



CRYPTOOL (1&2) |

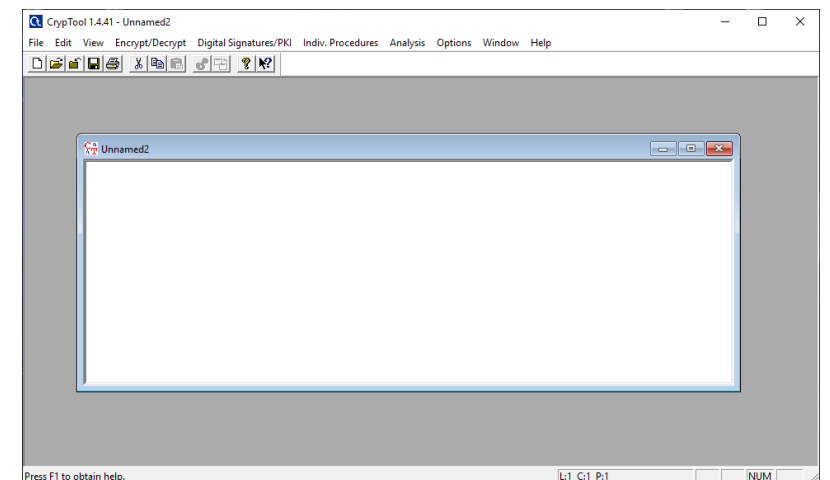
WHAT IS CRYPTOOL?

A freeware Originally developed as an awareness program for a large bank (internal training purpose)

Considered as « the most comprehensive cryptography learning tool worldwide »

2 versions : Cryptool 1 and Cryptool 2 (both for windows) + JCryptool, ...

→ <https://www.cryptool.org>



WHAT IS CRYPTOOOL?

Main features:

- classical cryptography
- cryptanalysis : attack on classical methods, analysis methods
- visualisations / demos

DEMONSTRATION: VIGENERE ANALYSIS

Encrypt a sample file with **TESTETE** (for instance:

<https://www.nytimes.com/2019/04/11/world/europe/uk-theresa-may-brexit.html>)

- “*Crypt/Decrypt*” \ “*Symmetric (classic)*” \ “*Vigenère*”
- Enter TESTETE → “*Encrypt*”

Analysis of the encryption results:

- “*Analysis*” \ “*Symmetric Encryption (classic)*” \ “*Ciphertext only*” \ “*Vigenère*”
- Derived key length 7, derived key TESTETE

DEMONSTRATION: VIGENERE ANALYSIS

Encrypt starting sample with **TEST**

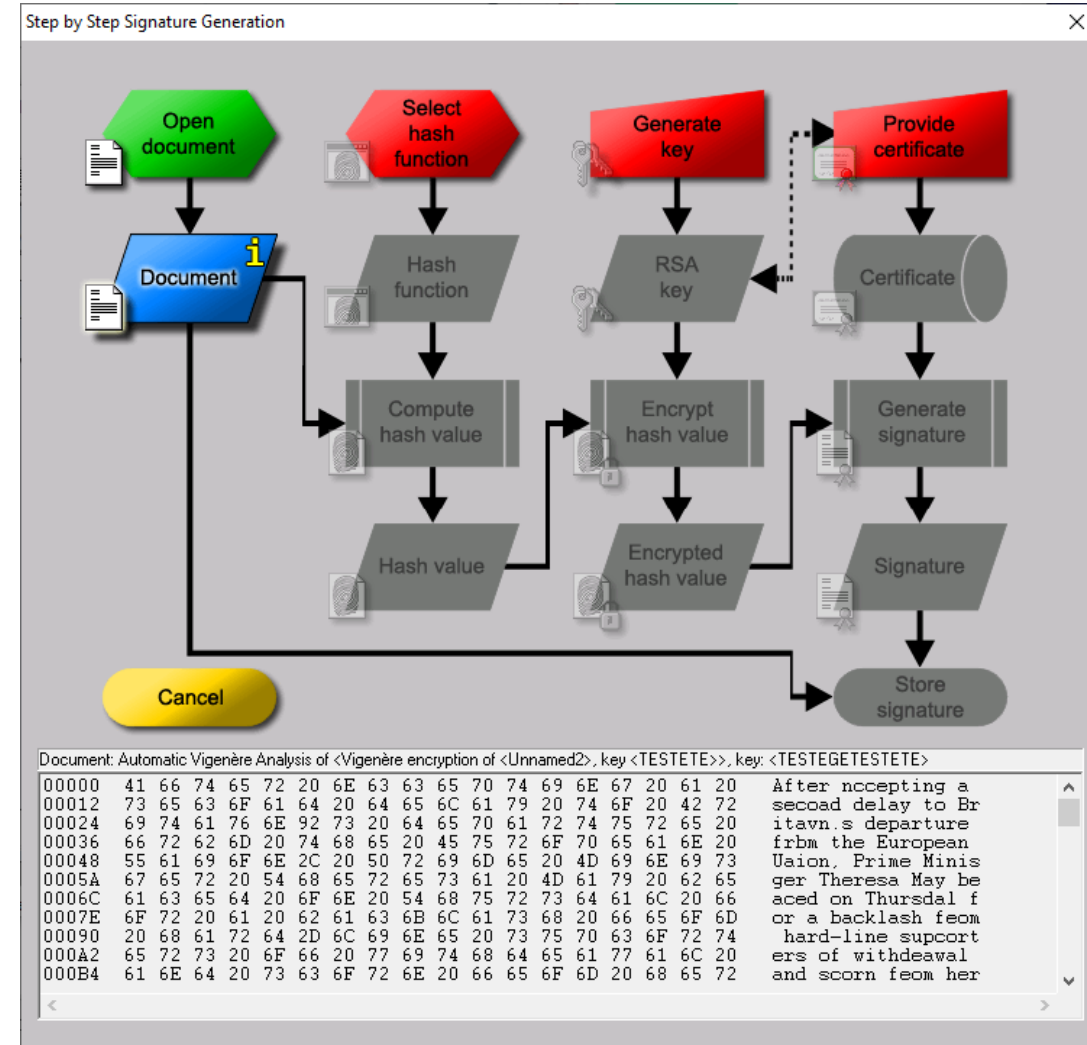
- “*Crypt/Decrypt*” \ “*Symmetric (classic)*” \ “*Vigenère*”
- Enter TEST → “*Encrypt*”

Analysis of the encryption results:

- “*Analysis*” \ “*Symmetric Encryption (classic)*” \ “*Ciphertext only*” \ “*Vigenère*”
- Derived key length 8 – incorrect
- Key length automatically set to 4 (can also be adjusted manually)
- Derived key TEST

EXAMPLES

Digital Signatures/PKI | Signature Demonstration



BASICS

To begin with, open the CrypTool and go **File | New**. In the newly opened window type the message you wish to encode. The contents of your message is your personal choice, however, you should ensure its length is greater than 64 characters for the purpose of later analysis.

select **Crypt/Decrypt | Symmetric (classic) | Caesar / ROT-13...** From here you will be presented with the option of encrypting with either Caesar or ROT-13 variants.

BASICS

Now, you can analyse the strength of the encryption using a variety of techniques. We shall begin by looking at the entropy, for a description of what entropy calculates please refer to chapter 2.1 CrypTool Manual.

Select from the menu bar **Analysis | Tools for Analysis | Entropy**.

This should display the calculated result. In the same manner proceed to analyse your text using the other tools available: Floating Frequency Histogram N-Gram Autocorrelation Periodicity (All of which can be accessed through the menu bar, **Analysis | Tools for Analysis**)

Q : Which tool or technique would be most effective for a cryptanalyst to use to decipher a text encrypted with the Caesar cipher, and why?

BASICS

Select **Crypt/Decrypt** | **Symmetric (classic)** | **Vigenère**. Think of a key to use and select **Encrypt**. Like earlier, analyse your encrypted message with all of the tools available.

Q. What do you notice about the histogram results when text is encrypted with the Vigenère cipher in comparison to the results of the Caesar cipher? Why is this the case?

BASICS

The next cipher that we will look at is the **Playfair** cipher. Using this cipher we shall encrypt one of Albert Einstein's famous quotes:

The difference between stupidity and genius is that genius has its limits.

Select this cipher for encryption in the usual manner. Make sure the 5x5 Matrix is selected (the 6x6 Matrix is for the inclusion of numbers) and use the key phrase:

AlbertEinstein

Q. There is an error in the following ciphertext representation of this quote, what is it?
SDAHFOWGRABSSRERIVBYBSCIMQTFNIVETGHBSNQCNCSDTDHBSNQCD
ECNICIFCTIC

Q. Of the three discussed ciphers (Caesar, Vigenère, Playfair), which is the most secure and why?

DIFFERENT TOOLS

Indiv. Procedures | Password Quality Meter...

✕

Password Quality Meter

Description

It is not possible to exactly determine and quantify the security of passwords. But it is possible to estimate the security of passwords based on certain assumptions.

Below you can see four implementations of password quality meters, helping you to estimate the security of your password.

Password input

Please enter your password here. The password quality is shown in percent and updated with every key stroke.


