بسم الله الرحمن الرحیم

\*نام و نام خانوادگی:

محدثه عظیمی

\*شماره دانشجویی:

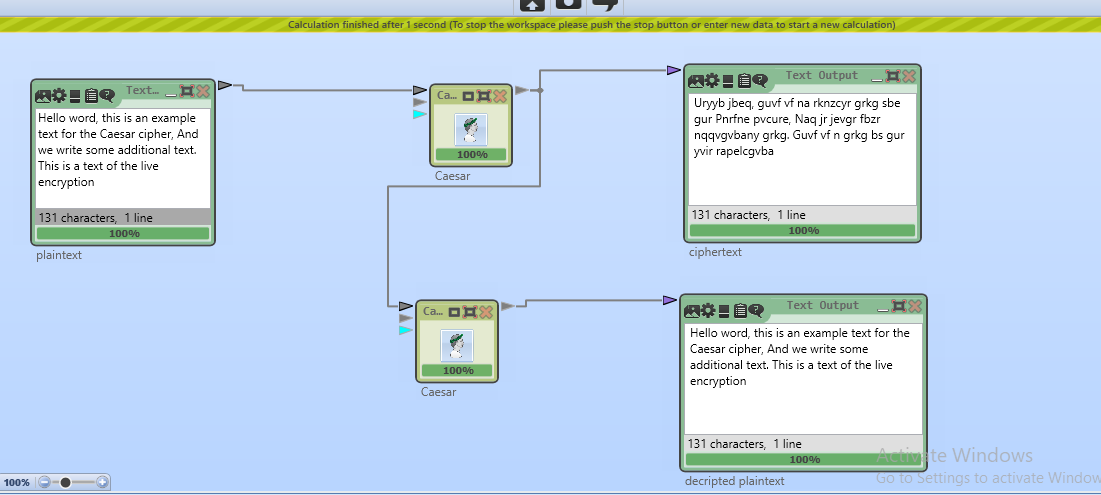
94471010

\*پروژه رایانش امن

\* دی ماه ۱۳۹۸

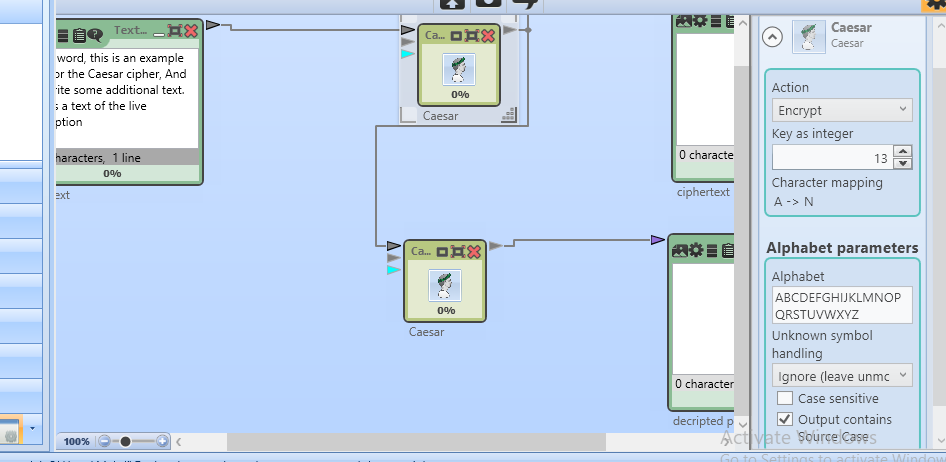
1-caesar encrypt and decrypt cipher :

بطور کلی پروژه بصورت زیرهست :

