

PythonMTC3

New MTC3 international cipher contest

Florian Marchal

November 1st, 2019

20+ Years of CrypTool



MTC3 Recap

PythonMTC3

Status & Outlook

Participation

Demonstration

Feedback

MTC3 Recap

PythonMTC3

Status & Outlook

Participation

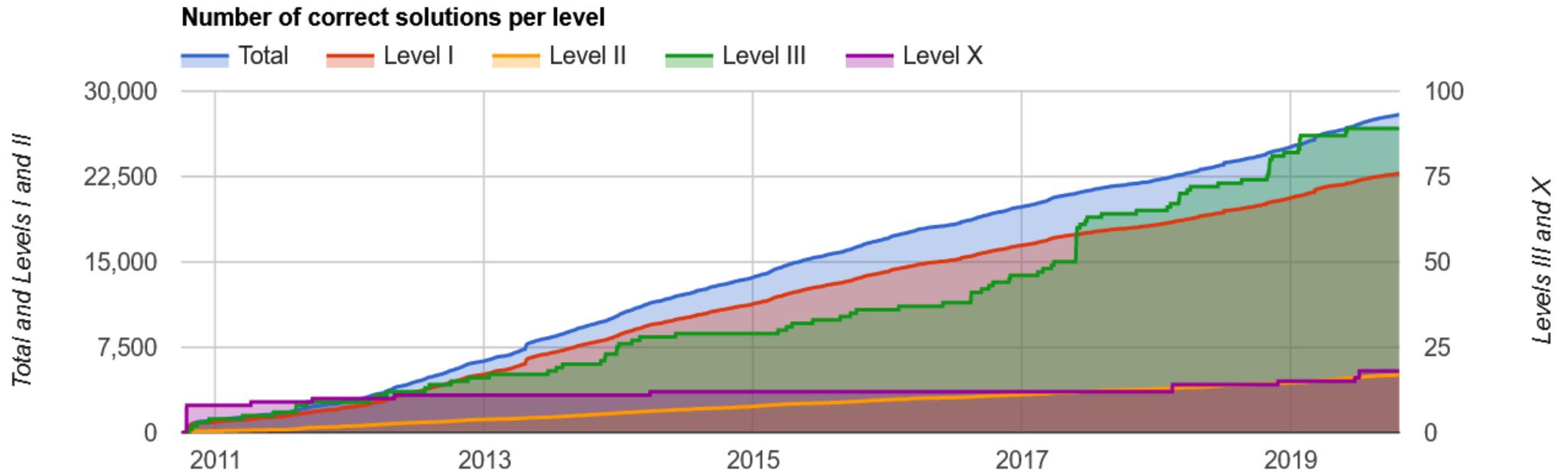
Demonstration

Feedback

MysteryTwister C3 (<https://www.mysterytwisterc3.org>)

