**Advanced Security – Lab Sheet 4**

**Part C:**

Examples of attacks that can be mounted against a system with a lock include setting the clock back, stopping the clock and setting the clock forward, with the clock referring to the Network Time Protocol (NTP) which is a networking protocol used for clock synchronization between computer systems. This is accomplished using time stamps that allow events from different logs on different machines to be correlated.

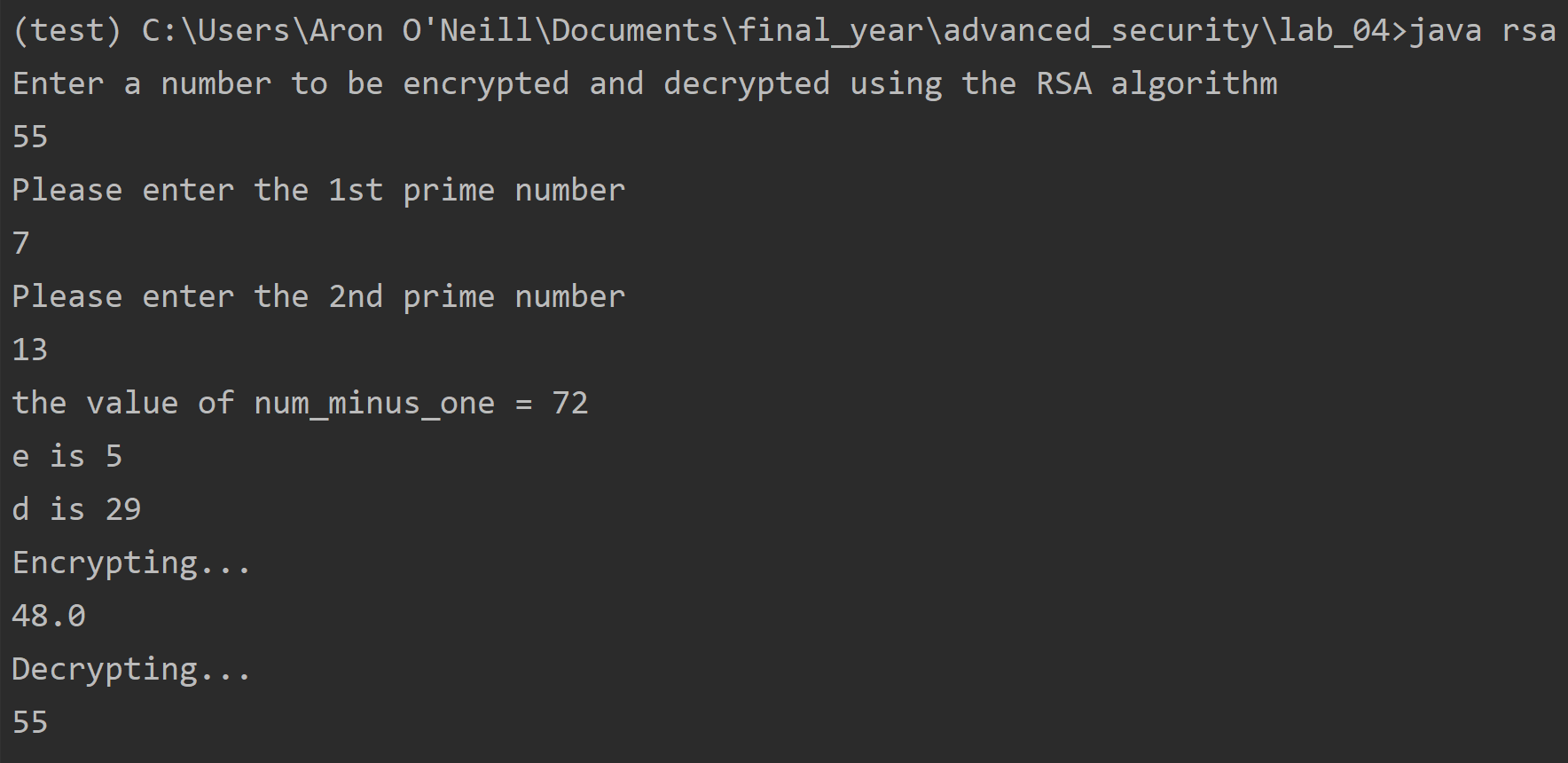
One example of an attack against a system with a lock involves setting the NTP clock back. This method of attack sees an attacker set the clock of a system to sometime in the past so that the machine mistakenly believes that it lives in the past. This can have detrimental effects on the system being used, with the severity depending on the type of system. For example, an ex-employee could potentially attack a machine he previously had access to by setting the clock of machine back to within his employment period so that it restores his access to sensitive data. An attack with more sever implications could see attack made against an automated task carried out by an HR computer. This would involve repeatedly setting the clock back so that their automated payroll is continuously sent out until the company’s bank balance has depleted. An attack which sets the clock back can be subsequently be catastrophic for a company.

Another potential attack that could be carried out against a locked system is stopping the NTP clock of a system. Systems are designed to rely on time behaving normally which results in many systems behaving in unpredictable ways. The problems associated with this type of attack can range in severity. A less severe attack could take the form of getting the wrong time on audit logs whereas a more catastrophic attack could see the financial paperwork of a transaction sent out with the wrong date and time on it which would lead to serious complications. Therefore, stopping the clock is an example of an attack which can be potentially dangerous when mounted against a system with a lock.

Similar to setting the clock back, an attack against a system could see the attacker set the NTP clock forward so that the system believes that its in the future. Setting the clock forwards to a few years in the future, would see all credit cards transactions be refused as they have now expired. This attack could be carried out so that the attacker could move eBay’s clock forward, thus eliminating many other bidders so that the attacker can obtain a cheaper price. Setting the clock forward can also have impacts on the security of a system with certain data being kept secret until the specified time has elapsed. Overall, these three examples of attacks against a system with a lock have the potential to cause detrimental effects against any system.

**Part D:**

This part involved making an rsa algorithm which can both, encrypt and decrypt. The program output is as follows:



The code which implements the above output is as follows: