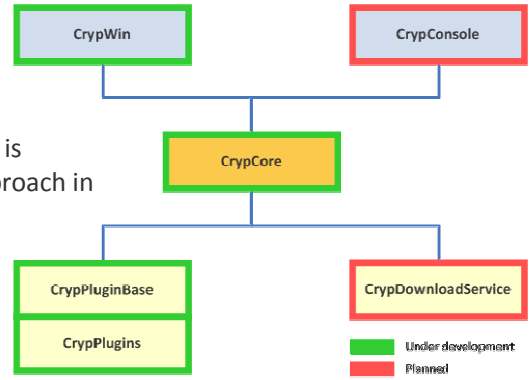
CrypTool Roadmap

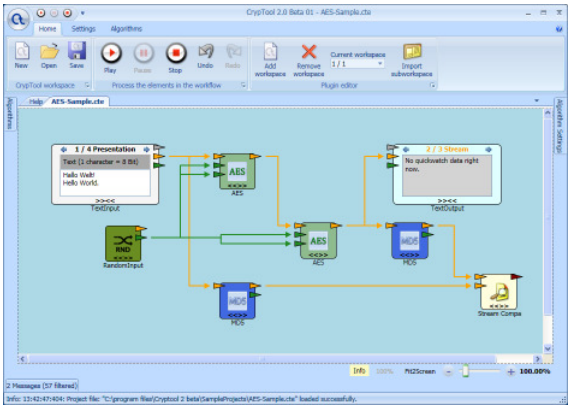
In the autumn of 2007 a small group of experienced software developers, from the German universities Duisburg-Essen, and Siegen, decided to work on a worthy successor to the well renowned e-learning application, **CrypTool 1.x**. By the spring of 2008 the new application design and architecture had been published to the open-source community, with the intention of delivering a range of cryptographic and teaching functions quickly and efficiently whilst at the same time ensuring that the high standards set by its predecessor were also met. Further development work throughout 2008 has seen the publication of an Alpha and Beta version of the new **CrypTool 2.0** framework.

The architecture of CrypTool 2.0 has been designed to ensure maximum flexibility and a lean low footprint framework. This ensures the effort required to integrate new functionality will be significantly less compared to CrypTool 1.x. This improvement is facilitated by a general modular design where almost every feature is provided as a plug-in. Figure 1 demonstrates the new architecture and modular approach in CrypTool 2.0:



The upper layer shows two different CrypTool 2.0 application interfaces; a command line interface (**CrypConsole**) which can easily be automated and a graphical user interface (**CrypWin**) which is based on the Windows Presentation Foundation (WPF).

The GUI is composed of two components: the main window which provides the primary interface and control elements for the application. This complies with the Microsoft Office 2007 User Interface Design Guideline, providing a consistent and rich user experience. Within the main window a visual programming control, provided by a plug-in, provides visualisation and workflow controls (cf. Figure 2) to enable intuitive manipulation and interaction of cryptographic primitives supported in CrypTool 2.0.



CrypCore provides the central point of administration for the plug-ins that implement CrypTool 2.0 functionality. A granular design and approach was taken for this critical system component allowing for a global plug-in store (amendable only by system administrators), along a user specific plug-in repository. This allows common functionality to be provided as a base to all users and where required an individual may install plug-ins specific to their needs and only accessible to that specific user.

The **CrypPluginBase** contains a collection of interfaces and attributes a plug-in developer must implement when writing a CrypTool 2.0 plug-in. A standardised interface is the primary mechanism that gives the CrypTool 2.0 core (**CrypCore**) the ability to automatically categorise, administer and manipulate every given plug-in.

The **CrypDownloadService** is a globally available web service providing certified and digitally signed CrypTool 2.0 plug-ins for download. A client embedded within makes the whole process of locating, downloading and installing plug-ins simple and transparent to the end user. The CrypTool 2.0 application can be configured to ensure that only digitally signed plug-ins can be loaded and executed.

Application localisation has been engineered into CrypTool 2.0 from the very beginning. Unlike CrypTool 1.x, CrypTool 2.0 has the ability to change the language at runtime suiting the users' requirements. To make a globally usable and standard version of CrypTool 2.0 available, every developer is required to provide an English user interface and user manual. As the language resources are separated from the application logic translations can be carried out easily with the aid of the separate localisation tool, **CrypResource**.

By means of the inline code editor C# code can be written, compiled and executed within CrypTool 2.0. This would allow lecturers to create valuable interactive educational exercises. For example the code outline of an algorithm could be provided to the students who then have to implement the lower level details. Subsequently, the result can be verified against a reference implementation made available in CrypTool 2.0.