

Exercise 1

See Fig. 1.

Exercise 2

See Figures 2 and 3.

Exercise 3

Without the `dsaparam` option, the generation of DH parameters takes much longer because it generates a *strong prime*, i.e. a prime number p such that $(p-1)/2$ is also prime. This ensures that the multiplicative group \mathbb{Z}_p^* does not contain small subgroups. The existence of small subgroups within a larger group in a cryptographic protocol is undesirable in the sense that it confines shared secrets to a smaller set of possible values than if it were to use the whole group \mathbb{Z}_p^* .

On the other hand, using the `dsaparam` DSA rather than DH parameters are read or generate, which are then they are converted to DH format, making the key exchange process more efficient.

Note: See Figs. 4 and 5.

Exercise 4

Running the following function with the previously generated DH parameters, we can see that $X^y \pmod{p} = Y^x \pmod{p}$ holds.

```
from sage.all import *

def ex4(p, q):
    x = randrange(q)
    y = randrange(q)

    X = Mod(q ** x, p)
    Y = Mod(q ** y, p)

    return Mod(X ** y, p) == Mod(Y ** x, p)
```

Note: See Figs. 6 and 7.

Exercise 5

We know that $p = 1373, g = 2, X = 974$ and $y = 871$. We can determine Y by computing the following:

$$Y = g^y \pmod{p} = 2^{871} \pmod{1373} = 805$$

Knowing the value of X and y , we can then determine the shared secret g^{xy} by computing the following:

$$g^{xy} = (g^x)^y = X^y = 974^{871} \pmod{1373} = 397$$

Finally, we can find Alice's secret exponent by solving:

$$X = g^x \bmod p \Leftrightarrow 974 = 2^x \bmod 1373 \Leftrightarrow x = 587$$

Exercise 6

The Computational Diffie-Hellman Problem (CHD) consists in computing the shared secret g^{ab} given only the public values g^a and g^b , and not any of the secret values a or b . The motivation is to ensure that even if an eavesdropper captures g^a and g^b , they will not be able to determine the shared secret g^{ab} .

The Decisional Diffie-Hellman Problem (DDH) is stronger than the CDH. To ensure that an attacker can't learn anything about the shared secret g^{ab} , this value needs only to be indistinguishable from a random group element. This being said, given g^a, g^b and a value that is either g^{ab} or g^c for a random value c , each with probability $1/2$, the DDH problem consists of determining whether g^{ab} was chosen.

An algorithm that solves the Computational Diffie-Hellman problem can be used to solve the Decisional Diffie-Hellman problem. Given g^a, g^b and g^c , and assuming we can solve CDH, we can derive g^{ab} from g^a and g^b . Then, to solve DDH, we only have to check if the result equals g^c .