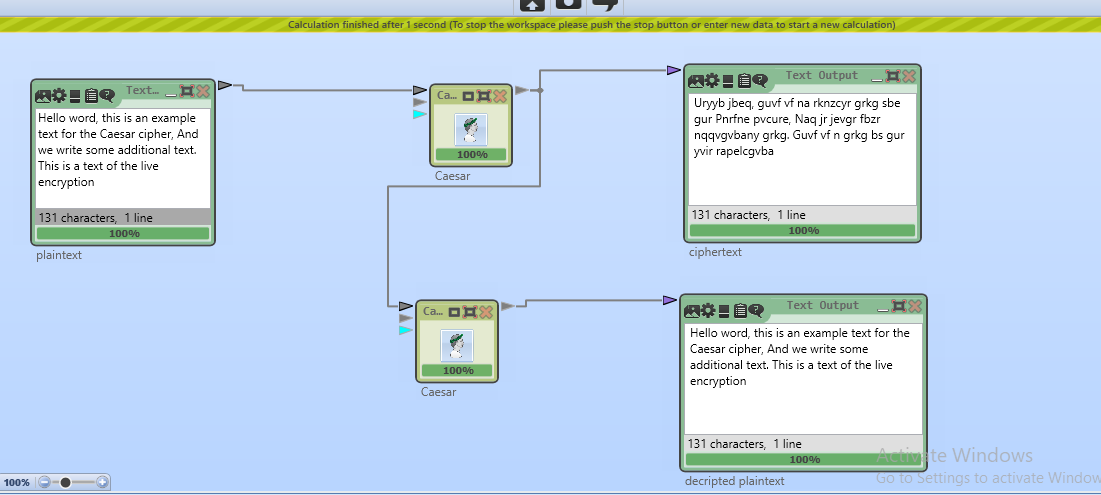


ما می خواهیم رمزگذاری و رمزگشایی رمز سزار را انجام بدیم ‍‍‍‍،میریم تو قسمت components و Caesar را سرچ می کنیم و میاریمش تو صفحه و می دونیم که دارای یک input و output و key هست ، حالا text input و text output را سرچ می کنیم و میزاریم داخل صفحه که داخل text input می تونیم plaintext را قرار بدیم و text output برای نمایش خروجی هست.

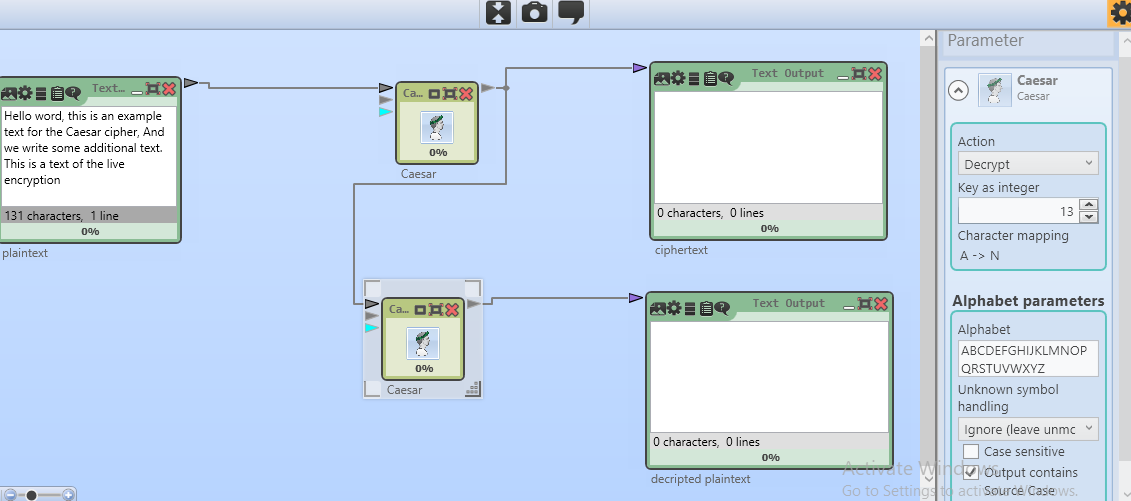
حال برای Caesar cipher میریم داخل تنظیماتش و واسش کلید را انتخاب می کنیم که ما اینجا 13 رو انتخاب می کنیم برای کلید و همینطور گزینه output contains source case را تیک میزنیم برای اینکه خروجی ها شامل source case باشد مانند شکل زیر:



این برای قسمت encrypt بود و حال برای قسمت decrypt :

