Get server key

Clear

Key size 512

Get key

Modulus 976CE483778B2195B81D4B16372ED02592B5508F98C8B6D6C230A82FFB24E01C09BD40D9EC77A104884C4

Public exponent 10001

```
server = User("Server")
server.n = 0x976CE483778B2195B81D4B16372ED02592B5508F98C8B6D6C230A82FFB24E01C09BD40D9EC77A104884C4C9D2732402C537DEF3D25DF5B5CB
server.e = 0x10001
server.print_vars_hex()
```

```
user Server:
  p = -0x1
  q = -0x1
  n = 0x976ce483778b2195b81d4b16372ed02592b5508f98c8b6d6c230a82ffb24e01c09bd40d9ec77a104884c4c9d2732402c537def3d25df5b5cbba9098d7db42b95
  φ = -0x1
  e = 0x10001
  d = -0x1
```

```
client = User("Client")
client.gen_keys(rand_prime(), rand_prime())
client.print_vars_hex()
```

```
user Client:
  p = 0xeb6c89d281e20b9334d1a574c99faed3d123fab1ac35c6e5b75e8631960a5799
  q = 0xc4645be8e618de25bcf0ffbdc27e45b7f500afcef3acd9466ef0165144939a0d
  n = 0xb49b6470c4a0ea65294c078dfec4b04f9de42d7f4bb1641afe143128244e7f00ef727a80f181e61df3df6639ac59c2856b
  φ = 0xb49b6470c4a0ea65294c078dfec4b04f9de42d7f4bb1641afe143128244e7eff3fa194c58986fc65021cc107203bcdf9a5
  e = 0x78999be0b38ad62752871c561be566ec094418b62eb39fc6fed01a029a28fc26917047a747f389160d69e7c46cf38d444c
  d = 0x36ac18b56f187b5665eb81cec187cfa9e8c39107aaeda4d78e9caaa2b5cc86cb01f2256002ca4cda5bf71de1422ab2fff6
```

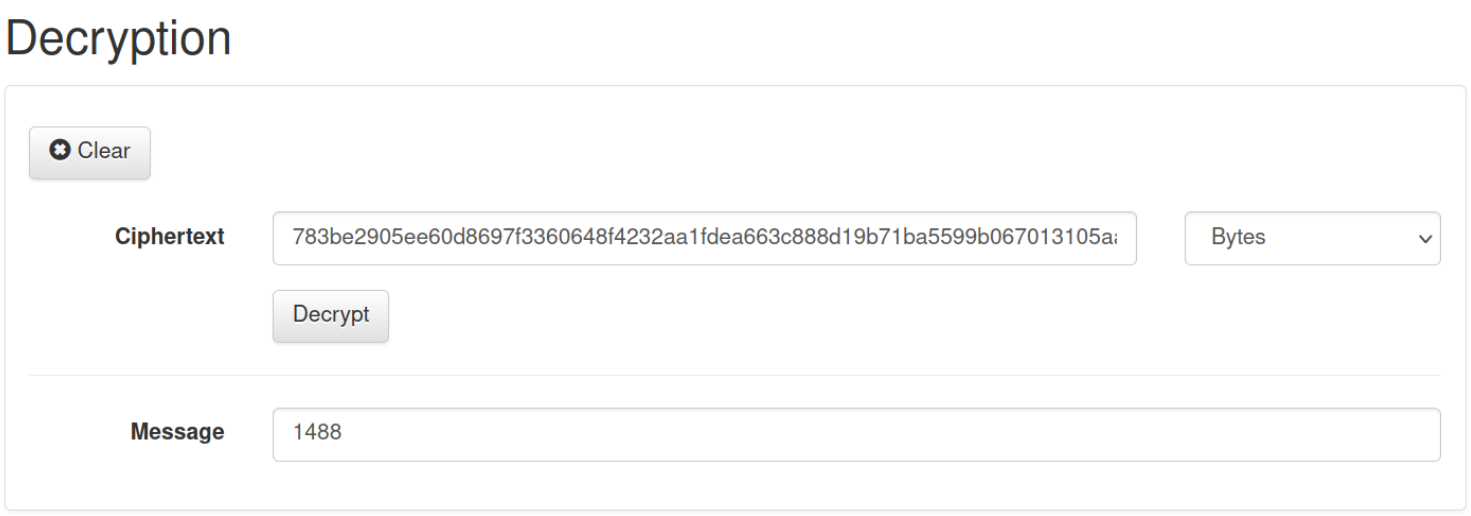
Client encrypts msg for server

```
msg = 0x1488

msg_enc_by_client = encrypt(msg, server.e, server.n)
print(f"Client encrypts msg for Server:\n    {hex(msg_enc_by_client)}")
```

```
Client encrypts msg for Server:
    0x783be2905ee60d8697f3360648f4232aa1fdea663c888d19b71ba5599b067013105aad548c9a9795a119be785de3d0148ee55f7d3fbff77c18e1906c9ee658fe
```

