به نام خدا

در این قسمت ابزار هایی را برای حمله ی متن آشکار به Hill Cipher معرفی می کنیم .

(نکته : ابزار هایی نیز برای حمله متن آشکار به فایل و تصویر وجود دارد ولی باتوجه به صورت سوال 2-27 تمرکز ما بر روی متن می باشد . )

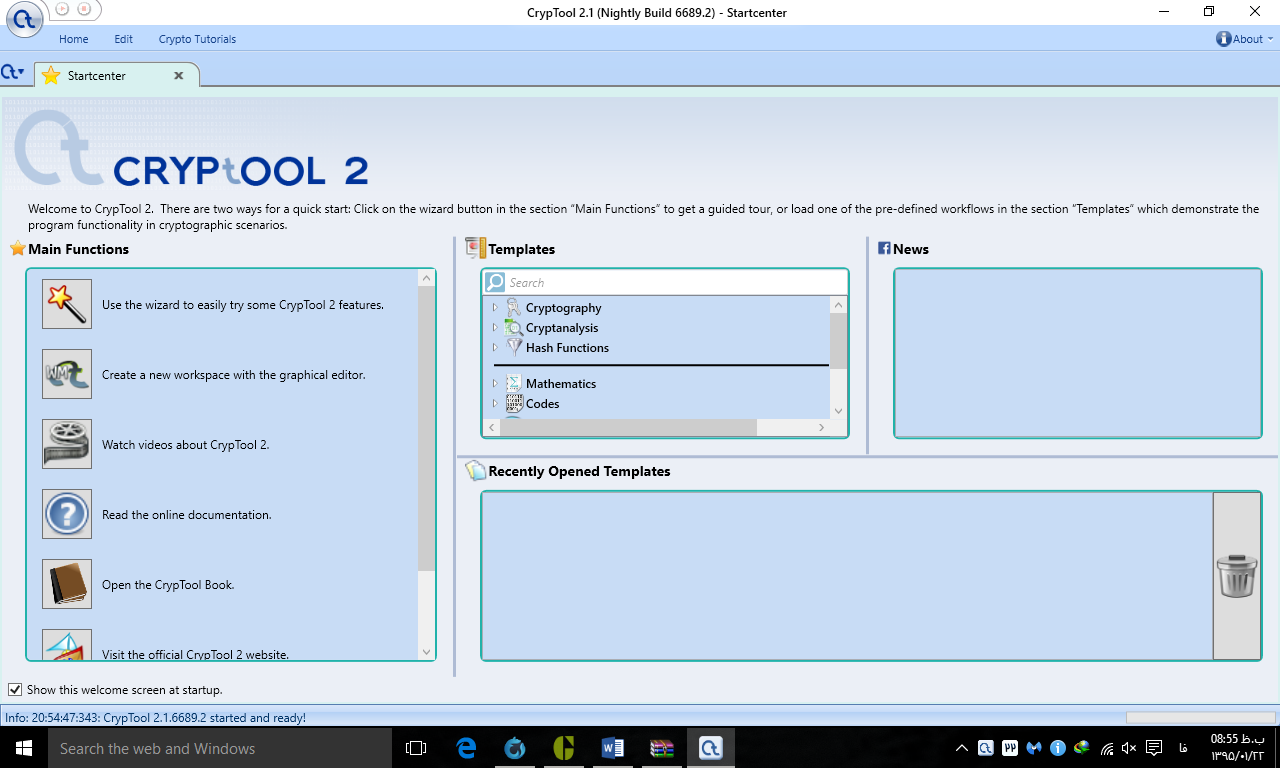
(نکته 2 : کد هایی نیز موجود هستند که حمله ی متن آشکار را روی رمزنگاری هایی غیر از HILL مثل Engima انجام میدهند)

ابزار اول

ابزار Cryptool

این ابزار یکی از قدرتمند ترین نرم افزار های آنالیز رمز می باشد .

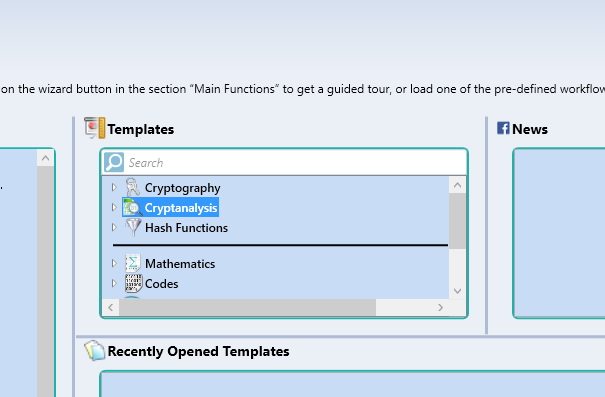
با اجرای نرم افزار چنین صفحه ای ظاهر می گردد .