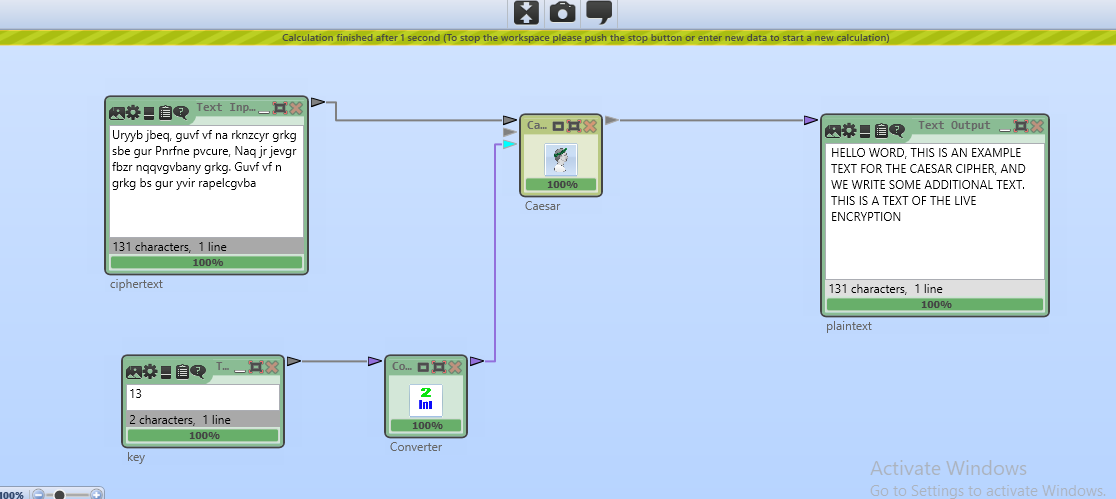


داخل همان صفحه که encrypt را انجام دادیم میایم یک Caesar دیگه اضافه می کنیم داخل صفحه و داخل تنظیمات Caesar برای قسمت action گزینه decrypt را انتخاب می کنیم که برای ما عملیات رمزگشایی را انجام بدهد و همینطور گزینه output contains source case را تیک میزنیم و خروجی Caesar قسمت رمزگذاری را به عنوان ورودی به Caesar رمزگشایی می دهیم همانند شکل زیر:



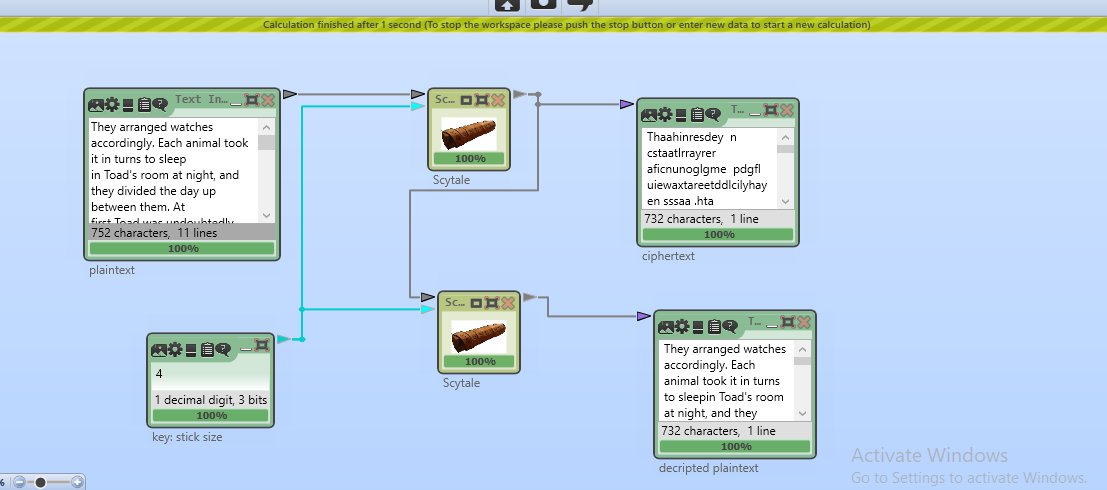
حال متن ورودی plaintext را وارد میکنیم و پروژه را play می کنیم مشاهده می کنیم که هم زمان برای ما عملیات رمزگذاری و رمزگشایی را انجام می دهد.

حال اگر خروجی متن رمز شده را برداریم و به قسمت input ، brute force angriff auf caesar بریم و به عنوان متن ورودی واردش کنیم ، عملیات رمزگشایی یا شکستن رمز را برای ما انجام می دهد که در اینجا لازم به ذکر هست که کلید اینجا باید 13 انتخاب شود تا این عملیات به درستی صورت بگیرد چون متن را در قسمت قبل با کلید۱۳ در نظر گرفتیم و برای اتصال قسمت key به قسمت ورودی کلید caesar ، باید خروجی key را به یک converter بدیم و نوع int را از تنظیمات برای ایجاد داده عددی انتخاب کنیم و خروجی این converterرا به قسمت کلید رمز caesar متصل می کنیم و حال پروژه را play می کنیم و می بینیم که رمز سزار به درستی شکسته شد و ما به متن اصلی دست پیدا کردیم همانند شکل زیر :‌



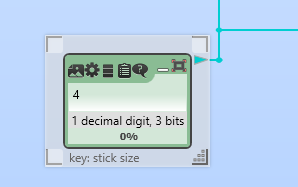
2- scytale encrypt and decrypt cipher :

به ظور کلی پروژه بصورت زیر است:

