758f86515f117501bc0e758e0e32f9c1d3722dbe3f3bbc3c8eca2cc28f1fd74770ebdfd74824ff9b1c209b0f7eaf44df1e98700575d3e1e1115edf3e880494177d4125fb4516ca4310cac5b3d83cc8ed712b5931cf0755e36b96965ed9c75285 | 2d4d6d83353acd9bab237837c970e98360638163bb59421b | 9003f05abe63abbbdb7cc93859eb97f6e6ad2333a77bb6796e1505531e54a361b10db7bd1577bd16498a57febc80d17239402b8a9f970fc54fd490e45cb11c5b5350fae53f8e4a856f1f3ca70a5519c8e427320277c9e1687bd35e0a5434850eb9aa514c17044cece61158b63c61219e0e7fd42b2a9f9cc78e73f5ab06b47345adff6092552f94ea66df82dbd79898395cb48267e0a596203eb4113188deefd2bfb72e0 | 1a1e9d8b805d3047c55d31f613a43f0a7eff875ea89469651cb39deebde3342a646892a4be47b5547a52ea1c291a83892d4df8cdef0321755807223eefaf468f51acb2b221c7a43f94f2eaac2daceab2c356cecc0400ab4fc437ecef0787a71191ac0b62c431e13ffda23ecd02313ffe0cb2c4317bd666327dd9baea67502cd9626555702f59c64139dc3386635bf8e8b52a23641b6072e8a51f87f3678b46f368dbce3a | 20fa182eb1b183c298e7893bf8e3228eb8f48e3675f2bb862 | \_ | \_ | incorrect |
| 2 | 1f45d0d8819e722b3bd16f1dc28c64c1c49712f91b9d4b0beb874c136038a7c8c1fa3d088baddaabf36c0ca2e9e532b9b | fa2e86c40cf39159de8b78ee1463260e24b897c8dcea585f5c3a609b01c53e460fd1e8445d6ed55f9b6065174f2995cd | 848eed6ba10d64bd7b15a0c84de514f6d48c4d305a71b16dd159898dae7419612005bf942f296c0dfa8dd1058cb928af | d254d45b0486f1b0845c66679545dde0e356096cc8e6295d214454a4dcc4b08b26e8afb57b07e64a3776d214b58e7f3 | 16ee5166a2794634726dd052a54a26a1afe78de061de854a394d845772eefd941fa68352e5e45a1faeee5c062820e96c5 | 1da6b35002be1a72d7be51df92c3605bbe757cf147497fbcc67581caaa8e31b960bf2b056fd4f0d208b771b6f25935e18 | 6c931fa82980782ba1984874ff21d37808f70a29c5ae3b4fd08cc2df5fb3c417700f650d87b60f62eae4932d63a87c07 | \_ | \_ | correct |
| 2 | 103fb179699c855326ebe3e03d8d0e930c9d8f089a7ff785e4a6c539968fd33cf4544ee3fe282b16a667ff9d3bfeed96b | 81fd8bcb4ce42a99375f1f01ec68749864ec7844d3ffbc2f253629ccb47e99e7a2a2771ff14158b5333ffce9dff76cb5 | 535699dcc403d3bcbc8709e2cccd79b32a723615c73902d1d4d57a4700909d54f13296072c8587a258f5a14597b3f45c | 2d0178bf864f223ad12184998311c77498a5cec2fe25677dc1cd475a0d9de831b1e5dbeb431bd86ebd74302089208874 | \_ | a03477b384734a97ae43d4bb3b282643a68a7e2bd1ef7d0fd757e61cab0deac51c8a3ec7c398e3b6ce2b2b5e555acaaf | 716170998809dd26f0e6d2df547ab331dcec48204d34713a3ef4f11574f3f10812eb42de7be06b5e49d26ab4acc855f5 | 3ee15b291c64356124c896d52b1e951703623210043a18de410f6c3f93f375ab9daabbf755a2d98cbb60b5946071eed | 6b44b21ebc19a91afc773f9362385ff0a3199c06774be89c550fd9ef70da5780746fb5acaab3a2d4802d26c3fc22f72b | \_ |