Anurag Gulavane

Cryptography Assignment 3

```
import numpy as np
import time

# Baby Step-Giant Step Algorithm
def baby_step_giant_step(alpha, beta, p):
    m = int(np.ceil(np.sqrt(p - 1)))
    alpha_m = pow(alpha, m, p)

    baby_steps = {}
    for j in range(m):
        baby_steps[pow(alpha, j, p)] = j

    alpha_inv_m = pow(alpha, -m, p)
    x = beta
    for i in range(m):
        if x in baby_steps:
            return i * m + baby_steps[x]
        x = (x * alpha_inv_m) % p

# a
p_a = 2199023255867
alpha_a = 3
beta_a = 1228035139812

start_time_a = time.time()
log_a = baby_step_giant_step(alpha_a, beta_a, p_a)
end_time_a = time.time()

print(f"a: x = {log_a}")
print(f"Time taken: {end_time_a - start_time_a} seconds")

#b
```

```
p_b = 23058430092136999 19
alpha_b = 3
beta_b = 259893785866906004

start_time_b = time.time()
log_b = baby_step_giant_step(alpha_b, beta_b, p_b)
end_time_b = time.time()

print(f"b: x = {log_b}")
print(f"Time taken: {end_time_b - start_time_b} seconds")
```

For a & b the estimated time spent to complete the attack is “3.48 seconds”.