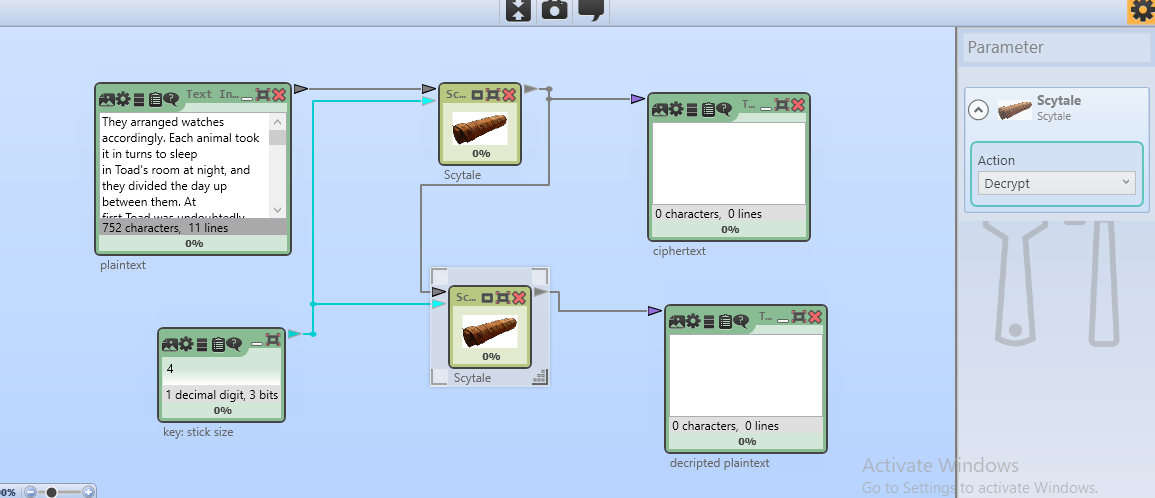


داخل components ، scytale را سرچ می کنیم و می گذاریم داخل صفحه و داخل تنظیمات scytale برای قسمت action گزینه encrypt را انتخاب می کنیم که برای ما عملیات رمزگذاری را انجام بدهد می دونیم که دارای یک input و output و key هست ، حالا text input و text output را سرچ می کنیم و میزاریم داخل صفحه که داخل text input می تونیم plaintext را قرار بدیم و text output برای نمایش خروجی هست.

Scytale نیاز به کلید دارد که فضای کلید بستگی به stick size داره و برای این که ما ورودی کلیدمون رو به رمز scytale وصل کنیم نیاز به یک number input داریم که داخل این باید stick size رو انتخاب کنیم مثلا داخل این پروژه ما سایزش رو ۴ در نظر گرفتیم مانند شکل:

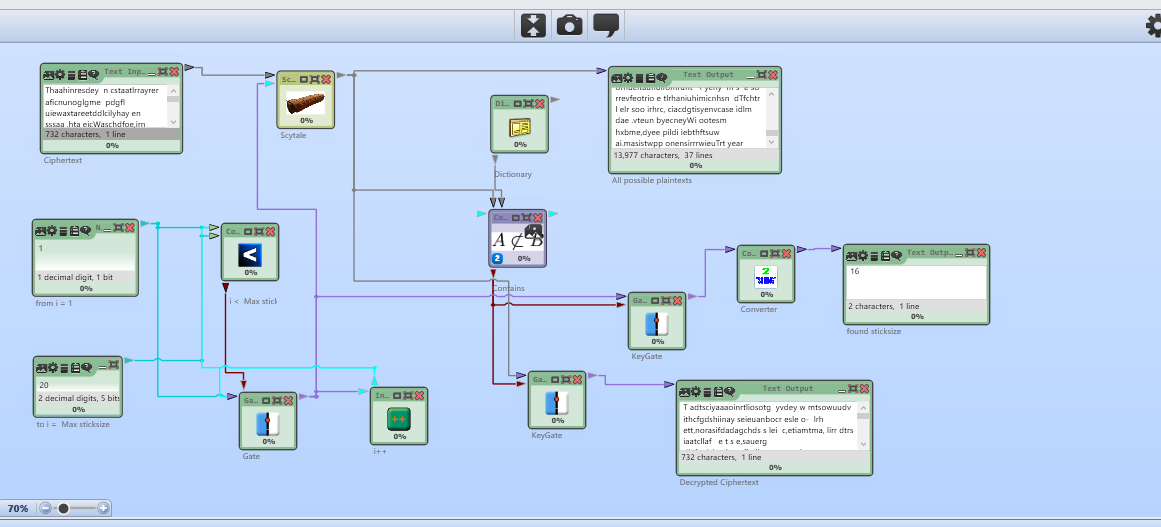


داخل همان صفحه که encrypt را انجام دادیم میایم یک scytale دیگه اضافه می کنیم داخل صفحه و داخل تنظیمات scytale برای قسمت action گزینه decrypt را انتخاب می کنیم که برای ما عملیات رمزگشایی را انجام بدهد و خروجی scytale رمزگذاری را به عنوان ورودی برای scytale رمزگشایی در نظر می گیریم، همانند شکل زیر:

