RSA (Rivest-Shamir-Adleman) er en asymmetrisk krypteringsalgoritme, der bruger en offentlig nøgle til at kryptere data og en privat nøgle til at dekryptere data. Her er en grundlæggende forklaring på, hvordan RSA-kryptering fungerer:

1. Generering af nøgler: Først genereres et nøglepar, der består af en offentlig nøgle og en privat nøgle. Den offentlige nøgle kan deles med alle, mens den private nøgle kun kendes af ejeren.
2. Kryptering: For at kryptere data bruger afsenderen den offentlige nøgle til at kryptere beskeden. Den krypterede besked kan kun dekrypteres ved hjælp af den private nøgle.
3. Dekryptering: Når modtageren modtager den krypterede besked, bruger han eller hun sin private nøgle til at dekryptere beskeden.

RSA-kryptering er en af de mest anvendte krypteringsalgoritmer i verden og bruges i en række forskellige applikationer og protokoller, såsom SSL/TLS, SSH, PGP og andre. RSA er også kendt for at være en af de sikreste krypteringsalgoritmer, der er tilgængelige i dag.