Important Information

Included in this repository is an extra file named “initial output.txt.” This is the output from the first time I ran this code and therefore still has some debug statements I removed in the final product and some missing formatting information. However I still think it’s important as a way to see my process on this assignment, so I’ve left it in the repository

Missing Private Keys

The missing private keys I found were as follows:

Test #5 -	27349951181233
#6 -	2323746989340161
#7 -	9843735732800705
#8 -	76293746632708505
#9 -	118522796289119907429
#10 -	293246614767735773573
#11 -	35538931134044276033

Questions

1. The part of cracking RSA that is assumed to be computationally infeasible would be the factoring of p & q into n. As seen with my code, it took over an hour for my PC to crack a 55-bit private key, and most RSA are now 2048 bits or larger.
2. Integer factorization is a threat to RSA encryption as it is a way to see how fast one can crack the computationally infeasible part of RSA. The larger the bit size of the key that’s cracked with integer (and is known about), the more “safe” a certain bit size of an RSA key is. In terms of its impact on affected symmetrical encryption, it may not harm the symmetrical algorithms themselves, however symmetric encryption relies on asymmetric encryption to securely transmit keys. Integer factorization is a threat to RSA, and therefore a more indirect threat to symmetric encryption.
3. Quantum computing is a threat to RSA encryption as quantum computers can run all possible superpositions of a problem at the same time. This would greatly speed up the ability to crack the factoring of RSA, and thus make it wildly insecure. This is also a threat to symmetric encryption like how integer factorization is. Although it may not affect the algorithm directly, symmetric encryption relies on asymmetric in many ways, so if one is cracked, the other becomes less secure.
4. The thing that struck me the most about this article is that although I was passingly aware of how quickly escalating computing power is putting systems like cryptography at risk, I didn’t realize just how at risk these systems are. Doing a little bit of poking around I saw people on stackexchange theorizing that 1024-bit RSA could be cracked within 5 years, which is really soon all things considered.

5. My PC cracked a 77-bit RSA key in a little over 6 seconds. The community at large agrees that 1024-bit RSA keys are no long secure, and now suggests you use keys that are 2048-bits and larger.