الگوریتم RSA

فرض کنید فرستنده پیام جفت عدد صحیح و بزرگ (e,n) را بعنوان کلید عمومی برای رمزنگاری اطلاعات خود در اختیار دارد. در طرف مقابل ،گیرنده نیز جفت عدد (d,n) را برای رمزگشایی پیام بکار می برد.بدیهی است که دو جفت عدد (e,n) و (d,n) با یکدیگر ارتباط زیرکانه ای دارند ولی بگونه ای نیست که بتوان با در اختیار داشتن e و n براحتی d را استنتاج کرد.با فرض وجود چنین کلید هایی ،الگوریتم RSA در نهایت سادگی به صورت زیر است:

الف)پیامی که باید رمز شود به بلوکهای K کاراکتری تقسیم بندی می شود.

ب)هر بلوک طبق قاعده ای کاملا دلخواه به یک عدد صحیح به نام Pi تبدیل می گردد.

ج)با جفت عدد (e,n) به ازای یکایک بلوکهای Pi اعداد جدیدی طبق رابطه زیر بدست می آیند:

Ci = (Pi )e mod n

د) کدهای Ci بجای کدهای اصلی Pi ارسال می شوند.

روش رمزگشایی داده ها دقیقا مثل روش رمزنگاری است یعنی با داشتن جفت عدد (d,n) بلوکهای رمز شده بصورت زیر از رمز خارج می شوند:

Pi = ( Ci )d mod n