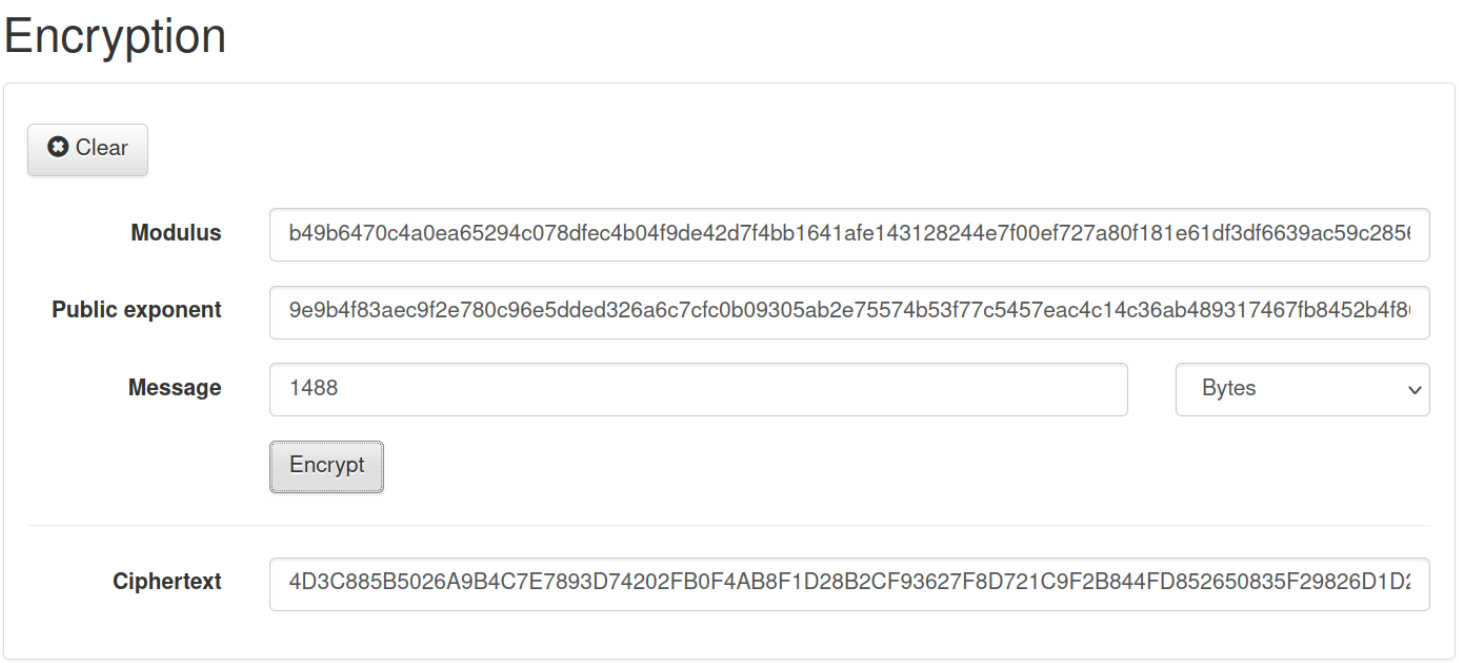
Server decrypts msg from Client



Server encrypts msg for client

```
msg_enc_by_server = encrypt(msg, client.e, client.n)
print(f"Server encrypts msg for Client:\n    {hex(msg_enc_by_server)}")
```

```
Server encrypts msg for Client:
    0x4d3c885b5026a9b4c7e7893d74202fb0f4ab8f1d28b2cf93627f8d721c9f2b844fd852650835f29826d1d2be8bb49e578ba9fc85c1b1a9d58603b6dec5001d08
```