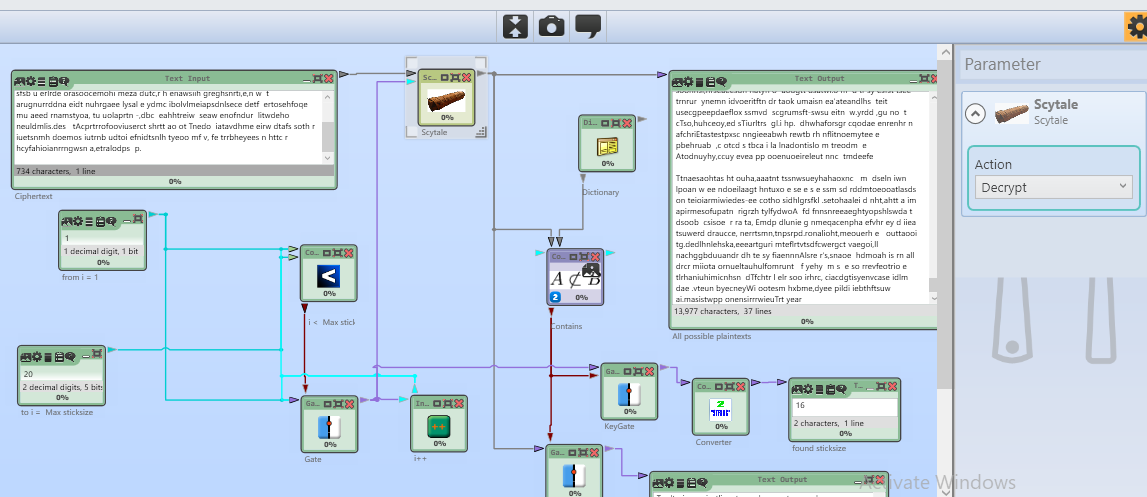


و یه خروجی هم برای قسمت رمزگشایی به نام decripted plaintext هم درنظر می گیریم ، حال خروجی stick size:key را به قسمت ورودی کلید هر دو رمز scytale متصل می کنیم، حال متن ورودی اصلی مورد نظرمون رو داخل text input وارد می کنیم به عنوان plaintext و حال پروژه را play می کنیم ، مشاهده می کنیم که برای ما هم زمان عملیات رمزگذاری و رمزگشایی را انجام می دهد.

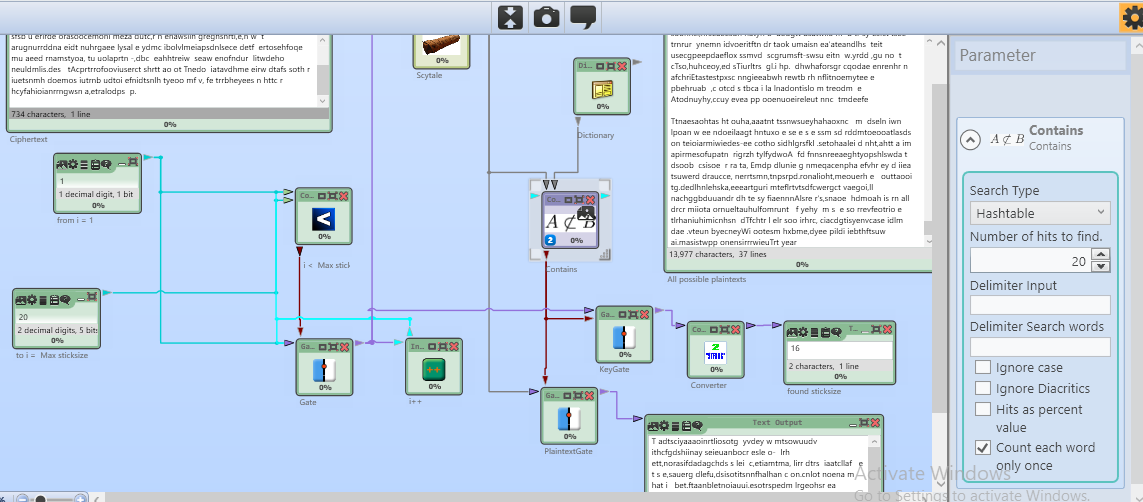
حال اگر خروجی متن رمز شده را برداریم و به قسمت input ، Scytale Brute force Analysis بریم و به عنوان متن ورودی وارد کنیم مشاهده می کنیم که متن رمز شده بصورت کامل تجزیه و تحلیل می شود و به عبارتی شکسته می شود بطور کلی پروژه بصورت زیر است:



