NAME : JAWAD AHMED

ROLL NO : 20P-0165

Section : BCS-17A

Assignment # 04

INFORMATION SECURITY

Q1:- What is Birthday Paradox?

Ans:- The word "paradox" means the results surprise people.

The Birthday paradox also know as Birthday Problem, is a famous probability puzzle that may seem conterintuitive at first.

The problem can be stated as follows

"In a group of just 23 people, there is a better than even chance that at least two people share the same birthday."

Q2. What is BirthDay Attack. How It is used in cryptographic / hash to lose Data Integrity. Write Python Code Also?

Ans:- A Birthday Attack is a type of cryptographic attack that exploits the probability of two different inputs producing the same hash value.

Example:-

Suppose you have a hash of orignal window 11. You download window 11 compute it's hash and match with orignal window 11 hash you have. Both are same OK it's orignal.

Now Imagine a scenario that attacker change the window 11 ISO file to hack the user system Who install this window 11. Now be that window 11 is also producing same

hash as original window 11. Now this is attack using the Birthday and that will cause many security problems.

Python Code

```
import random

def generate_random_birthdays(n):
    birthdays = [random.randint(1, 365) for _ in range(n)]
    return birthdays

def has_collision(birthdays):
    return len(birthdays) != len(set(birthdays))

def birthday_attack_simulation(num_simulations, num_people):
    collisions = 0
    for _ in range(num_simulations):
        birthdays = generate_random_birthdays(num_people)
        if has_collision(birthdays):
            collisions += 1
```

```
    collision_probability = collisions / num_simulations
    return collision_probability

num_simulations = 10000
num_people = 23
collision_probability = birthday_attack_simulation(num_simulations,
                                                   num_people)
print("collision Probability", collision_probability).
```

Output

50.23 %