1966: Project Proposal - Jacob Shin

RSA is a well-known asymmetric (one key to decrypt and a different key to encrypt) cryptographic algorithm that is widely used to secure data even today. However, there are certain ways to "break" RSA, or decrypt the data even without initially knowing any of the secret information. For example, Wiener's attack takes advantage of a small private key, d, to recover the d from only the provided public key. Another attack is Håstad's attack, which takes advantage of multiple messages containing the same content that all utilize the same e (public exponent). There are many other attacks on RSA that are able to take advantage of small exponents or other misconfigurations when RSA is used to decrypt data and get the private key. In my paper, I will explore some of these different attacks, provide examples and code on how to utilize these attacks, and go over some of basic theory behind some of these attacks.