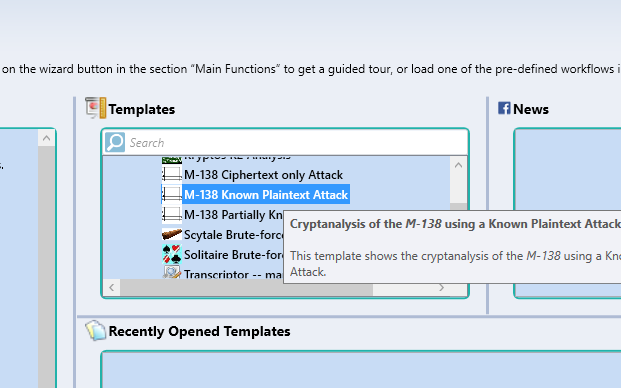
صفحه اصلی نرم افزار

این نرم افزار از هم رمزنگاری های مدرن و هم رمزنگاری های کلاسیک پشتیبانی می نماید .

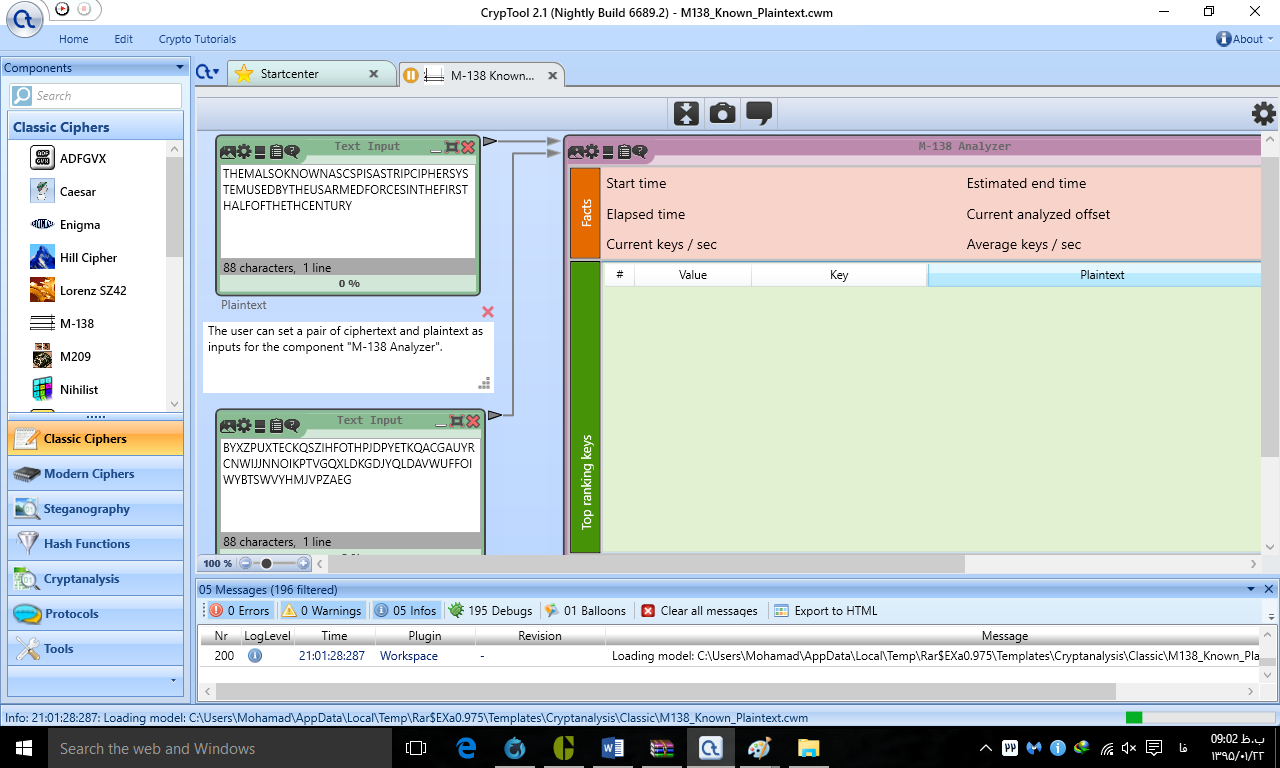
برای حمله در این نرم افزار از قسمت Template ، Cryptanalysis را انتخاب می نماییم .



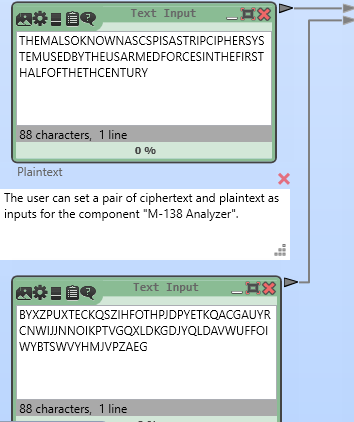
سپس برای حمله ی متن آشکار به رمز نگاری هیل دسته ی Classical را انتخاب کرده و سپس قسمت حمله متن آشکار را انتخاب می نماییم .