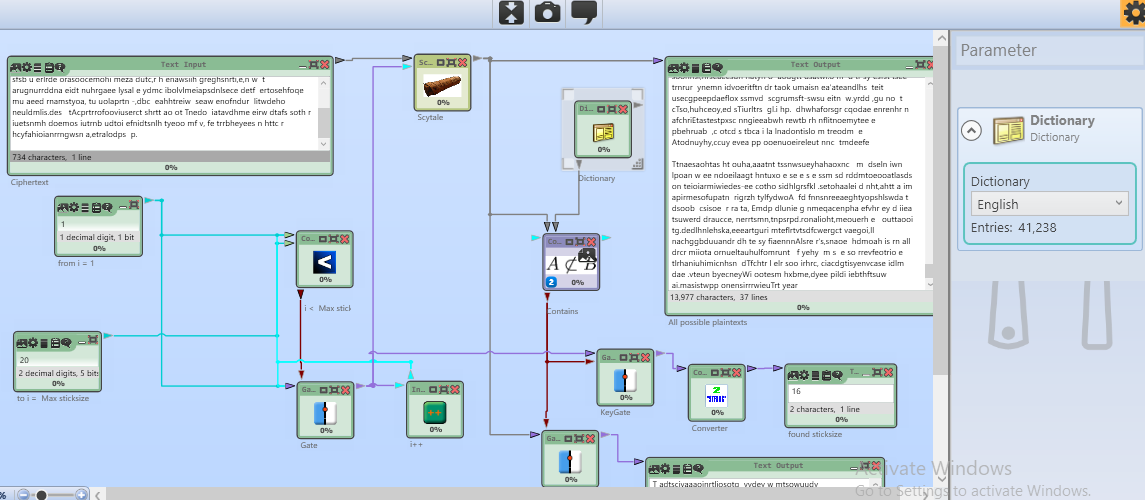
در اینجا ما یک scytale داریم مانند شکل زیر که در قسمت تنظیمات برای حالت action گزینه decrypt را انتخاب می کنیم زیرا عملیاتی که اینجا داریم مربوط به رمزگشایی رمز هست :



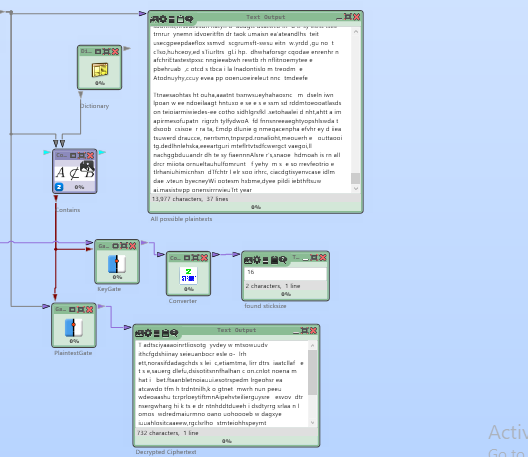
و همینطور دارای یک input و output و key هست ، مانند شکل زیر از contains استفاده کردیم که در این پروژه نوعش را hash table انتخاب می کنیم و number of hits to field را هم ۲۰ در نظر گرفتیم :



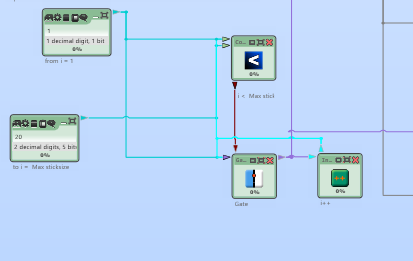
و از dictionary استفاده کردیم واسش که زبان دلخواه خودمون رو انتخاب می کنیم که اینجا زبان انگلیسی را انتخاب کردیم :



حال اگر contains بتونه 20 تا word پیدا کنه یه خروجی بولین میده به دو تا گیت که گیت اول اسمش هست KeyGate که برای مشخص کردن و پیدا کردن stick size هست که ابتدا خروجی گیت به یک converter میره تا خروجی string برای ما تولیدکند و سپس خروجی converter را به output می دهیم و گیت دوم به اسم PlaintextGate برای نشان دادن decrypt هست که مستقیم به ورودی یک output میره همانند شکل زیر:

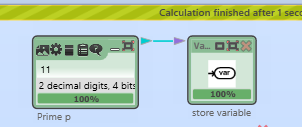


و قسمت سمت چپ پروژه که همانند یک loop به نظر می رسد یک چرخه ای هست برای محاسبه و شمارش اعدادی که مدنظرمونه مثلا در اینجا ما میخواهیم از ۱ تا ۲۰ را برای ما انجام بدهد که تعداد شمارش های این چرخه وابسته به stick size مختلف هست ، شکل زیر:

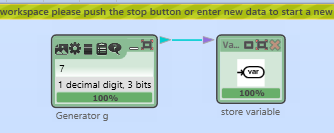


3- Diffie-Hellman Key Exchange

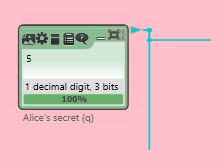
در مدل تبادل کلید دیفی ـ هلمن یک عدد اول p به تصادف انتخاب می کردیم که در این پروژه با گذاشتن یک number input در صفحه می توانیم عدد تصادفی p دلخواهمان را وارد کنیم و چون به این عدد احتیاج داریم برای اینکه این عدد تصادفی را نگه داریم از یک variable store برای ذخیره و نگه داری از آن استفاده می کنیم مانند شکل زیر :