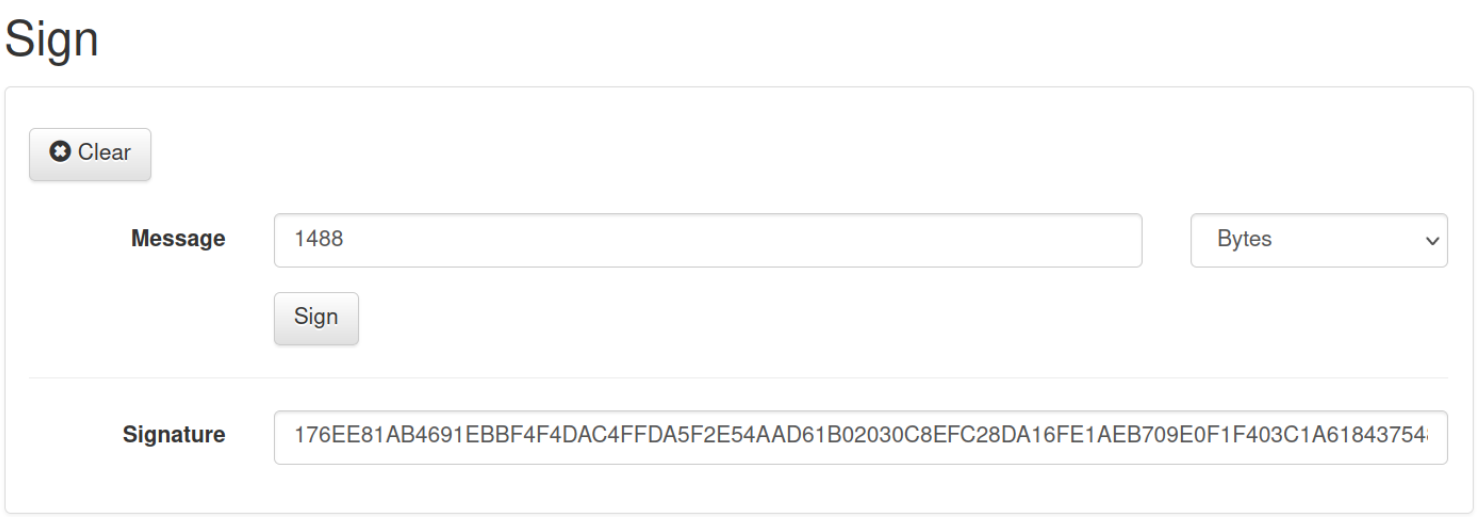


Client decrypts msg from server

```
msg_dec_by_client = decrypt(msg_enc_by_server, client.d, client.n)
print(f"Client decrypts msg from Server:\n    {hex(msg_dec_by_client)}")
```

```
Client decrypts msg from Server:
    0x1488
```

Server signs msg



Client verifies Server's msg

```
signature_by_server: int = 0x176EE81AB4691EBBF4F4DAC4FFDA5F2E54AAD61B02030C8EFC28DA16FE1AEB709E0F1F403C1A6184375484C21CA51A249
print(f"Client verivies msg from Server: {verify(msg, signature_by_server, server.e, server.n)}")
```

