Assignment 08

cryptology – b keerthana

AMRUTHESH

241059041

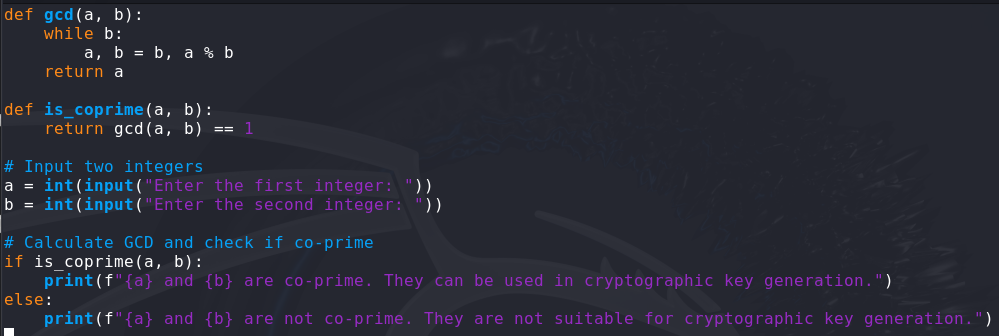
M.E – Cyber Security

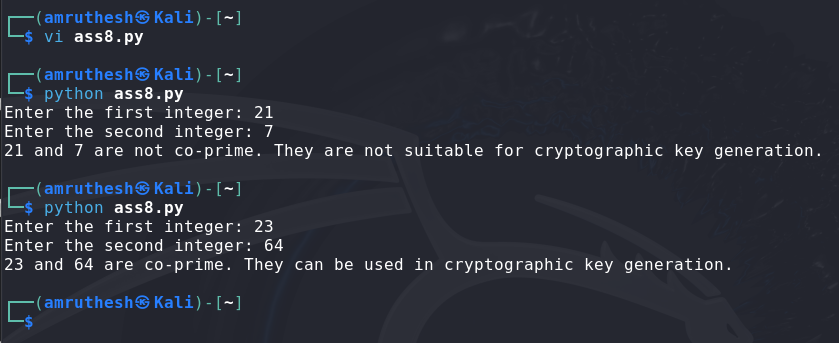
MSIS, MANIPAL

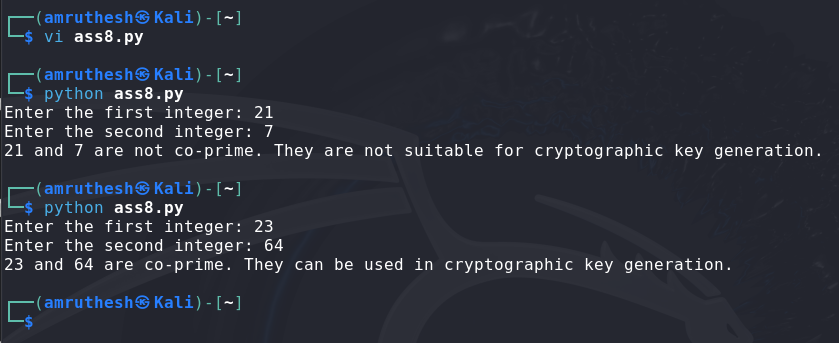
**1. GCD using Euclidean Algorithm and Co-prime Check**

The Euclidean algorithm is a method for finding the greatest common divisor (GCD) of two integers. It works by repeatedly replacing the larger number with its remainder when divided by the smaller number, until the remainder becomes zero. At this point, the smaller number will be the GCD of the two original integers. If the GCD of two numbers is 1, they are considered co-prime, meaning they share no common divisors other than 1, making them suitable for cryptographic key generation, like in RSA encryption.

