Izaan
P20-0613

A birthday attack in cryptography exploits the birthday paradox, where a collision (some hash value) becomes likely as attempts increase. To compute the probability understand the birthday paradox define hash space size and attempts, then use the formula P(collision) = 1 - (1-1 /Hashspace) ^Attempts.
Example: For a 128 bit hash space find P after 2^64 attempts. Larger hash spaces resist birthday attacks, highlighting the importance of sufficient bit length in hash function design for cryptographic security.

```
import math
def
birthday_attack_probability (hash_bits num attempts):
    hash_space = 2** hash bits
    Collision_probabitily = 1 - math.pow (1-1/hashspace, num
    return collision probability.

#Example: Calculat the probability for a 128 bit bit
          hash after 2^64 attempts

num_attempts = 2**64
probabity = ?
So,
birthday_attack_probability (hash_bits, num_attempts
print ("Probability of collision: probabily: 1 of")
```