PythonMTC3
New MTC3 international cipher contest

Florian Marchal
November 1st, 2019
20+ Years of CrypTool
// Agenda

- MTC3 Recap
- PythonMTC3
- Status & Outlook
- Participation
- Demonstration
- Feedback
// Agenda

- 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

Number of correct solutions per level
- Total
- Level I
- Level II
- Level III
- Level X

MTC3 Statistics Oct 23, 2019
// Agenda

- 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
// PythonMTC3 – Redevelopment of MTC3

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
// Agenda

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
// Agenda

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
// Agenda

- MTC3 Recap
- PythonMTC3
- Status & Outlook
- Participation
- Demonstration
- Feedback
...zzzZZZzzz...
Questions and Answers

Florian Marchal
florian@marchal.de
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 1 to 3, 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 Token +++ T00D/FUXME +++ MTC3 Fake Token +++
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 cryptography 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 cryptographic 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.
## Maintain Authors

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