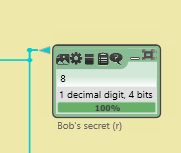
حال باید یک g را به تصادف از بازه {p-1 ،...،1، 0} انتخاب کنیم که نباید اعداد 0و1 را انتخاب کنیم و برای وارد کردن g ما نیاز به یک number input داریم که عدد g را وارد می کنیم و برای نگه داری عدد g ما به یک variable store نیاز داریم زیرا این عدد نیز برای ادامه کار مورد نیاز است ، مانند شکل زیر:



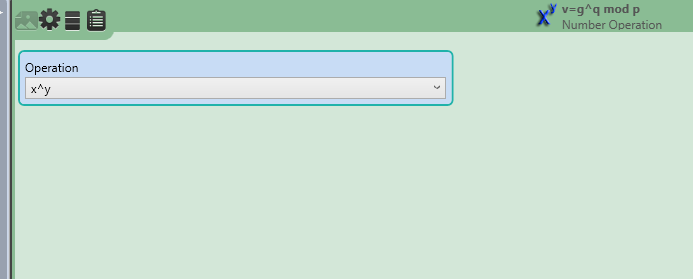
در ادامه مثلا دو فرد به نام های Alice و Bobداریم که می خواهند از طریق طرح برقراری کلید دیفی-هلمن تبادل کلید کنند که در آخر هم به یک مقدار مشترک می رسند ، در ابتدا هر دو فرد باید یک کلید خصوصی تصادفی را برای خود انتخاب کنند مانند شکل زیر که Alice یک کلید خصوصی به اسم q برای خودش انتخاب می کند که برای این کار نیاز داریم به یک number input که داخل این میاد عدد مورد نظرش را وارد می کند :



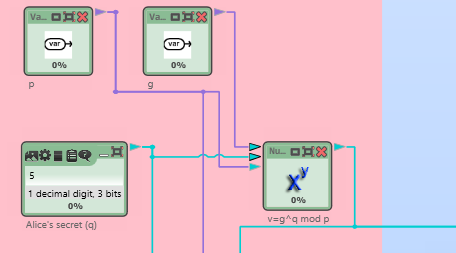
و به همین ترتیب Bob نیز یک کلید خصوصی r به صورت زیر برای خود انتخاب می کند :



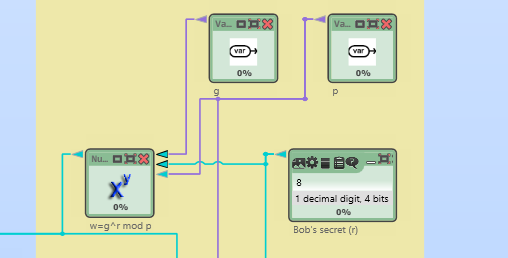
و در ادامه برای Alice یک number operation میزاریم برای انجام محاسبات ریاضی که داخل تنظیمات این قسمت باید عملیات به توان رساندن را انتخاب کنیم به این صورت :



که اینجا عملیات v= g ^ q mod p محاسبه می شود که این شامل سه ورودی و یک خروجی هست که ورودی اول را مقدار g میدیم که قبلا داخل یک variable store گذاشته بودیم و ورودی دوم را از number input می گیرد که کلید خصوصی q را دارد و به همین ترتیب برای ورودی سوم مقدار p را می دهیم و خروجی را به number operation دوم که برای محاسبه s هست برای خودش و همینطور قسمت Bob می دهیم :

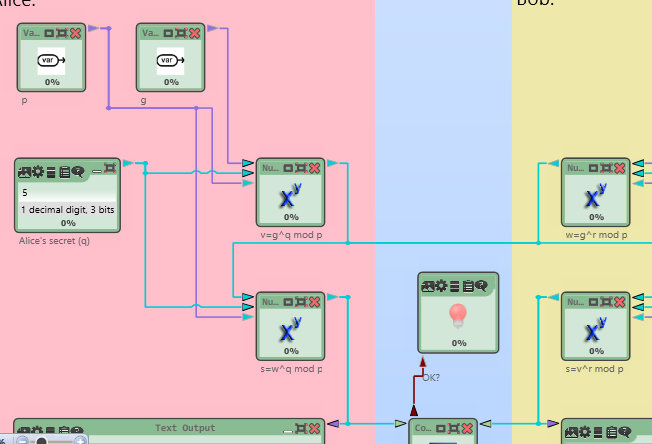


و به همین ترتیب برای ‌Bob هم همین کارها را انجام می دهیم مانند شکل زیر :



