Decrypting Encryptions

Shubhro Gupta

August 30, 2024

Table of Contents

- Encryption is the process of converting information or data into a code, especially to prevent unauthorized access.
- Encryption helps protect data you send, receive, and store using any device.
- Encryption is a way to enhance the security of a message or file by scrambling the contents so that only someone with the right encryption key can unscramble it.

Modular Function

Basically the remainder of a division operation.

$a \mod b = r$, where r is the remainder when a is divided by b.

Prime Numbers. A $1 < n \in \mathbb{N}$ that is not a product of two smaller natural numbers.

Semiprime. A $n \in \mathbb{N}$ that is the product of two prime numbers.

Coprime. Two numbers are coprime if their greatest common divisor is 1.

Euler's Totient Function

The totient function $\phi(n)$ is defined as the number of positive integers less than n that are coprime to n.

$$\phi(8)$$

$$GCD(1,8) = 1$$
$$GCD(2,8) = 2$$
$$GCD(3,8) = 1$$
$$GCD(4,8) = 4$$
$$GCD(5,8) = 1$$
$$GCD(6,8) = 2$$
$$GCD(7,8) = 1$$

$\phi(8) = 4$, since there are 4 numbers that are coprime to 8.

$$GCD(1, 8) = 1$$
$$GCD(2, 8) = 2$$
$$GCD(3, 8) = 1$$
$$GCD(4, 8) = 4$$
$$GCD(5, 8) = 1$$
$$GCD(6, 8) = 2$$
$$GCD(7, 8) = 1$$

Similiarly, $\phi(9) = 6$, $\phi(10) = 4$, $\phi(11) = 10$, $\phi(12) = 4$.

History

- Developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977.
- RSA is an algorithm used by modern computers to encrypt and decrypt messages.
- It is an asymmetric cryptographic algorithm.
- It is based on the fact that finding the factors of a large composite number is difficult.

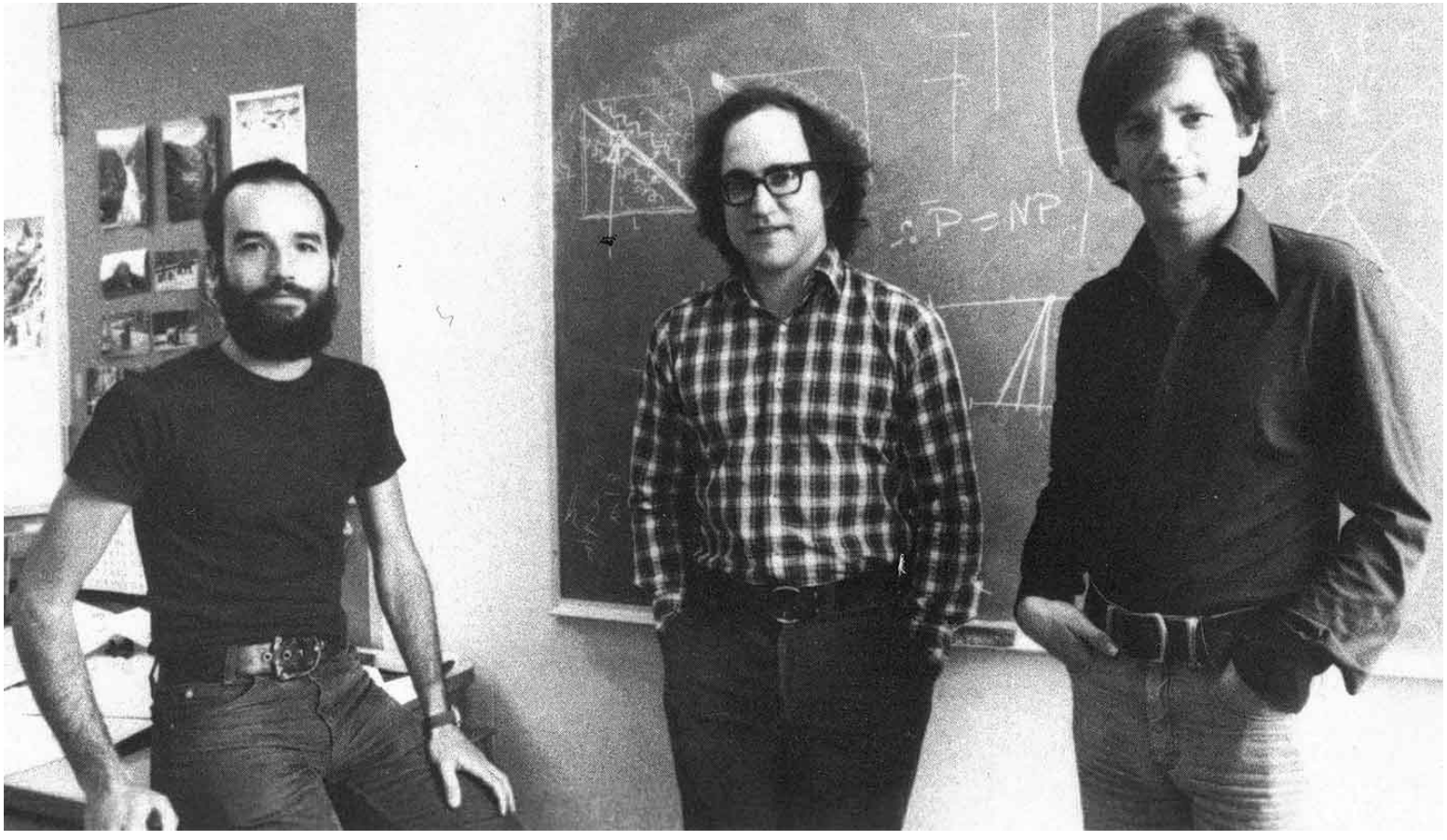

Figure: Rivest, Shamir, Adleman at MIT

hello