پس از انتخاب گزینه صفحه ی زیر باز می گردد .

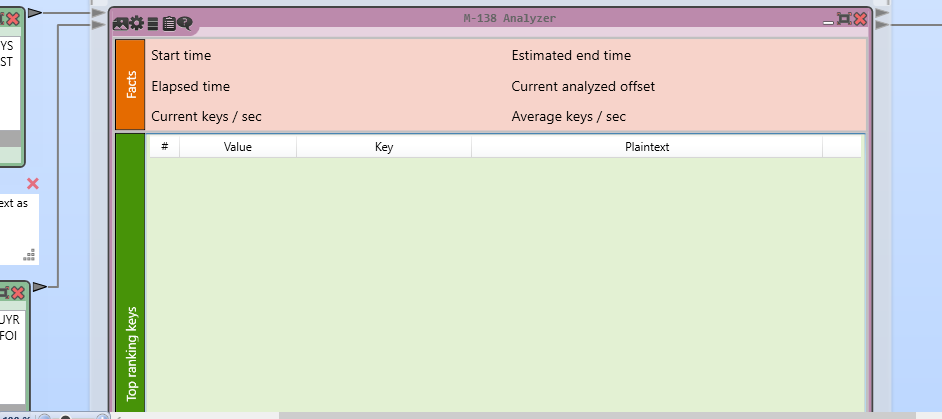


در قسمت زیر می توانیم متن اصلی و متن رمز شده را وارد کرده و در قسمت راست نتیجه را مشاهده نماییم .



محل ورود متن اصلی و رمز شده (تصویر 1)

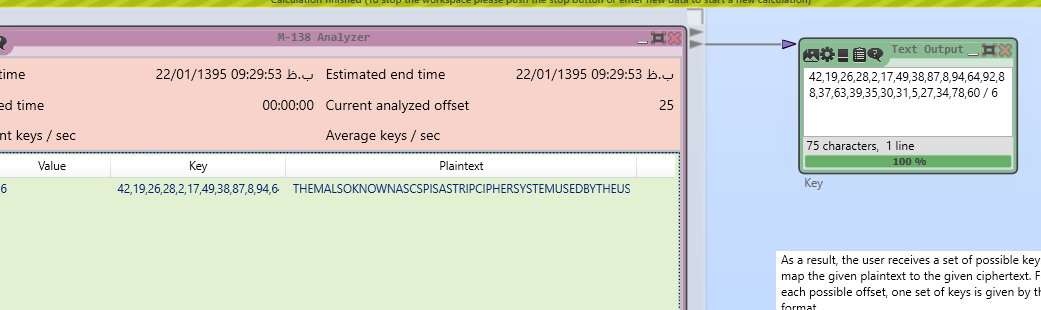
با ورود متن اصلی و متن رمز شده حتی این نرم افزار پر قدرت می تواند کلید های با اولویت بیشتر را نیز مشخص نماید .



در انتها پس از ورود متن اصلی و متن رمز شده بر روی دکمه play در نوار بالا کلیک کرده و آن را اجرا می نماییم .

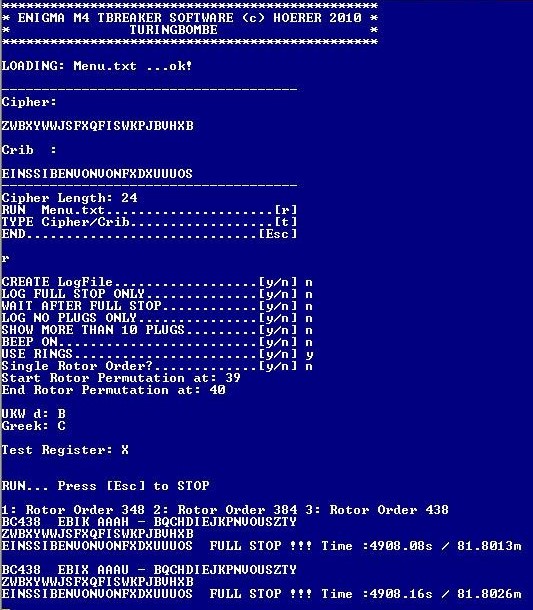


در شکل زیر نتیجه ی اجرا را برای متن اصلی و متن رمز شده ی تصویر 1 مشاهده می کنید . که کلید به دست آمده است .



ابزار بعدی ابزار Bombe Full Stop می باشد .

که در تصویر زیر نمایی از آن در حال اجرای حمله ی متن آشکار با استفاده از حلقه مشاهده می گردد .



ابزار سوم نیز ابزار Tbreaker می باشد که در زیر تصویر این نرم افزار نیز مشاهده می گردد .