Password:

☒ Show password

Password length:

Password quality based on assumptions (and password entropy in bit)

KeePass:	<div><div></div></div>	15 % (19 bit)
Mozilla:	<div><div></div></div>	60 %
PGP:	<div><div></div></div>	14 % (17 bit)
CrypTool:	<div><div></div></div>	8 % (10 bit)



Resistance against dictionary attacks (evaluates only the first 32 characters)

Compliant with password guidelines:

- No (Password is too short: 6/8)
- No (Password contains too few special characters: 0/1)

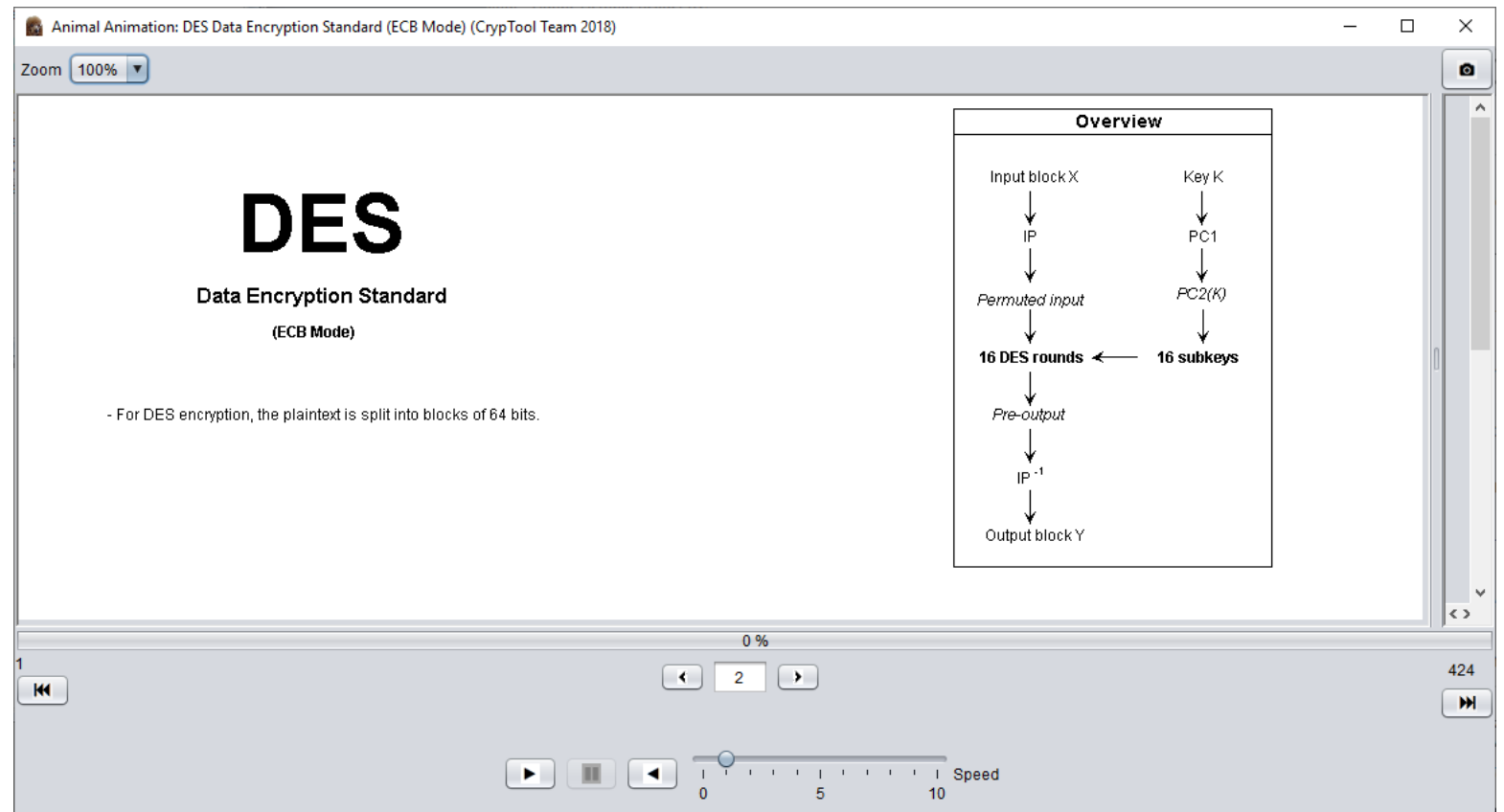
Reconstruction from words, sequences and patterns:
Found: -
Patterns: -
Sequences: 123456
Keyboard sequences: 123456
Dictionary words [1,648,594]: 123456

