## Lab 04- Report

**Part C**

**Question: List and give examples of attacks that can be mounted against a system with a clock**

Example 1:

Network time protocol(NTP) is used all over the world to synchronize times between systems. Attackers are able to utilise of the vulnerabilities within this protocol by altering the clocks on client systems for the potential to accept rouge Transport Layer Security Certificates that may have already been denied, thus giving an attacker a viable way to decrypt previously encrypted communications.

Example 2:

An NTP attack sending a primary server forwards in time has the potential to cause timestamps on DNSSEC cryptographic keys and signatures to expire, thus causing the server and every one of its clients to then lose connectivity to domains secured with DNSSEC (Domain name system security extensions).

Example: 3

Another attack method takes advantage of the KoD(key on Demand) mechanism. This is done by sending high volumes of queries to NTP servers that are spoofed to make it seem like they are coming from a legitimate client system. This prompts the server to issue a KoD packet and block the client from sending further queries.

**Part D**

**Code summary**

Initialise prime numbers, calculate n and phi, private key initially empty

Graphical user interface, text

Description automatically generated

Encryption and Decryption methods with their outputs

Choose a number e coprime to phi and find their GCD

Calculate private key d equal to e to the power of negative 1 mod phi

Text

Description automatically generated

GCD function

A picture containing diagram

Description automatically generated

Text

Description automatically generated**Output:**

Message is : 12

First prime is : 5

Second Prime is: 11