**Advanced Security Class Test 2**

****

Lecturer: Dr Aneel Rahim

Student Name: Philip Herweling

Student No.: c18470774

Student Email: [c18470774@mytudublin.ie](mailto:c18470774@mytudublin.ie)

**Question 1:**

The first thing I learned about number theory is that it’s the devoted study of the natural numbers and the integers. There are a few different algorithms and theories I have learned about, and I will talk a bit about all of them.

1. **Divisibility and the division algorithm**

Divisibility refers to a numbers quality of being evenly divided by another number without a remainder left over. There are a few basic rules that can tell you if a number is divisible by another number or not. For example if b divides a and there will be no remainder but if b doesn’t divide a then there is a remainder.

1. **The Euclidean algorithm**

This is a basic technique in number theory and is used to determine the GCD (Greatest common denominator) of two positive integers. If the GCD of two numbers is 1 then they are considered relatively prime.

1. **Modular arithmetic**

Modular arithmetic seeks to find the remainder of a number. For example if I have an integer a and a positive integer n I would define them as a mod n and the answer would be the remainder when a is divided by n. The integer remainder is known as the modulus. E.g. 5 mod 3 = 2.

1. **Prime Numbers**

A prime number is any number which only has two divisors, 1 and itself. An example of a prime number would be 7. Prime numbers are very important in security as the security of many encryption algorithms are based on the fact that its very quick to multiple two large prime numbers while the revers of this is extremely computer intensive. There are a few algorithms which test the primality of a given number, they include, Mill-Rabin, a deterministic primality algorithm and distribution of primes.

1. **Fermat’s Theorem**

Is a theorem which states that if p is a prime number, then any positive integer is not divisible by p.

1. **Eulers Theorem**

Plays an important role in public key cryptography. It states that if the gcd(a,n) = 1 then a^φ(n) ≡ 1 (mod n).

1. **Chinese remainder theorem**

Is one of the most useful results of number theory and basically says that its possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli.

**Question 2:**

The plain text m as an integer is 48

**Question 3:**

6^472 mod 3415

6^1 mod 3415 = 6

6^2 mod 3415 = (6^1 \* 6^1) mod 3415 = (6^1 mod 3415 \* 6^1 mod 3415) mod 3415

sub

6^2 mod 3415= (6 \*6) mod 3415= 36

6^2 mod 3415= 36

6^4 mod 3415= (6^2 \*6^2) mod 3415= (6^2 mod 3415\* 6^2 mod 3415) mod 3415

sub

6^4 mod 3415= (36 \* 36) mod 3415= 1296

6^4 mod 3415= 1296

6^8 mod 3415= (6^4 \* 6^4) mod 3415= (6^4 mod 3415\* 6^4 mod 3415) mod 3415

sub

6^8 mod 3415= (1296\* 1296) mod 3415 = 1679616 mod 3415 = 2851

6^8 mod 3415= 2851

When I keep subbing in I eventually get an answer of

6^472 mode 3415 = 3346.

**Question 4a:**

|  |  |  |  |
| --- | --- | --- | --- |
| 4A | 7F | 6B | BF |
| 21 | 40 | 3A | 3C |
| 8D | 18 | C7 | C9 |
| B8 | 14 | D2 | 22 |

**Question 4b:**

|  |  |  |  |
| --- | --- | --- | --- |
| 67 | A7 | 78 | 97 |
| 99 | A6 | D9 | 35 |
| 68 | 0F | 61 | 68 |
| 21 | 82 | FA | B1 |