Appendices

Exercise 1

```
DH Parameters: (4096 bit)
prime:
00:fc:e2:cb:4a:5b:fa:9e:31:60:51:d4:d1:47:2e:
8e:cd:b3:2b:12:f0:7c:90:c2:0a:fa:77:1d:98:86:
bc:20:c5:0e:15:ee:54:b9:39:74:ff:76:3d:c0:b7:
b5:02:8f:3b:0f:55:b9:72:64:79:e4:ff:22:3d:02:
c2:c1:2e:45:0f:82:05:7d:a2:4a:13:7c:d6:4e:fd:
4d:6b:3f:ae:b5:5a:9a:a1:c4:ff:1c:30:3a:a4:56:
ad:fd:9f:b6:7a:00:19:b3:ae:7d:11:22:86:3a:24:
7b:76:91:72:c0:12:da:50:de:8f:3e:1c:90:ef:8b:
a6:09:1e:e8:41:a5:69:4f:f4:51:77:30:df:8c:ba:
cd:62:14:a8:78:00:86:c3:90:96:e4:98:71:49:62:
6d:6a:ba:0e:0b:74:8b:0e:e9:0f:3f:b2:b2:2e:0d:
55:03:ba:6c:85:5f:e1:aa:d7:a5:a9:1e:42:b8:4e:
d5:50:a8:d8:f9:8c:c2:cd:4c:a0:5d:62:27:12:69:
b8:6b:c2:45:b0:30:95:c6:6f:43:b9:70:14:0d:6e:
e5:6d:86:11:42:ff:ea:51:5f:be:75:5f:01:b3:6a:
9c:91:37:2f:f8:b5:b8:e5:0c:63:87:82:dc:e9:c8:
7b:24:bb:6b:63:69:8e:24:a6:5a:b5:fc:fe:dd:1a:
1e:03:8f:c3:f1:9b:30:7e:82:ee:0b:0d:98:ba:23:
31:0f:a7:a6:49:4c:ef:41:3f:60:58:d4:c9:da:47:
d0:43:ce:60:4a:b0:8c:19:7d:dc:24:c7:0d:44:f6:
41:c4:a4:5f:1f:79:6d:74:c6:90:fd:ef:a5:3f:ef:
dc:e4:55:c5:2b:f0:52:dd:64:06:0a:aa:8f:c8:26:
72:12:25:ae:9c:e0:a6:c4:b3:cc:20:55:a8:af:d2:
da:b5:03:2a:61:7d:a6:ac:db:bf:87:86:d6:14:a8:
9a:28:0a:98:86:81:a4:00:ac:06:a2:d5:11:37:01:
2a:0e:aa:9d:2b:ed:d8:56:82:53:59:b1:68:d0:b2:
e5:7e:d7:12:75:a8:57:1b:d8:d6:a5:cb:aa:93:95:
95:c4:2f:c8:ee:b1:d7:d1:4f:4a:a9:3e:3d:4a:19:
20:6c:58:c2:78:6f:1b:03:35:52:03:45:8e:b4:cf:
6b:e8:76:32:7a:ff:45:8b:f6:67:16:61:9a:c6:e3:
15:2b:cb:4a:da:46:4e:03:01:77:76:69:b1:7c:d8:
7c:47:8a:3f:05:c4:e8:d9:35:97:b9:39:48:9a:2d:
3f:66:83:5b:79:c6:4c:28:d5:bf:82:7f:47:b7:3c:
98:82:b7:1c:49:0e:d9:3d:d4:14:8b:ff:39:36:c9:
2f:ba:93
generator: 2 (0x2)
```

