Status of CrypTool 2
Munich, October 31st 2019

Dr. Nils Kopal
CrypTool 2 Project
kopal@cryptool.org
CrypTool Meeting 20+ Years
1. What is CrypTool 2?

2. Highlights

3. Future Plans
1. What is CrypTool 2?
1. What is CrypTool 2

• „Graphical programming language“
  – over 170 components for cryptography/cryptanalysis
  – over 220 templates for cryptography/cryptanalysis

• **Classical and modern cryptography**
  – Caesar, substitution, transposition, ADFGVX, Enigma, M209, etc.
  – AES, RC2, RC4, DES, Diffie-Hellman, RSA, SHA-1, Keccak (SHA-3), etc.

• **Cryptanalysis of classical and modern ciphers/protocols**
  – Vigenère analyzer, keysearcher (brute-force attacks on symmetric modern ciphers), factorization, Enigma analysis, etc.
1. What is CrypTool 2

• **CT2 current version:** *2.1*
  - next release in December (Christmas update)

• **Different types of builds**
  - Nightly builds every night 😊
  - Betas and releases 1-3 times a year

• **Two installation types**
  - Installation via executable (NSIS installer)
  - ZIP-installation via unpacking

• **Automatic updates**
  - Both installation types support auto-updates
1. What is CrypTool 2

• Three Languages: **English, German, and Russian**
  – Main application, components, help, templates, Wizard
  – Russian done by automatic translation 😊

• .NET Version: **4.7.2**

• We use **Visual Studio 2019 (Community Edition)**
Some challenges we faced and solved in the last year(s)

• Update of Visual Studio to new version (from 2010 to 2019)
  – Pro: newest version 😊
  – Contra: update of build server takes a lot of time and is difficult

• Change from x86 to x64 target
  – Pro: more memory!! 😊
  – Contra: update all libraries and components to x64

• Update of all C++ libs to newest Visual C++ redistributables
  – Pro: no need for parallel installations of different redistributables
  – Contra: update of all libraries and components to the newest version
1. What is CrypTool 2

1. The Startcenter – the entrance into the application
# 1. What is CrypTool 2

## 2. The Wizard – for beginners

![Wizard Image]

**WIZARD**

Please select the kind of task you want to fulfill and click “Next” to proceed.

<table>
<thead>
<tr>
<th>Task Selection</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption/Decryption</td>
<td>Selecting this allows you to encrypt a plaintext or decrypt a ciphertext. You can choose which algorithm you want to use for doing this.</td>
</tr>
<tr>
<td>Cryptanalysis</td>
<td></td>
</tr>
<tr>
<td>Hash Functions</td>
<td></td>
</tr>
<tr>
<td>Mathematical Functions</td>
<td></td>
</tr>
<tr>
<td>Codes</td>
<td></td>
</tr>
<tr>
<td>Tools</td>
<td></td>
</tr>
</tbody>
</table>
1. What is CrypTool 2

3. The Workspace Manager – implements the graphical programming language
1. What is CrypTool 2

4. The CrypCloud – allows distributed cryptanalysis in the „cloud“
1. What is CrypTool 2

5. The CrypTool Store – allows to easily publish components
1. What is CrypTool 2

6. The Online Help – contains information about each component (en/de/ru)
2. Highlights
2. Highlights

1. Enigma visualization of internal workings
2. Highlights

2. One-time pad misusage (same key used twice)

This template shows why the One Time Pad should always be used only once.

Plaintext A and plaintext B are both encrypted using the same one-time pad:

\[ \text{Encrypt}_A = \text{Plaintext}_A \oplus \text{One Time Pad} \]
\[ \text{Encrypt}_B = \text{Plaintext}_B \oplus \text{One Time Pad} \]

Both ciphertexts analyzed independently do not offer any information if the attacker has not the one-time pad. But if the attacker combines \( \text{Encrypt}_A \) and \( \text{Encrypt}_B \) using the XOR function, he can reveal a huge amount of information.

