سیستم رمزگذاری RSA عمدتا سه مرحله دارد -

اولین مورد Key Generation است - هرکسی که بخواهد پیام های مخفی دریافت کند یک کلید عمومی (که منتشر می شود) و یک کلید خصوصی (مخفی نگه داشته می شود) ایجاد می کند. کلیدها به گونه ای تولید می شوند که ساخت آنها را پنهان کرده و یافتن کلید خصوصی را فقط با دانستن کلید عمومی دشوار می کند.

پیام دوم رمزگذاری است - یک پیام مخفی برای هر شخصی می تواند توسط کلید عمومی وی رمزگذاری شود (که می تواند به طور رسمی به عنوان شماره تلفن درج شود).

مورد سوم رمزگشایی است - فقط شخصی که مخاطب قرار دارد می تواند به راحتی با استفاده از کلید خصوصی پیام مخفی را رمزگشایی کند.

لازم بود ابتدا کلید خود را به اشتراک بگذارید. از آنجا که شما دقیقاً کلید را برای برقراری ارتباط رمزگذاری شده از طریق یک کانال ناامن به اشتراک می گذارید ، باید آنها را از قبل به اشتراک بگذارید ، این امر با شنود کلیدها هنگام انتقال ، امکان شنود را باز می کند.

اکنون به دو کلید ، یک کلید عمومی (رمزگذاری) و یک کلید خصوصی (رمزگشایی) نیاز دارید. شما کلید عمومی را با دیگران به اشتراک می گذارید و کلید خصوصی را با خود نگه دارید. کلید عمومی پیام را رمزگذاری می کند و کلید خصوصی پیام را رمزگشایی می کند. رمزگذاری تقریباً یک عملکرد یک طرفه است ، مگر اینکه الگوریتم رمزگشایی را اعمال کنید یا از کلید خصوصی برای رمزگشایی آن استفاده نکنید. این مکانیسم trapdoor شناخته شده است. به عنوان مثال ، بدن شما مخلوطی از خون و پلاسما دارد. نمی توانید آن را جدا کنید مگر اینکه از سانتریفیوژ استفاده کنید. سانتریفیوژ سپس درپوش شما است. همچنین می توانید به عنوان یک قفل در نظر بگیرید که به صورت باز ارسال شده و آن را قفل شده دریافت می کنید. سپس آن را با کلید باز می کنید.

بنابراین ، شما فقط به یک کلید خصوصی نیاز دارید. و کلید عمومی خود را با دیگران به اشتراک بگذارید. RSA از نظر ریاضی قوی است. این مکانیزم درب دام است.

مثلا -

شما ابتدا دو عدد اول تصادفی مانند p و q را انتخاب می کنید.

مدول n را بدست آورید ، به طوری که n = p × q.

از اعمال تابع totient ϕ (n) = (p − 1) × (q − 1)

بعد از آن عدد اول e را انتخاب کنید ، به عنوان مثال 1

e باید coprime با r (n) باشد.

e در اصل کلید رمزگذاری شما است.

د را محاسبه کنید. d اساساً کلید رمزگشایی شماست.

به گونه ای که e × d = 1modϕ (n)

اکنون کلیدها را دارید -

کلید عمومی = (e، n)

کلید خصوصی = (d ، n)

فقط کلید عمومی (e، n) منتشر می شود. تمام شماره های دیگر درگیر (p ، q ، φ ، d) باید خصوصی نگه داشته شوند! ویژگی اصلی این ساخت و ساز این است که محاسبه d فقط از اعداد e و n دشوار است.

رمزگذاری و رمزگشایی هر دو به یک ماژول کاهش یافته از یک ماژول m نیاز دارند. اگر قبل از شروع محاسبه مدول ، کل توان محاسبه شود ، این ممکن است بسیار ناکارآمد باشد و شامل تعداد زیادی باشد. بنابراین ، از یک روش کارآمدتر برای کاهش در حال حاضر مدول توانهای میانی استفاده می شود.