**Code for GCD and Co-prime Check:**

****

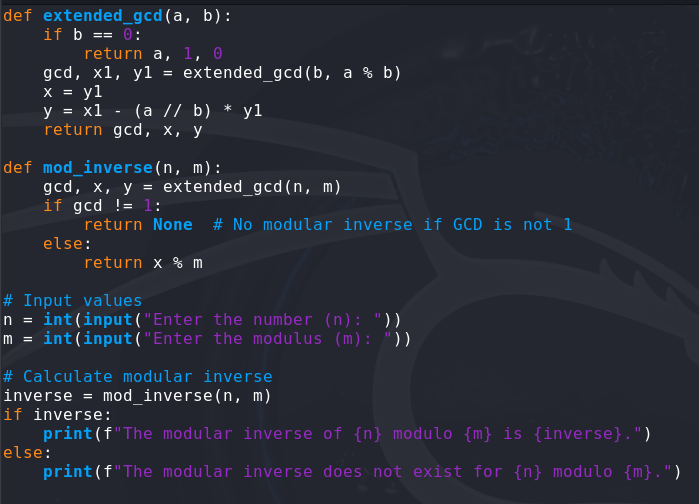
****

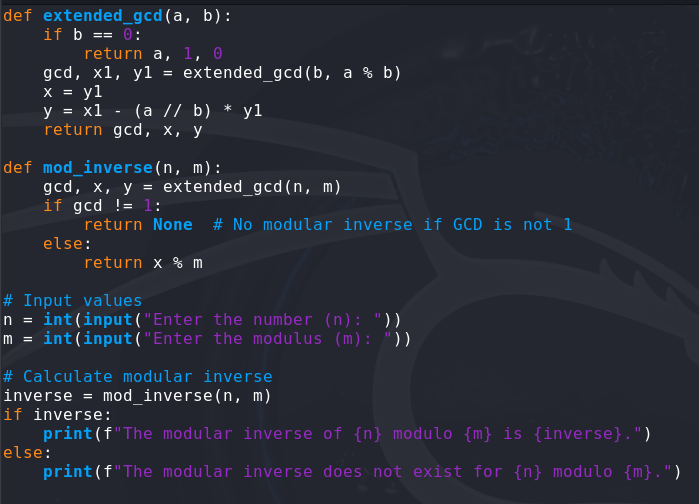
****

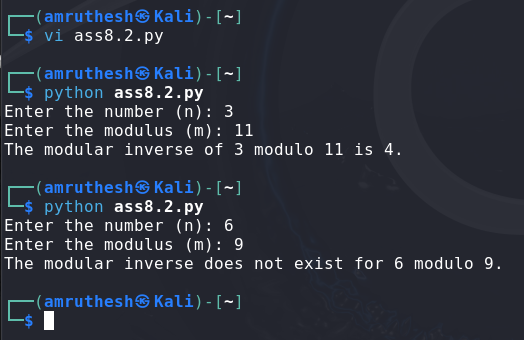
**2. Modular Inverse using Extended Euclidean Algorithm**

The extended Euclidean algorithm is an extension of the Euclidean algorithm that finds not only the GCD of two numbers but also the coefficients (usually referred to as x and y) that express this GCD as a linear combination of the two integers. For a number n and a modulus m, if their GCD is 1, the modular inverse of n modulo m is the value x such that n \* x ≡ 1 (mod m).

**Code for Modular Inverse:**

****

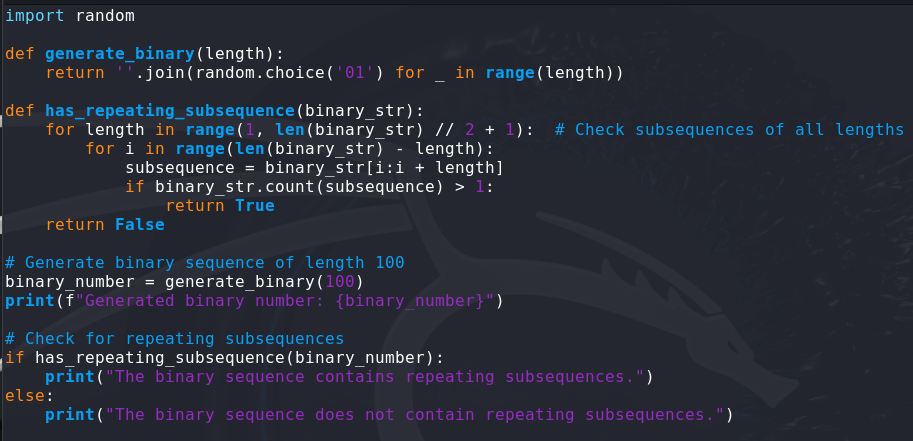
****

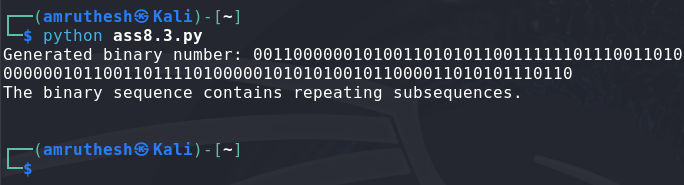
****

**3. Generate Random Binary Number and Check for Repeating Subsequence**

To generate a random binary number of a specified length, we can use Python's random module to generate a sequence of random bits. Then, we can check for repeating subsequences within the binary string. A subsequence is a contiguous block of digits, and we'll look for any such block that repeats within the sequence.

**Code for Generating Binary and Checking for Repeated Subsequence:**

****

****

**4. Golomb Test for Binary Sequences**

The Golomb test is used to check the randomness of a binary sequence. It involves checking if the number of runs (sequences of consecutive identical bits) of a certain length is consistent with a given distribution. A sequence that passes the Golomb test exhibits uniformity in the number of runs of each length.

**Code for Performing the Golomb Test:**

**Explanation of Tests in the Golomb Function:**

* The function golomb\_test() looks at consecutive runs of identical bits in the binary sequence and counts how many runs of 0s and 1s there are. The Golomb test expects a balanced number of these runs for good randomness.