This can easily be explained by looking at the equations:

\[ \text{Encrypt}_A \oplus \text{Encrypt}_B = (\text{Plaintext}_A \oplus \text{One Time Pad}) \oplus (\text{Plaintext}_B \oplus \text{One Time Pad}) = \text{Plaintext}_A \oplus \text{Plaintext}_B \]

Thus using a one-time pad twice an attacker may remove the one-time pad completely from both ciphertexts and gain information about both plaintexts.

So using a one-time pad more than once is a bad idea :(
3. Vigenère cryptanalysis – breaking of Kryptos K1 and K2

Kryptos is an encrypted sculpture by American artist Jim Sanborn located on the grounds of the Central Intelligence Agency (CIA) in Langley, Virginia. Since its dedication on November 3, 1990, there has been much speculation about the meaning of the encrypted messages it bears. Of the four messages, three have been solved, with the fourth remaining one of the most famous unsolved codes in the world. The sculpture continues to provide a diversion for cryptanalysts, both amateur and professional, who are attempting to decrypt the final section.

Source: http://en.wikipedia.org/wiki/Kryptos

With this template we demonstrate the solution of Kryptos K1 - the first message of the Kryptos sculpture.

The Vigenère Analyzer component takes the K1 ciphertext and the Kryptos alphabet (KRYPTOSA,B,C,D,E,F,G,H,I,J,K,L,M,N, Q,U,V,W,X,Y,Z) and performs a hillclimb-search for Vigenère keys between 5 and 20 using 100 restarts.

Nils Kopal

2019-10-31

17
2. Highlights

3. Vigenère cryptanalysis – breaking of Kryptos K1 and K2
2. Highlights

4. Letter frequency analysis and Friedman test
5. Homophonic Substitution Analyzer – breaking of the Zodiac-408 letter

Cryptanalysis of the Zodiac-408 cipher

"Zodiac Killer" is the pseudonym of a serial killer who operated in Northern California. The killer's identity remains unknown; Zodiac murdered victims in Berkeley, Lake County, and San Francisco between December 1968 and October 1969. Four men and three women between the ages of 19 and 26 were targeted. The killer originated the name "Zodiac," in a series of haunting messages sent to the local Bay Area press. These messages included four ciphers (or ciphers). Of the four ciphers send, only one (Zodiac-408) has been definitively solved. Source: https://en.wikipedia.org/wiki/Zodiac_Killer

This template allows to break the Zodiac-408 message using the Homophonic Substitution Analyzer by iteratively solving cryptograms. The interactive, semi-automatic mode is selected by default in the analyzer's settings.

After starting the template’s workspace, the first step is clicking the Pay button. The analyzer needs some time to load huge cryptograms' language statistics and to fit the plaintext and the ciphertext areas with letters.

In the semi-automatic mode, the 8 buttons: "AnalyzeCiphers," "Tweak plugged values," and "Hide/Show words" within the analyzer components are enabled. To start the analysis process click on the "Analyze" button. After some time, the software will automatically lock already revealed words. You can stop "Show" and return "Analyze" the analysis process at any time. When the analysis is stopped, you can see two boxes with single letters of the revealed plaintext. By yourself, you will reveal the ciphertext. If loading a better with the "Pay" message button, you can change settings using the right mouse button. Click on the right mouse button shows the next valid letter filling the right mouse button plus Shift selects the previous letter in the plaintext's alphabet.

