RSA Cryptography is a way of encrypting text securely.

RSA Cryptography is used to securely encrypt and decrypt messages. RSA stands for Ron Rivest, Adi Shamir, and Leonard Adleman. They were the first who publicly described it in 1978. It is based on the principle that it is easy to multiply large numbers, but finding the factors is very difficult. RSA has stood the test of nearly 40 years of attacks, making it the algorithm of choice for

encrypting Internet credit-card transactions, securing e-mail, and authenticating phone calls.

RSA is an asymmetric scheme. Thus, it is useful when two partied who have never met each other want to communicate securely. RSA is used regularly in web browsers, chat applications, email, VPNs, and any other kinds of communication that require sending data securely to servers or people.

RSA encryption is important for today’s security on the transfer of web.

The security of the RSA Algorithm is based on the belief that factoring large integers is and will continue to be computationally expensive. RSA has been in use for more than 30 years and to this day is still considered secure, provided keys of sufficient length are used. Keys created today are typically at least 2048 bits.

**Why is RSA so popular?**

* It's not governed by any active patents. Anyone can use it, royalty free in any private or commercial product.
* RSA can do encryption, decryption, signature and signature verification -- all with the same two functions.
* It has been around for more than 30 years and has not been compromised

RSA USES

Cyber management and security

Malware detection