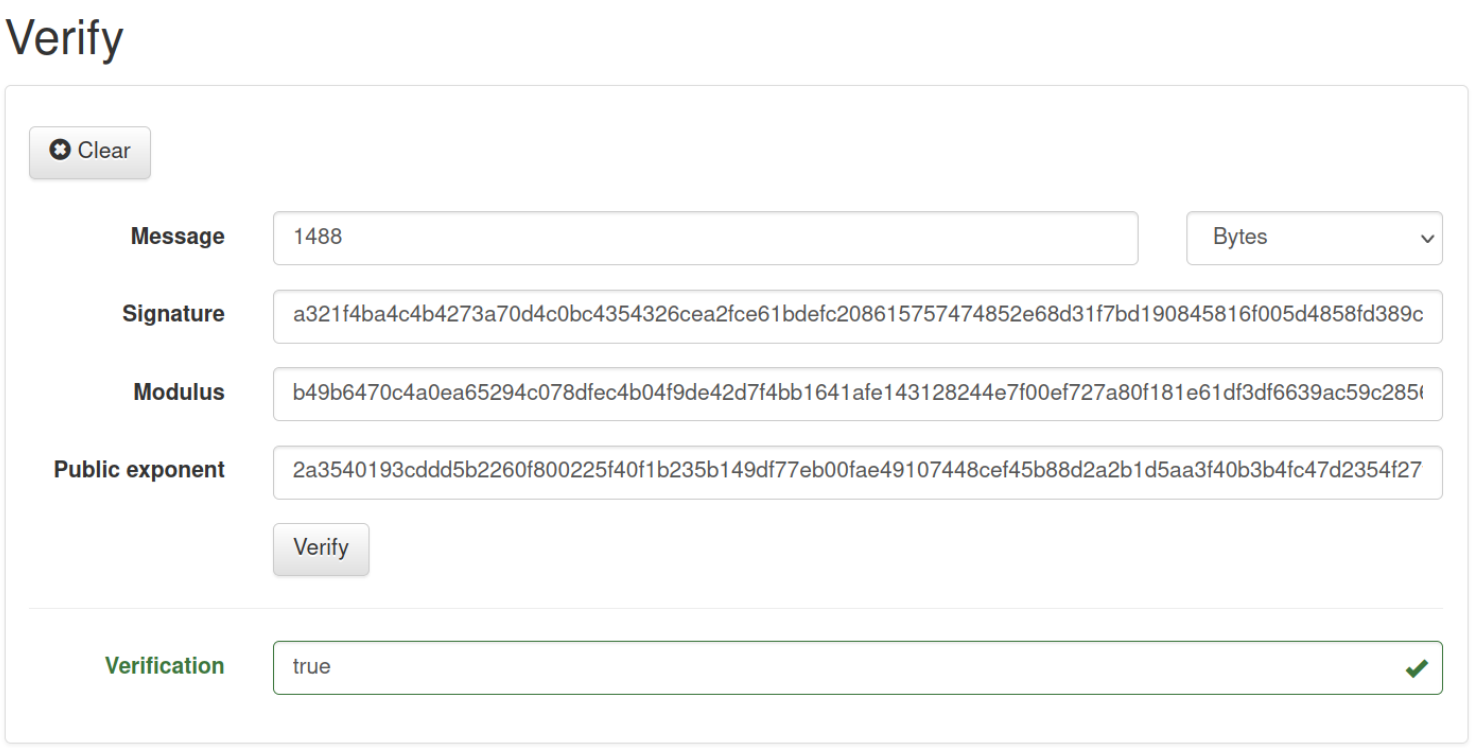
```
Client verivies msg from Server: True
```

Client signs msg

```
signature_by_client: int = sign(msg, client.d, client.n)
print(f"Client signs msg: \n    {hex(signature_by_client)}")
```

```
Client signs msg:
    0xdc22f1660276d519c25b55a033a73775a321f4ba4c4b4273a70d4c0bc4354326cea2fce61bdefc208615757474852e68d31f7bd190845816f005d4858fd389c
```

Server verifies msg



Regen Client's keys so that $n_{Client} < n_{Server}$

```
client.regen_n_less_than(server.n)
client.print_vars_hex()
```