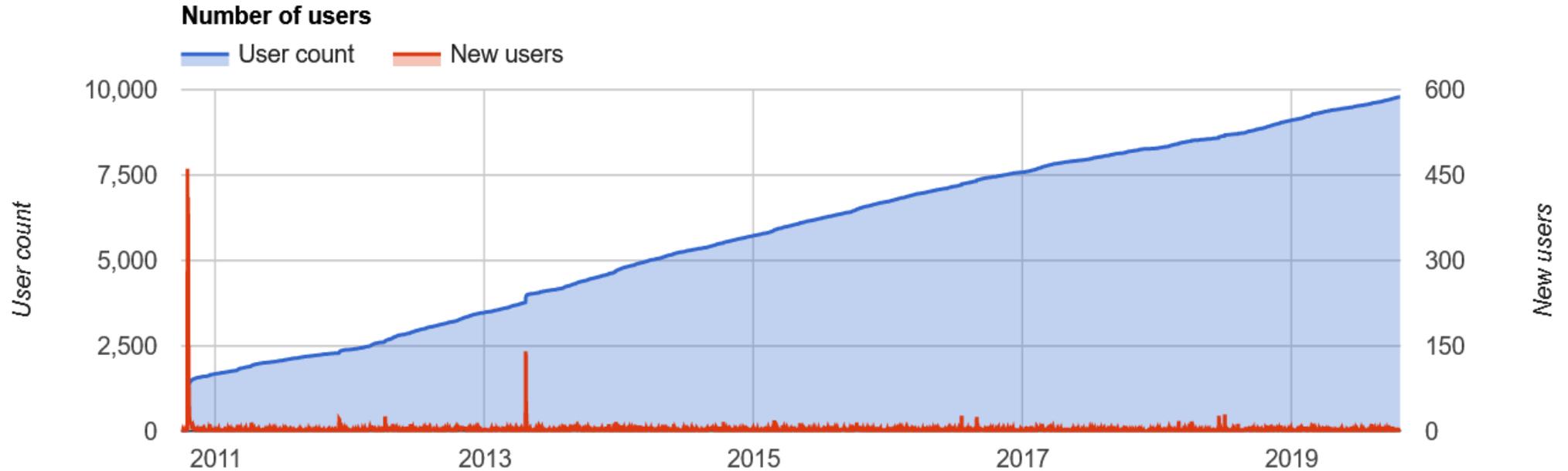
- Origin: design study “Crypto Challenge by CrypTool”
- Almost 10,000 active members
- Wide range of challenges (levels L1, L2, L3, X)
created by more than 50 different authors
- For beginners and experts alike

// MTC3 Recap



MTC3 Statistics Oct 23, 2019

// MTC3 Recap



MTC3 Statistics Oct 23, 2019

MTC3 Recap

PythonMTC3

Status & Outlook

Participation

Demonstration

Feedback

Why redevelop MTC3?

- Security (no external CMS)
- Responsiveness (mobile users)
- Maintainability
- Performance
- Some new features in the GUI

Why redevelop MTC3 using Python and Django?

- Python is easy to read and write
- Django is sort of state-of-the-art
- Django takes care of a lot of the heavy lifting

Frontend vs. backend

- Python (3.6.8) + Django (2.15)
- RabbitMQ and Celery (async)

- HTML + CSS + Bootstrap (4)
- JavaScript (as little as possible)

Pitfalls

- No prior experience with Django
- Django often has its own way of doing things
- Transformation of database into Django models
- General inconsistencies in the existing database

MTC3 Recap

PythonMTC3

Status & Outlook

Participation

Demonstration

Feedback

Status

- Static content is almost finalized
- Account management is production-ready
- Database transformation is a work-in-progress

... therefore a lot of functionality is still missing

Outlook

- Database is not fully finalized
- Configuration of production environment
- TESTING!!!

... going live is planned for end of November

MTC3 Recap

PythonMTC3

Status & Outlook

Participation

Demonstration

Feedback

Any help appreciated!

- Code is not open-sourced yet
- Private GitLab Repository: <https://gitlab.com/flomar/pythonmtc3>
- Just ask for privileges: florian@marchal.de

MTC3 Recap

PythonMTC3

Status & Outlook

Participation

Demonstration

Feedback

...zzzzZZZZzzzz...

MTC3 Recap

PythonMTC3

Status & Outlook

Participation

Demonstration

Feedback

Questions and Answers

Florian Marchal

florian@marchal.de

// Appendix – PythonMTC3 Screenshots

The screenshot shows the homepage of the MysteryTwister C3 website. The header includes the logo 'MysteryTwister C3 THE CRYPTO CHALLENGE CONTEST' and navigation links for Home, Challenges, Forum, Search, Account, Language, and Staff. A large banner features the text 'CHALLENGE YOUR KNOWLEDGE' and 'MTC3 tests your knowledge of cryptography.' Below the banner, the text reads 'Welcome to MTC3!' and 'The Cipher Contest'. A paragraph describes the site as a place for riddles and cryptograms. Another paragraph explains the challenge levels from Caesar cipher to AES. A final paragraph suggests starting with solved challenges. The footer contains the text '+++ MTC3 Fake Ticker +++ TODO/FIXME +++ MTC3 Fake Ticker +++'.

MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Home Challenges Forum Search Account Language Staff

CHALLENGE YOUR KNOWLEDGE

MTC3 tests your knowledge of cryptography.

Welcome to MTC3!

The Cipher Contest

You like riddles? You always loved to solve the crosswords in your newspaper? Or maybe you are just curious and want to find out about some of the ways to hide a secret (and possibly even to uncover it)? This is your place!

Here at MysteryTwister C3 you can solve crypto challenges, starting from the simple Caesar cipher all the way to modern AES, we have challenges for everyone. Our challenges range from level I to III, and an additional level X for "mystery" challenges (they may have been unsolved for a long time, mostly we don't know their solution or have no idea whether there is a solution at all).

If you are a beginner, it's probably best if you start trying those challenges that have been solved mostly (see table below). Additional information regarding MTC3 can be found [here](#).

You might want to try some of these challenges...

+++ MTC3 Fake Ticker +++ TODO/FIXME +++ MTC3 Fake Ticker +++

// Appendix – PythonMTC3 Screenshots

MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Home Challenges Forum Search Account Language Staff

The Four Levels



Level I Challenges - Pen & Paper

Level I challenges are similar to crossword puzzles from newspapers and can be solved with little cryptographic background. You might not even need a computer for solving level I challenges – all you need is a bit of clever thinking and probably a pen and paper. A program like [CrypTool](#) applied to a level I challenge can help reveal the answer within minutes or even seconds, if the necessary algorithms are already built in. Hence, if you are new to cryptography, but nonetheless interested in the mysterious topic of cryptanalysis, give the level I challenges a try. You will almost assuredly meet quickly with success.



Level II Challenges - Programming Skills Required

Level II challenges require some background knowledge in cryptology and usually some computational power. Additionally, you may require tools that are not available in such convenient packages like [CrypTool](#), [OpenSSL](#) or [Sage](#). Therefore, you must first thoroughly understand the problem in order to write a computer program, which helps you getting along. It could take hours or even days to solve a level II challenge. Hence, if you consider yourself well-armed with cryptologic knowledge (such as if you are a university student in a cryptographic course), give the level II challenges a try. Success may not come easily, but it will be a worthwhile endeavor.



Level III Challenges - Extensive Computing Power Recommended

Level III challenges require a thorough background in cryptanalysis and usually significant computational power as well. The problems in this level represent current research topics that are believed to be very difficult to solve. Thus, practical solutions may not even exist and ready-to-run tools almost certainly do not. The methodology to solve some of these challenges may already be known, but it may require such a huge amount of computational power that only a large group of people working together in a distributed system could obtain the solution. Challenges in this category mark the thin line between algorithms that are still secure and those that are not. Solving them may take weeks or even several months. Hence, challenges in this level are intended for entire research groups with many experts in cryptanalysis, programming, and distributed systems. Success cannot be guaranteed, but if you are the first to successfully solve one of these challenges, it probably would catch the attention of the scientific community. Of course, it still remains up to you to publish or present any such scientific

+++ MTC3 Fake Ticker +++ TODO/FIXME +++ MTC3 Fake Ticker +++

// Appendix – PythonMTC3 Screenshots

MysteryTwister C3 THE CRYPTO CHALLENGE CONTEST Staff Interface

Home Challenges Forum Search Account Language Staff

Maintain Authors

Authors Challenges Solvers List Create Edit Delete

#	Name	User
1	Mark Stamp	
2	A. Wacker	
3	T. Schroedel	
4	Lehrstuhl für Kryptologie u. IT-Sicherheit, Ruhr-Universität Bochum	
5	K. Schmeh	
6	Ed Schaefer	
7	<i>No name assigned.</i>	
8	Sören Rinne	
9	Nina Schöllhammer	
10	Pascal Schöttle	
11	Coen Ramaekers	
13	Henning Wolter	
14	Dennis Grunert	
19	Volker Simon	