Asymmetric Encryption

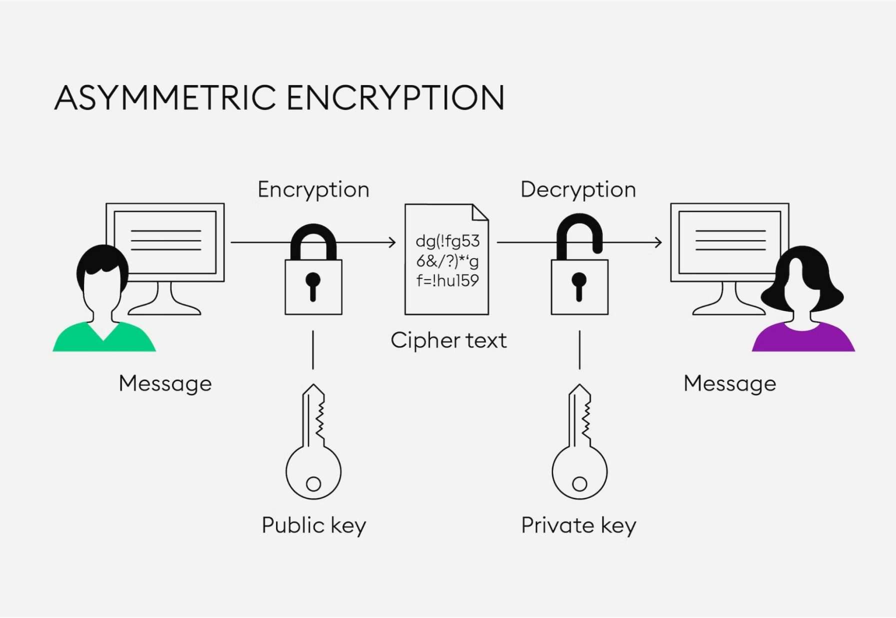
Gianna Bauzil

What is encryption and why do we need it?

- Uses mathematical algorithms to transform messages into an unreadable format (ciphertext) using keys
- Increases security of a message using keys
- Prevents attackers from understanding messages being sent between hosts
- One form of this is asymmetric encryption!

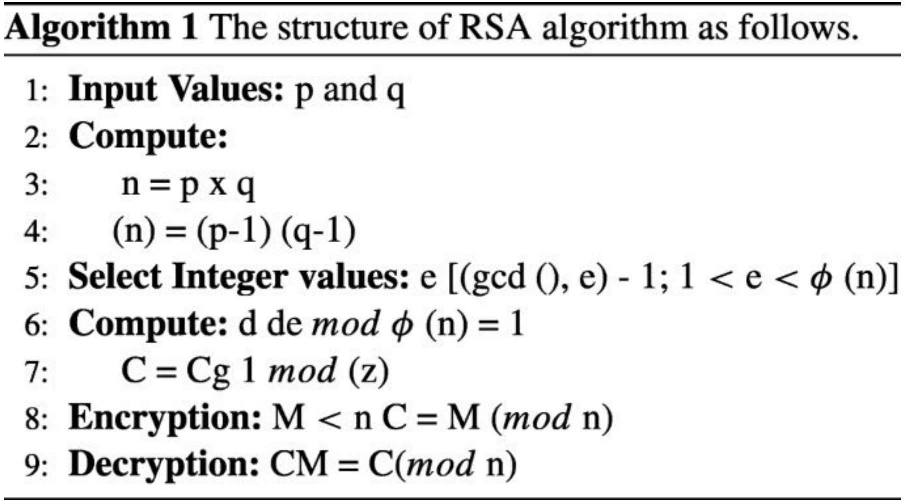
How it works

- Each user has a public and private key
- Before a message can be sent, it is encrypted using the receiver's private key
- The receiver uses their private key to decrypt the message



Rivest Shamir Adleman (RSA) Algorithm

- Invented in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman
- Algorithm ensures that the public and private keys are secure
- Keys are generated starting off with two large prime numbers and a series of mathematical equations