Figure 1: Generation of DH parameters without the dsaparam option

Exercise 2

```
DH Parameters: (4096 bit)
prime:
00:a1:45:4e:ac:71:31:85:e9:4a:07:9e:50:80:9a:
7b:2c:0b:ac:41:1b:f5:85:fa:19:fb:ab:00:f8:ec:
17:c3:21:0e:be:b3:14:d4:be:0f:24:42:1c:cd:26:
41:b9:09:06:19:e8:5a:0a:d9:79:d9:0f:39:57:b3:
96:7e:73:ef:20:29:94:0c:0e:00:b7:a6:6e:33:5a:
b4:2c:2c:a1:4f:ea:65:00:b8:6f:a3:d2:c1:6c:dc:
ea:97:a0:96:3f:2c:60:de:e1:7c:b2:7a:21:89:70:
f5:8f:65:6e:81:c5:a4:bd:b1:e9:9b:6a:98:89:9d:
e9:44:7f:67:01:9c:f0:03:f1:ff:04:d9:1d:c1:de:
89:90:dc:c3:eb:b9:91:59:9d:d9:c3:c3:92:f0:f5:
ac:62:79:be:b3:e5:1f:95:9c:65:89:0e:22:90:b9:
8b:9b:b5:d4:8f:93:9c:c3:93:1c:cb:3e:e4:69:fb:
57:e1:8e:1b:3f:71:09:b9:31:ec:98:e0:25:b3:33:
53:81:12:80:fc:8d:30:1c:36:10:9a:00:10:8f:93:
35:aa:d1:60:41:2d:22:a7:85:a0:54:0e:24:3b:49:
30:d4:f4:fc:c8:d7:24:90:21:fb:23:6e:43:c4:76:
20:5a:e5:b5:b7:d7:e5:dc:07:a2:cd:4e:81:93:50:
a5:78:68:73:ee:a4:76:3a:fb:af:7f:bd:cf:2f:8e:
c0:e0:0e:9f:20:f1:62:49:92:4f:c4:74:6c:ec:67:
06:8b:57:99:0f:ac:28:31:3a:ea:8a:e9:a7:21:f0:
58:64:f5:cb:0c:f4:3b:38:ca:e4:59:31:3d:ec:17:
02:80:4e:07:2c:f2:c4:78:66:d6:5a:9d:63:90:b5:
b0:65:85:2f:fc:0a:c8:1d:d3:10:d4:6f:7c:84:5d:
2a:52:18:18:ba:fd:fa:51:c9:01:82:a4:5c:44:f1:
37:52:ba:23:9b:f6:43:fa:76:53:3f:04:f4:af:d3:
ba:48:bc:c2:0e:8e:79:8f:ea:df:ab:8a:b0:8e:95:
8f:ab:ef:cc:fb:28:11:8b:28:8c:c1:63:0c:5c:70:
b1:77:10:49:80:ca:ef:0e:8f:c5:8f:c2:ed:49:61:
e0:59:0b:d3:ac:4b:79:57:44:18:fd:b1:54:7f:d7:
d8:d8:d1:ab:b3:e8:5f:13:18:d4:3c:09:f4:4e:cc:
59:a7:14:09:d0:43:1a:90:5a:72:e8:30:0f:51:f1:
33:34:e7:36:14:e3:de:d1:29:a5:fd:50:9b:3b:12:
30:c6:fd:f2:05:6a:03:60:80:f9:23:3a:33:e0:e3:
ce:23:c5:5e:b2:27:0e:96:36:f7:18:4c:81:13:15:
b0:e9:1b
```

Figure 2: Prime number generated using DH parameter generation with the `dsaparam` option

```
generator:
  7e:4f:9e:eb:dc:3d:4a:c6:1b:e8:4f:2f:30:54:d1:
  15:8f:8e:41:47:3a:52:8d:50:ec:58:81:3e:d8:05:
  6b:9c:ef:e3:67:01:5a:dd:b3:7c:15:bf:55:46:29:
  29:de:91:03:a5:ff:eb:8d:e7:47:69:75:e8:bf:fe:
  4e:4b:8b:bf:85:48:d4:7c:ea:2c:cc:c8:97:4f:a6:
  ed:46:7b:49:a9:af:90:58:12:8d:4c:55:ee:ff:ab:
  5a:c2:78:55:7f:d7:d5:bd:97:18:25:2f:0f:16:4a:
  34:23:cc:e7:a4:63:ea:83:d1:2c:8c:3b:29:8e:ac:
  52:7f:f2:9b:48:47:5b:0d:cc:a9:31:59:82:4e:2e:
  70:b3:e9:a7:9e:a8:37:fd:4c:c8:63:4e:1a:f1:c4:
  c3:f3:15:86:40:5d:37:f7:74:a3:cd:59:d9:f6:96:
  3a:c8:09:56:70:01:da:65:05:bc:f5:63:27:c7:d1:
  61:0b:c4:56:a7:0f:c9:f5:c4:9f:ff:fa:ee:da:c5:
  27:c6:d7:a6:c0:53:4d:3b:c4:67:dd:39:c0:4b:cb:
  98:2a:02:fd:79:14:b2:56:89:08:b9:6f:60:d8:f3:
  15:93:cd:a4:88:00:70:e2:16:1b:2b:6d:66:44:1f:
  a6:b0:93:95:6c:32:df:46:09:bb:b7:c1:3c:4a:61:
  1e:cb:c4:3b:37:b6:1f:95:8b:7e:0e:9e:70:ec:59:
  a4:a4:4b:bb:f4:00:b6:de:4e:4c:90:88:0c:6d:a3:
  8e:6b:63:bc:83:b0:c8:2d:08:27:18:28:98:41:74:
  67:c1:a7:a7:01:40:6c:db:0f:e9:93:c7:64:40:ad:
  3c:47:25:50:a0:c6:12:48:7f:c3:cb:42:d6:29:f9:
  d2:55:be:b7:6a:70:c3:4d:84:43:f2:2c:8a:0c:a0:
  9f:0c:92:68:d9:d3:ce:6a:1f:8f:ef:ad:42:23:d7:
  69:2d:29:5e:7c:35:21:b2:a3:a3:1b:5d:ab:8c:a7:
  15:bb:10:2e:95:e9:f4:fa:20:c6:f6:19:d2:b3:11:
  2e:dd:69:23:d1:48:f3:ae:8e:63:66:1f:68:9a:f0:
  81:75:70:a5:40:eb:0d:2c:81:b1:61:6e:57:40:b8:
  5a:fd:d2:93:8c:6c:83:26:af:b3:2e:24:2f:aa:21:
  ae:65:82:5d:2e:1b:6e:ed:08:76:bb:2a:fe:f9:62:
  32:8d:e2:96:33:8b:a4:d1:cb:cc:74:ae:b0:ef:62:
  20:b9:13:22:94:fd:40:4d:4e:6b:8e:6e:ca:42:d8:
  80:36:82:92:bb:8d:76:4b:1c:9b:34:02:52:0c:1d:
  5f:f2:e0:bb:4b:67:3f:29:0f:02:e9:d1:fd:1f:12:
  48:bf
```

