U.S. DEPARTMENT OF ENERGY'S
CYBERFORCE® PROGRAM

CyberForce® 101

RSA Encryption

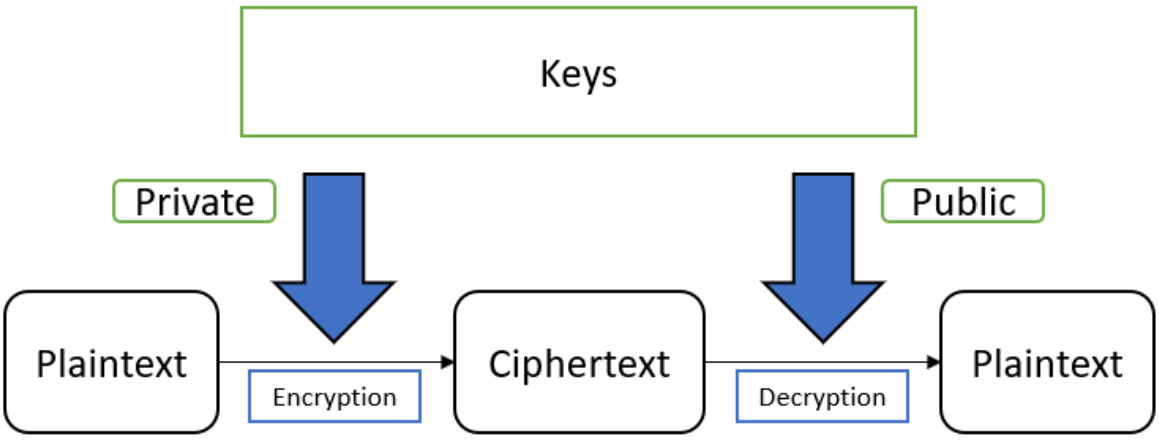
October 2023

cyberforcecompetition@anl.gov

RSA Encryption 101

RSA Function

RSA uses asymmetric encryption which requires two keys. One key is private and only the person/people who encrypted the information know it. The other key is public which means that it is open for anyone to use. Both keys can be used to encrypt and decrypt information.



RSA works because it uses algorithms in a way that it is easy to encrypt information, but extremely difficult to decrypt without the proper key. This is done by utilizing Euler's Totient which creates keys that are hundreds (if not thousands) of bits long. It is based on the fact that prime numbers are notoriously difficult to work with (especially when they are extremely large). This makes it so the two keys are incredibly difficult to guess and one key cannot be derived from the other.

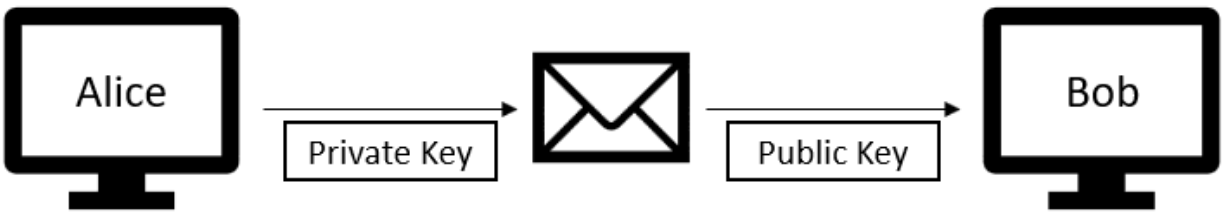
RSA's strength comes from the length of the keys it uses. The shorter the key, the easier it is to crack. This is because it is easier to factor a smaller number than a number that is over a thousand bits long.

RSA Uses

RSA encryption has many uses. This includes the exchange of sensitive information, digital signatures and information assurance.

The exchange of sensitive information through RSA encryption is very common. This is done so no one other than the people with the keys can access the information being sent. It also protects against the information being intercepted while in transit because it is sent in ciphertext.

Using RSA as a digital signature is also common. By encrypting a message with a private key (or a public key that is kept private) it assures the recipient that the person sending the information is who they say they are. If only one person/group of people have the key needed to encrypt the message, then that person/group must be the one who sent it.



Using RSA encryption to send information significantly reduces the chances of the message being tampered with. This is because it is exchanged while in ciphertext and not plaintext making said message extremely difficult to change.

Sources

- https://www.youtube.com/watch?v=Pq8gNbvfaoM
- https://www.encryptionconsulting.com/education-center/what-is-rsa