**RSA REPORT**

**Group Members**

Qasim Hassan (**62357)**

Nabeel Anwar (**62553**)

Zahida Naz (**62366**)

**Introduction:**

RSA (Rivest–Shamir–Adleman) is an [algorithm](https://simple.wikipedia.org/wiki/Algorithm) used by modern computers to [encrypt](https://simple.wikipedia.org/wiki/Encryption) and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different [keys](https://simple.wikipedia.org/wiki/Key_(cryptography)). This is also called [public key cryptography](https://simple.wikipedia.org/wiki/Public-key_cryptography), because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a large [composite number](https://simple.wikipedia.org/wiki/Composite_number) is difficult. When the factors are [prime numbers](https://simple.wikipedia.org/wiki/Prime_number), the problem is called [prime factorization](https://simple.wikipedia.org/wiki/Prime_factorization). It is also a key pair (public and private key) generator.

**What is RSA Encryption?**

Let’s assume you desire to inform your mate a secret. If you’re directly near to them, you can just murmur that. If you live on opposing views of the countryside, this certainly won’t serve. You could address it down plus post it to them, or utilize the telephone, but every of those message carriers is vulnerable and anyone amidst a firm enough motive could efficiently hinder the message. If the secret meant important sufficient, you wouldn’t venture writing it down commonly–spies or a rogue carrier representative could be peering into your post. Furthermore, someone could be tapping your telephone externally without your consciousness and logging all the particular calls you make. One answer to preventing listeners from obtaining information content is to encrypt that. That primarily intends to attach a key to the information which transforms it in a jumbled mixture. If your key is adequately complicated, formerly the just people that will be capable to obtain the initial information are those who possess access to the key. The aforementioned is one of the major obstacles of cryptography, which should be directed by public-key encryption schemes (also known as asymmetric encryption) like RSA.

**Where is RSA encryption utilized?**

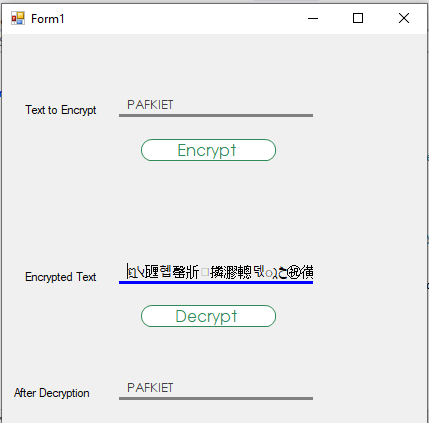
RSA encryption is usually utilized in mixture amidst other encryption plans, which can verify the authenticity and probity of information. It isn’t usually utilized to encrypt complete messages or records, because that is less effective and further source-heavy than symmetric-key encryption.

To compose something more valuable, a file will usually be encoded with algorithm, including then the symmetric key will be encrypted amidst RSA encryption. Following this method, only an entity that possesses access to the RSA private key will be capable to decrypt the symmetric key.

Without being authorized to obtain the symmetric key, the initial file can’t be decrypted. This process can be utilized to retain messages and files protected, without taking exceedingly large or wasting multiple computational sources. This encryption can be utilized in a quantity of various ways. It can be executed in plenty of different cryptographical libraries.

Being one of the primary broadly utilized public-key Encrypted plans, RSA placed the bases for many of our reliable connections. It was traditionally utilized in TLS also was more the initial algorithm utilized in PGP. RSA is yet viewed in a variety of network browsers and other news carriers.

**Screen Shots:**

****