Figure 3: Group generator generated using DH parameter generation with the dsaparam option

Exercise 3

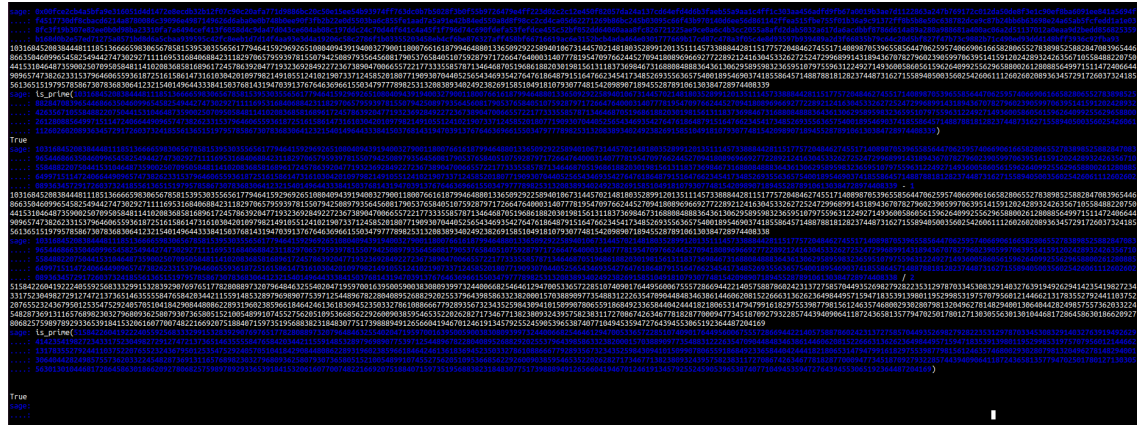


Figure 4: Prime number generated using DH parameter generation without the dsaparam option