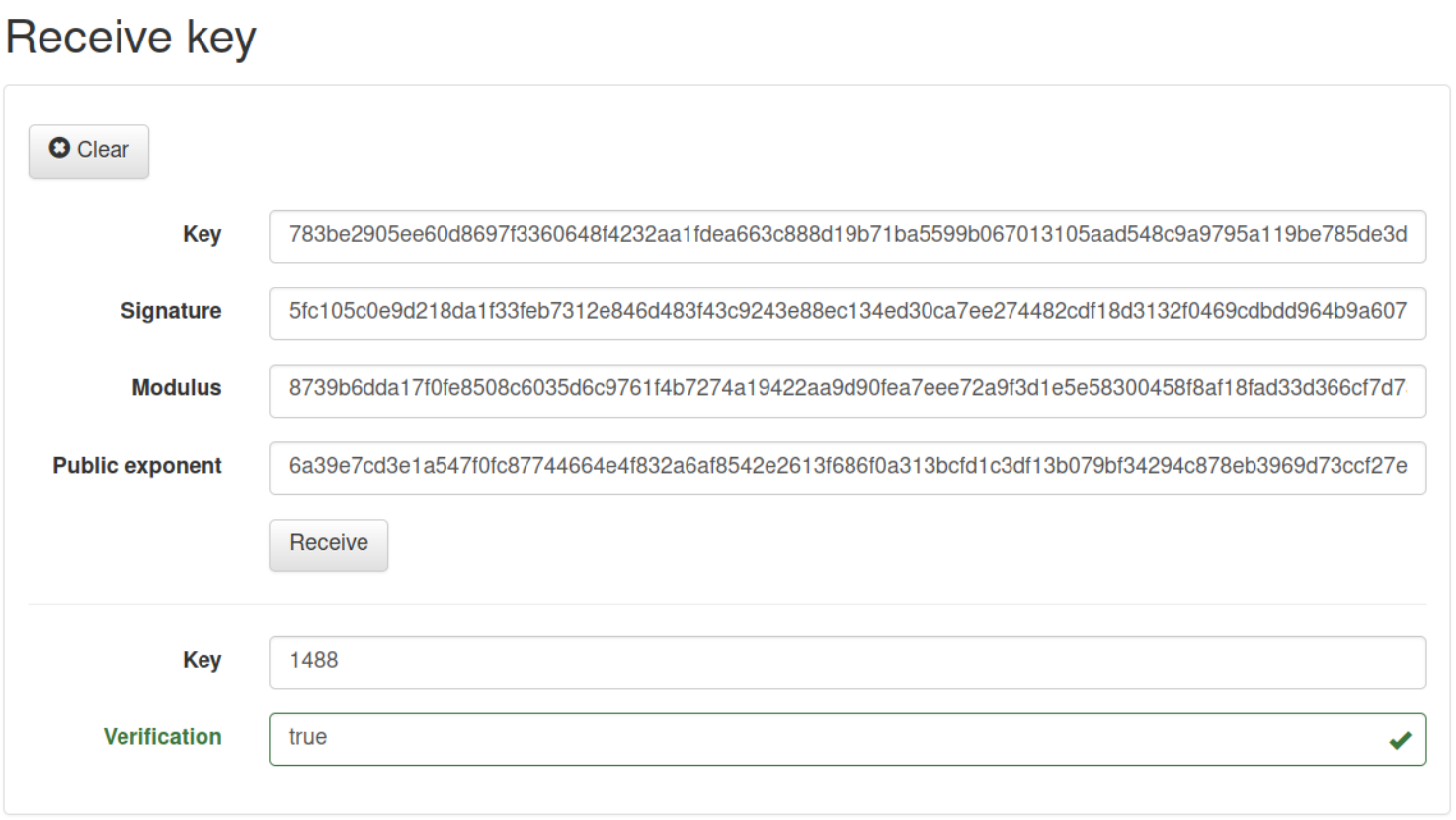
```
user Client:
  p = 0xe08223cee541e8ae7b1b305b5af3f0227339fd9dd0647b8241059de4f8fded89
  q = 0x9a3184beaaf621e308227ac8692e64def286cf97b8b606f4c3c4ecee54d67e5f
  n = 0x8739b6dda17f0fe8508c6035d6c9761f4b7274a19422aa9d90fea7eee72a9f3d1e5e58300458f8af18fad33d366cf7d7358a33675109af2eced8e218e5aa93d7
  φ = 0x8739b6dda17f0fe8508c6035d6c9761f4b7274a19422aa9d90fea7eee72a9f3ba3aaafa27420ee1d95bd2819724aa2d5cfc96631c7ef2cb7ca0e574597d627f0
  e = 0x1561ebb6428dd62f9b29a0322c34b9eb88b9cfc7734122e20ddf52b3796d40bb5e448ecaf3d9d6314c498a8cf3964ff7ee2da88721fb5e959b40a9ba69a77d53
  d = 0x40133373ded68888f6e1a64c801bf11aeb51b83c9430f0b8f5d39b8c2cf468697bffb1b43778d8b5023bcc755d1cc41b4384dd960b2c84f55e6d465925f88fb
```

