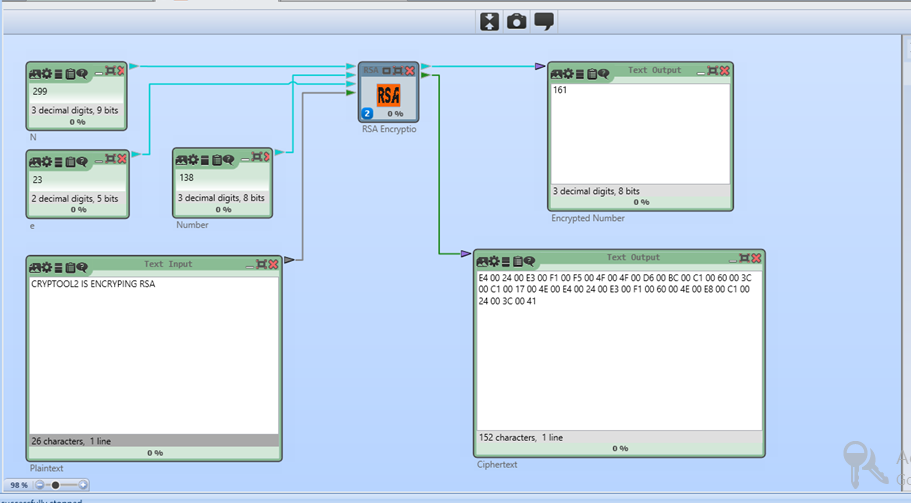
الگوریتم RSA

الگوریتم از دو کلید عمومی و اختصاصی برای فرایند رمزنگاری استفاده می کند .

از کلید عمومی برای رمزنگاری پیام و از کلید اختصاصی برای رمزگشایی پیام استفاده میشود. در این روش از سه الگوریتم به شرح زیر در فرایند رمزنگاری استفاده میشود:   
- الگوریتم تولید کلید   
- الگوریتم رمزنگاری   
- الگوریتم رمزگشائی   
برای رمز نگاری به روش RSA ابتدا به صورت زیر عمل میشود   
  
**مرحله اول تولید کلید: برای تولید کلید اقدامات زیر را انجام میدهیم**- دو عدد p و q را انتخاب میکنیم به گونه ای که نسبت به هم اول باشند   
- مقادیر n و ø را بر اساس فرمول زیر محاسبه میکنیم   
n = pq   
ø= (p − 1)(q − 1)   
- عدد تصادفی e را به گونه ای ایجاد کنید که شرایط زیر برقرار باشد.   
1 > ø < e   
gcd (e; ø) = 1   
- از الگوریتم توسعه یافته اقلیدسی برای محاسبه d استفاده کنید   
  
- در این مرحله n ,e))بعنوان کلید عمومی و d به عنوان کلید اختصاصی معرفی می شود. 

**الگوریتم رمزنگاری RSA**

: این الگوریتم پس از تولید کلید و برای رمزنگاری و رمزگشائی داده مورد استفاده قرار می گیرد جزئیات این الگوریتم به شرح زیر است.   
  
**رمزنگاری**   
- ابتدا کلید های عمومی (n ,e) طرف مقابل اخذ می شود   
- پیام مورد نظر به اعداد بین صفر تا i-1 تبدیل می شود   
- هر عدد بدست امده با فرمول c=(i^e) mod n رمزنگاری می شود   
- مقدار c به عنوان پیام برای طرف مقابل ارسال می شود   
   
**رمزگشائی**   
پیام به کمک کلید اختصاصی m=(c^d) mod n رمزگشائی می شود