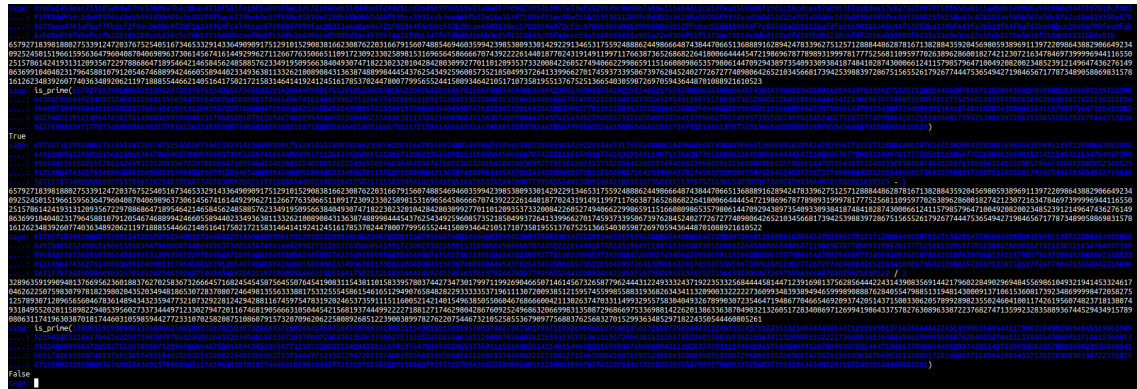


Figure 5: Prime number generated using DH parameter generation with the dsaparam option

Exercise 4

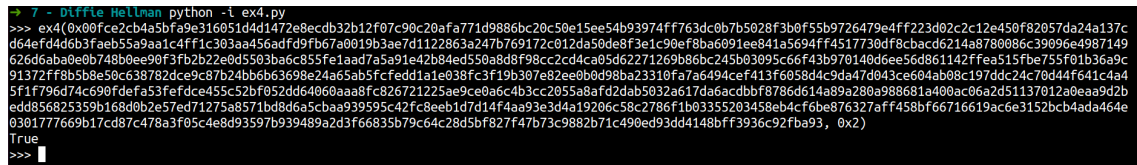


Figure 6: Checking that $X^y \pmod p = Y^x \pmod p$ holds for the DH parameters generated without the dsaparam option

```

➤ 7 - Diffie Hellman python -l ex4.py
>>> ex4(0x00a1454eac713185e94a079e50809a7b2c0bac411bf585fa19fbab00f8ec17c3210eb314d4be0f24421ccd2641b9090619e85a0ad979d90f3957b3967e73ef2029940c0e00b7a6
6e335ab42c2ca14fea6500b86fa3d2c16cdcea97a0963f2c60dee17cb27a218970f58f656e81c5a4bdb1e99b6a98899de9447f67019cf003f1ff04d91dc1de8990dcc3ebb991599dd9c3c392f0
f5ac6279beb3e51f959c65890e2290b98b9bb5d48f939cc3931ccb3ee469fb57e18e1b3f7109b931ec98e025b33353811280fc8d301c36109a00108f9335aad160412d22a785a0540e243b4930
d4f4fcc8d7249021fb236e43c476205ae5b5b7d7e5dc07a2cd4e819350a5786873eea4763afba7f7bdcf2f8ec0e00e9f20f16249924fc4746cec67068b57990fac28313aea8ae9a721f05864f5
cb0cf43b38cae459313dec1702804e072cf2c47866d65a9d6390b5b065852ffc0ac81dd310d46f7c845d2a521818bafdfa51c90182a45c44f13752ba239bf643fa76533f04f4afd3ba48bcc20e
8e798feadfab8ab08e958fabefccfb28118b288cc1630c5c70b177104980caef0e8fc58fc2ed4961e0590bd3ac4b79574418fdb1547fd7d8d8d1abb3e85f1318d43c09f44ecc59a71409d0431a
905a72e8308f51f13334e73614e3ded129a5fd509b3b1230c6fdf2056a036080f9233a33e0e3ce23c55eb2270e9636f7184c811315b0e91b, 0x00f8c068db078902615c411336d9b7b6425d5f
031a02480f7432c07809ae213a3b)
True
>>>

```

Figure 7: Checking that $X^y \pmod p = Y^x \pmod p$ holds for the DH parameters generated with the `dsaparam` option