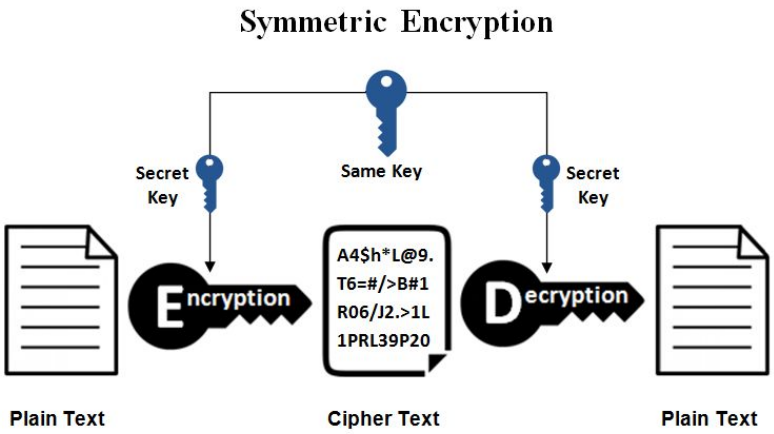


Algorithm 1 The structure of RSA algorithm as follows.

```
Input Values: p and q
Compute:
    $n = p x q$
    $(n) = (p-1) (q-1)$
Select Integer values: e $[(gcd (), e) - 1; 1 < e < \phi (n)]$
Compute: d de $mod\ \phi\ (n) = 1$
    $C = Cg\ 1\ mod\ (z)$
Encryption: $M < n\ C = M\ (mod\ n)$
Decryption: $CM = C(mod\ n)$
```

Advantages

- Most secure encryption process
- No need to exchange keys
- No need for computers to “handshake” before sending a message
- Provides message integrity
- Provides non-repudiation - decrypt digital signatures using private keys



How can one secret key be shared between 2 users safely? Asymmetric encryption provides a better solution!

Disadvantages

- Slower than symmetric encryption
- If a user loses their private key, then they cannot decrypt their messages
- Public keys are not authenticated
- If attacker discovers the private key, then a user’s messages can be read

Daily Uses

- Email security
- Web security when browsing
- Cryptocurrencies
- SSH

Sources

[1]Laboratories, Gustavus J. Simmons Sandia, et al. “Symmetric and Asymmetric Encryption.” *ACM Computing Surveys*, 1 Dec. 1979, https://dl.acm.org/doi/10.1145/356789.356793.

[2]Chen, Stephen. “What Is Data Encryption and Why Is It Important?” *TitanFile*, 22 Sept. 2022, https://www.titanfile.com/blog/what-is-data-encryption-and-why-is-it-important/.

[3]Miller, Brandon. “8 Pros and Cons of Asymmetric Encryption.” *Green Garage*, 14 Jan. 2017, https://greengarageblog.org/8-pros-and-cons-of-asymmetric-encryption.

[4]“What Is the RSA Algorithm?” *Educative*, https://www.educative.io/answers/what-is-the-rsa-algorithm.

[5]Brush, Kate, et al. “What Is Asymmetric Cryptography? Definition from Searchsecurity.” *Security*, TechTarget, 27 Sept. 2021, https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography.

[6]Daniel, Brett. “Symmetric vs. Asymmetric Encryption: What's the Difference?” *Trusted Computing Innovator*, Trenton Systems, Inc., 24 Mar. 2022, https://www.trentonsystems.com/blog/symmetric-vs-asymmetric-encryption.

[7]Abid, Rabia, et al. “An Optimised Homomorphic CRT-RSA Algorithm for Secure and Efficient Communication - Personal and Ubiquitous Computing.” *SpringerLink*, Springer London, 1 Sept. 2021, https://link.springer.com/article/10.1007/s00779-021-01607-3.

Sources cont.

[8]“Asymmetric Cryptography.” *Asymmetric Cryptography - an Overview | ScienceDirect Topics*, https://www.sciencedirect.com/topics/computer-science/asymmetric-cryptography#:~:text=Asymmetric%20encryption%20is%20used%20in,exchange%20over%20the%20public%20network.&text=Two%20keys%20(public%20and%20private,distributed%20without%20confidentially%20being%20compromised.

[9]Mutune, George. “5 Super Asymmetric Encryption Example Use Cases.” *CyberExperts.com*, 7 Dec. 2021, https://cyberexperts.com/asymmetric-encryption-example/#:~:text=Public%20key%20infrastructure%20(PKI)%3A,and%20confidentiality%20of%20encryption%20keys.