CRYPTOOLS

Cryp
Tools

An introduction to CrypTools

"Making cryptography more accessible through programming"

CrypTools is an open source organisation and a community of people
passionate about cryptography whose mission is to make cryptography more
accessible.

Arthur Guiot, Lucas Gruwez & Luka Lafaye de Micheaux

May 17, 2020

Contents

1 Introduction

Cryptools originated in late 2017 when a group of students interested in cryptography were startled by how few good, and open source resources they were able to find on the topic. This prompted us to explore cryptography further, and implement ciphers in several programming languages, later resulting in the creation of a GitHub organisation. The team was later expanded as we invited other contributors to join us on this open source journey.

2 Our Work

The goal of the CrypTools organisation was to offer an easily accessible database of ciphers implemented in several programming languages, mainly JavaScript, Python, Swift, C++ and C.

Although structure was lacking at the start of the project, a standardized file system and templates were created later on. The structure that was agreed on was that each individual cipher would be given its own repository in our organization, in which an extensive readme file would explain the history and workings of a cipher. The implementations would be sorted by language into two files, one for encrypting, the other for decrypting.

Ciphers are currently classified by their progress into four main stages: idea, in progress, code review, and implemented. Ciphers would progress through each stage, until they reach the code review, where they can either be accepted as implemented or placed back into "in progress". The ciphers as they are currently classified are listed below:

Idea	`https://github.com/CrypTools/EmojiCipher`
	
	 `https://github.com/CrypTools/L337L4N6U463`

In Progress	`https://github.com/CrypTools/RSA`
	
	 `https://github.com/CrypTools/HashFunctions`
	
	 `https://github.com/CrypTools/EZEncrypt`
	
	 `https://github.com/CrypTools/AESCipher`
	
	 `https://github.com/CrypTools/MixCipher`
	
	 `https://github.com/CrypTools/TEACipher`

Code review	`https://github.com/CrypTools/BitShiftCipher`
	
	 `https://github.com/CrypTools/HashShiftCipher`
	
	 `https://github.com/CrypTools/RegressionCipher`
	
	 `https://github.com/CrypTools/Random`

Implemented	`https://github.com/CrypTools/CaesarCipher`
	
	 `https://github.com/CrypTools/VigenereCipher`
	
	 `https://github.com/CrypTools/ATBASHCipher`
	
	 `https://github.com/CrypTools/ROT13Cipher`
	
	 `https://github.com/CrypTools/XORCipher`
	
	 `https://github.com/CrypTools/Base64`
	
	 `https://github.com/CrypTools/Binascii`
	
	 `https://github.com/CrypTools/RailfenceCipher`
	
	 `https://github.com/CrypTools/VernamCipher`
	
	 `https://github.com/CrypTools/AffineCipher`

These ciphers are made accessible in three different ways. Firstly, as they are open source, their source code can be accessed through their respective GitHub repositories. The second way is via our website, where we have a section dedicated to test some of these ciphers. Last but not least, we have three different apps to that implement the ciphers: the Windows/Linux app which was developed by Leo Gervoson, the macOS app, and an iOS app, which were both developed by Arthur Guiot.

3 CrypTools Learn

We later came to the conclusion that we could do better to help the crypto community. When we noticed that most people who visited our repositories were looking to understand what cryptography is, we decided to create a platform for these people to learn and practice. The platform is under the responsibility of Arthur Guiot, who developed the system and the different levels that compose it. Through this platform, we provide a free online course to learn cryptography. The user will try to solve problems and challenges to understand what cryptography is all about. And even if he already knows cryptography, we think that he should definitely try because challenges are fun and are becoming really hard at the end. The system was first designed for the web, using native HTML, CSS and JavaScript and then ported to iOS using Swift.

4 Our current team

Founders

- Arthur Guiot - `https://github.com/arguiot`

- Lucas Gruwez - `https://github.com/lucasgruwez`

- Luka Lafaye de Micheaux - `https://github.com/aeternesatiatus`

Contributors

- Artur Y - `https://github.com/Asinsk`

- Mathias Lafaye de Micheaux - `https://github.com/mathiaslafaye`

- Remy Samkocwa - `https://github.com/remyskw`

- Sasha - `https://github.com/Sascha-T`

- Leo Gervoson - `https://github.com/lgrvs`

5   TLDR;

CrypTools an open source organisation and a community of people passionate about cryptography whose mission is to make cryptography more accessible. We started creating ciphers in various programming language, and now we also have software for most devices. We also teach cryptography through our online platform, based on challenges. In the future, we will continue providing free quality software for everyone and create new tools.