Client sends secret k

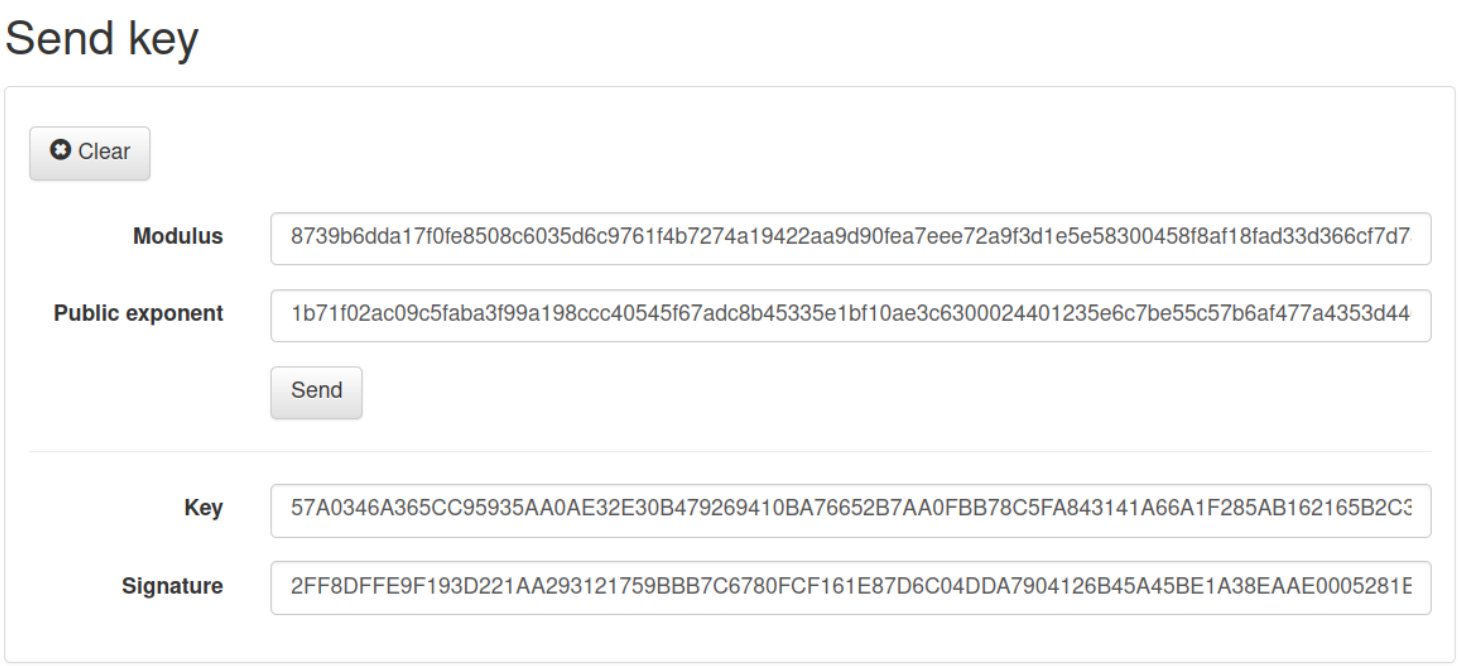
```
k_enc_by_client, S_by_client = send_secret_k(msg, client.d, client.n, server.e, server.n)
print(f"Client sends secret k")
print(f"  k_encrypted: {hex(k_enc_by_client)}")
print(f"  S_encrypted: {hex(S_by_client)}")
```

```
Client sends secret k
  k_encrypted: 0x783be2905ee60d8697f3360648f4232aa1fdea663c888d19b71ba5599b067013105aad548c9a9795a119be785de3d0148ee55f7d3fbff77c18e1906c9ee658fe
  S_encrypted: 0x5fc105c0e9d218da1f33feb7312e846d483f43c9243e88ec134ed30ca7ee274482cdf18d3132f0469cdbdd964b9a607c18289582ca28411724c3f618dc9ed1ff
```

Server receives secret k



Server sends secret k



Client receives secret k

```
print(f"Client receives secret k")
k_enc_by_server = int(input("  key: "), 16)
S_by_server = int(input("  signature: "), 16)
k_from_server = recv_secret_k(k_enc_by_server, S_by_server, server.e, server.n, client.d, client.n)
print(f"  {k_from_server}")
```

```
Client receives secret k
  key: 0x57A0346A365CC95935AA0AE32E30B479269410BA76652B7AA0FBB78C5FA843141A66A1F285AB162165B2C3C33991174CEFAD4EBB419F92E879AF01CFB
  signature: 0x2FF8DFFE9F193D221AA293121759BBB7C6780FCF161E87D6C04DDA7904126B45A45BE1A38EAAE0005281E6F118902BFF40CC549AD16750E6214
[recv_secret_k]
  decrypted k: 0x2a2f4121f06b09b0
  True
```