Cryptool dialog for encryption - Text data
## 2. Highlights

### 6. Avalanche effect visualization (AES)

#### Encryption Results after All Rounds of AES-128

<table>
<thead>
<tr>
<th>Round</th>
<th>Ciphertext (hex)</th>
<th>% of flipped bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>35-8D-9B-C5-D7-4C-5E-89-62-B2-AA-FF-6B-04-27-FC</td>
<td>0.8 %</td>
</tr>
<tr>
<td>1</td>
<td>7C-2B-01-04-BB-55-46-1A-62-D2-5C-6F-C0-47-28-4C</td>
<td>10.2 %</td>
</tr>
<tr>
<td>2</td>
<td>62-79-5C-07-67-94-68-2C-53-6A-83-28-3B-C4-10-9F</td>
<td>46.9 %</td>
</tr>
<tr>
<td>3</td>
<td>5C-99-CE-B1-F0-23-FD-8D-0F-E5-DB-96-10-30-A3-02</td>
<td>43.8 %</td>
</tr>
<tr>
<td>4</td>
<td>22-DF-26-4A-4B-AF-19-72-1D-66-AE-04-36-FC-30-CB</td>
<td>49.2 %</td>
</tr>
<tr>
<td>5</td>
<td>11-C7-D4-C8-5C-DD-3E-2E-A2-8C-C0-FB-4C-3B-D3-7E</td>
<td>42.2 %</td>
</tr>
<tr>
<td>6</td>
<td>16-F1-F2-EB-08-DE-C6-87-03-03-FD-DD-54-FF-91-8E</td>
<td>47.7 %</td>
</tr>
<tr>
<td>7</td>
<td>50-9E-D2-C5-8F-AP-7E-64-6B-D7-B7-80-1E-EB-50-CF</td>
<td>43.8 %</td>
</tr>
<tr>
<td>8</td>
<td>18-E0-CB-3B-1D-0F-0B-69-11-09-CD-29-31-17-F9-86</td>
<td>49.2 %</td>
</tr>
<tr>
<td>10</td>
<td>87-6B-3A-E8-58-FB-58-79-B7-E3-61-7F-00-63-4F-32</td>
<td>39.8 %</td>
</tr>
</tbody>
</table>

Check avalanche effect after round ...

---

Nils Kopal

2019-10-31
2. Highlights

7. Differential cryptanalysis
2. Highlights

8. Image hashing (robust hash functions)
2. Highlights

9. Factorization of big numbers with the quadratic sieve

Above in the input component, you can enter any number. This number will be factorized by the quadratic sieve component when executing the workspace (Play button). The result will be shown in the output component on the right.

Numbers can also be entered as a mathematical expression, e.g., $2^{10} + 13$. If the result of the mathematical expression is a fraction, only the integer part is used, e.g., $2^{10} + 13 - 7 / 2 = 36$.

The given number is $(2^{30} - 1) / 2$ which is 303 digits long and has 5 factors. After quickly splitting off the two small factors which are found first, most of the time (about 15 minutes) is used to factorize the 291 bit composite (88335578743).
2. Highlights

10. Visualization of the BB84 quantum key exchange protocol
2. Highlights

11. Cryptanalysis of (short) Playfair ciphers (using an external cryptanalysis program written by Lasry)

The Playfair cipher or Playfair square or Wheatstone-Playfair cipher is a manual symmetric encryption technique and was the first literal digram substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair for promoting its use. The technique encrypts pairs of letters (bigrams or digrams), instead of single letters as in the simple substitution cipher and rather more complex Vigenère cipher systems then in use. The Playfair is thus significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it.

605 characters, 1 line
100%

This template demonstrates a ciphertext-only attack on the Playfair cipher. The plaintext above is encrypted with the Playfair component and the resulting ciphertext is sent to the Playfair Analyzer.

Please note that in Playfair for every key there exist several equivalent keys that generate the same ciphertext.
12. AES-encrypted video chat (with Diffie-Hellman)

This template shows an AES encrypted video and audio chat over an IP-based network without any preshared key.

You have to set the IP of your chat partner below in order to connect to him. By default you will connect to yourself.

This template works basically in two phases.
In the first phase it will exchange an 128 bit AES session key with itself or with a remote version of itself, by using the Diffie-Hellman key exchange.

If the key is exchanged it will start the video chat and encrypt the packets with the session key.
2. Highlights

13. Connection to the DECODE database for downloading original historic ciphers
2. Highlights

14. DECODE Decipherer in CT2 – decryption of historic ciphers
3. Future Plans
3. Future Plans

- Make CT2 more attractive for users and developers
  - “Achievement system” (inspired by computer games)
- Establish CT2 more in research and teaching
- Continue implementing current developments of cryptology
  - Classic/historic cipher analysis: **DECRYPT project**
  - Modern cryptology/cryptanalysis, e.g. **post-quantum cryptography**
  - Cryptanalysis **framework of choice** (for symmetric ciphers)
- Implement a rich set of YouTube videos for users/developers
  - Create content for the CrypTool 2 **YouTube** channel
- Wishes? What do you think/want?
Questions and discussion

Thank you very much for your attention!

Do you have questions?