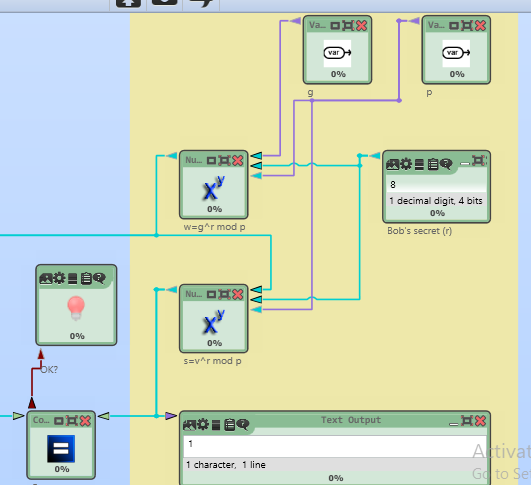
در ادامه برای قسمت Alice یک number operation دیگر اضافه می کنیم باز هم برای انجام محاسبات ریاضی که اینجا باید عملیات s = w ^ q mod p محاسبه شود تا به مقدار s برسیم برای این قسمت هم سه ورودی و یک خروجی داریم که ورودی اول را از مقدار

number operation قسمت Bob می گیرد یعنی مقدار w را می گیرد و به عنوان ورودی دوم مقدار کلید خصوصی Alice یعنی q را می گیرد و به عنوان ورودی سوم مقدار تصادفی p را می گیرد و خروجی این قسمت به عنوان ورودی به یک Comparator برای مقایسه داده می شود :

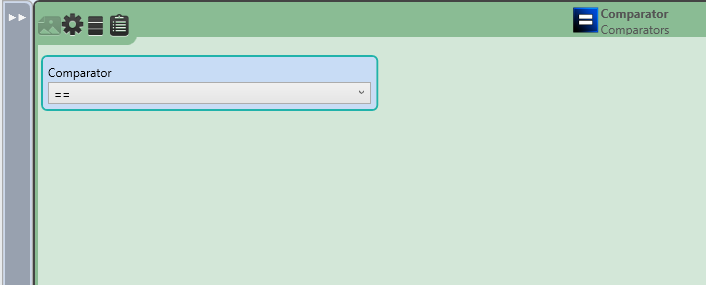


در ادامه برای قسمت Bob یک number operation دیگر اضافه می کنیم باز هم برای انجام محاسبات ریاضی که اینجا باید عملیات s = v ^ r mod p محاسبه شود تا به مقدار s برسیم برای این قسمت هم سه ورودی و یک خروجی داریم که ورودی اول را از مقدار

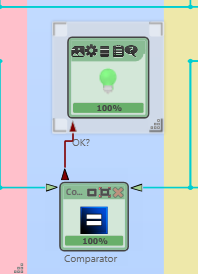
number operation قسمت Alice می گیرد یعنی مقدار v را می گیرد و به عنوان ورودی دوم مقدار کلید خصوصی Bob یعنی r را می گیرد و به عنوان ورودی سوم مقدار تصادفی p را می گیرد و خروجی این قسمت به عنوان ورودی به یک Comparator برای مقایسه داده می شود مانند شکل زیر :



حال هر دو خروجی number operation برای هر دو قسمت Alice و Bob را به عنوان ورودی به Comparator می دهیم برای مقایسه کردن دو مقدار به دست آمده در هردو قسمت که ما اینجا می خواهیم دو مقدار برابر بدست بیاوریم پس در قسمت تنظیمات Comparator باید عملیات مساوی را انتخاب کنیم بصورت زیر :

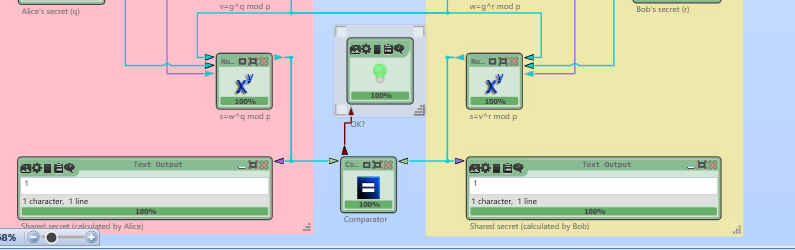


و در ادامه خروجی Comparator را به یک boolean output می دهیم که صحت عملیات مساوی را با روشن کردن چراغ سبز به ما نشان می دهد مانند شکل زیر :



در ادامه برای نمایش دو مقدار برابر به دست آمده از دو عملیات ، دو تا text output به صفحه اضافه می کنیم که یکی برای نمایش عدد بدست آمده از قسمت Alice هست و دیگری برای نمایش عدد بدست آمده در قسمت Bob هست که ووردی آن ها از قسمت

number operation دوم در هر قسمت است :



و بطور کلی پروژه بصورت زیر عمل می کند :