Password guidelines

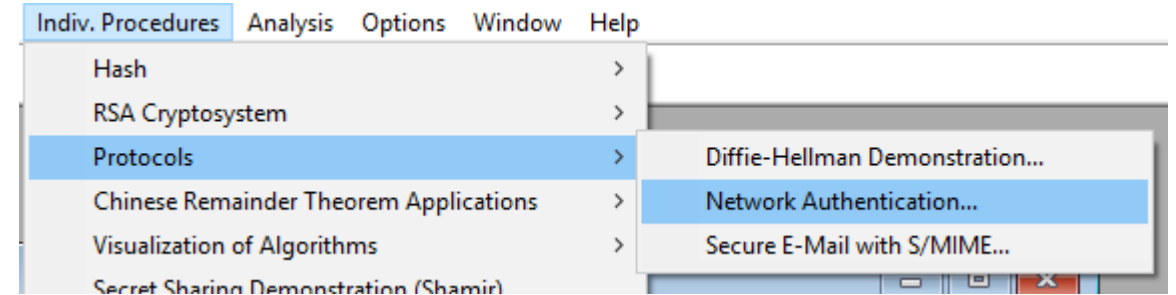
Cancel

DIFFERENT TOOLS

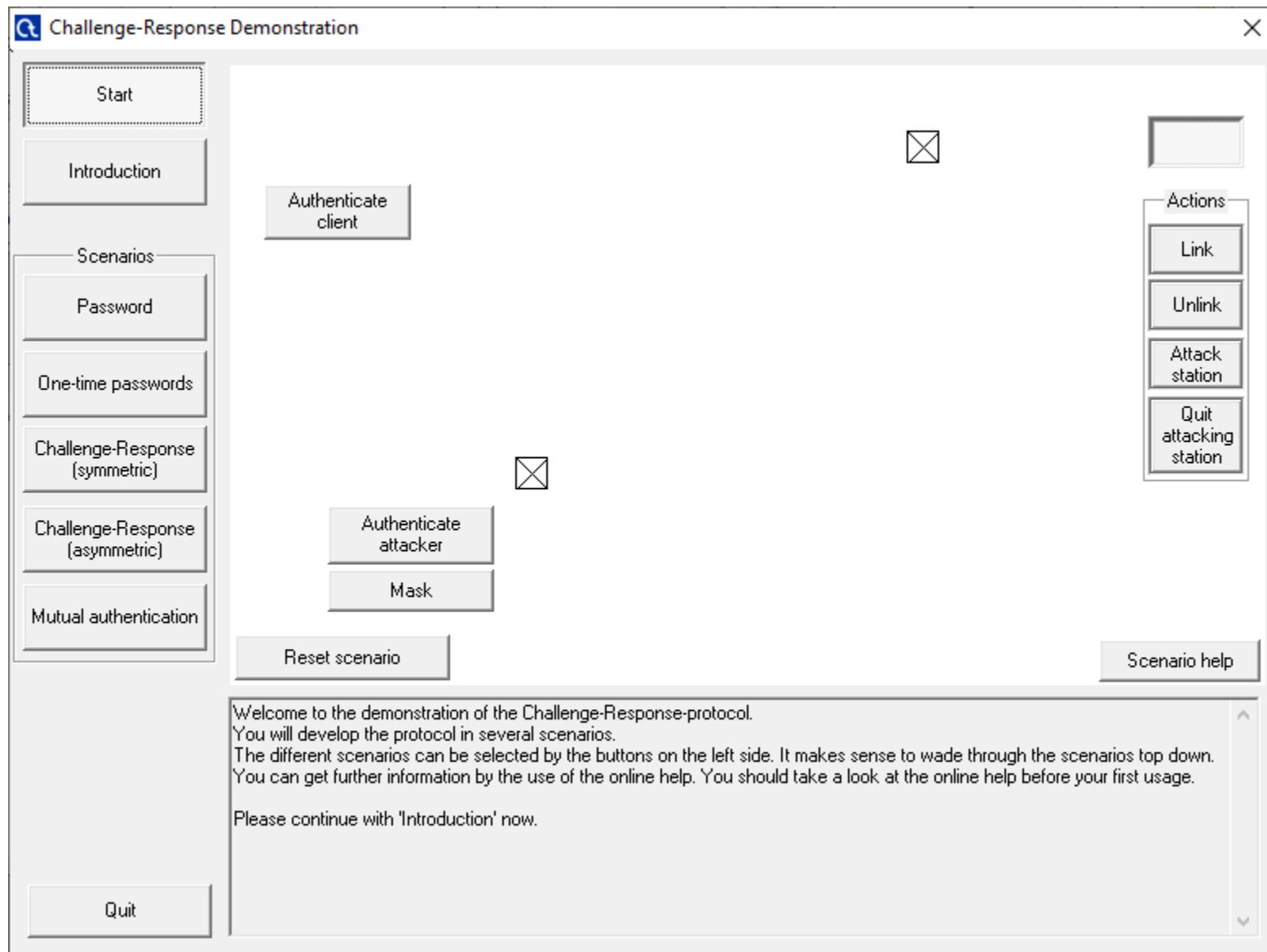
Indiv. Procedures | Visualization of Algorithms > ...



AND SCENARIOS!



Indiv. Procedures | Protocols | Network Authentication...

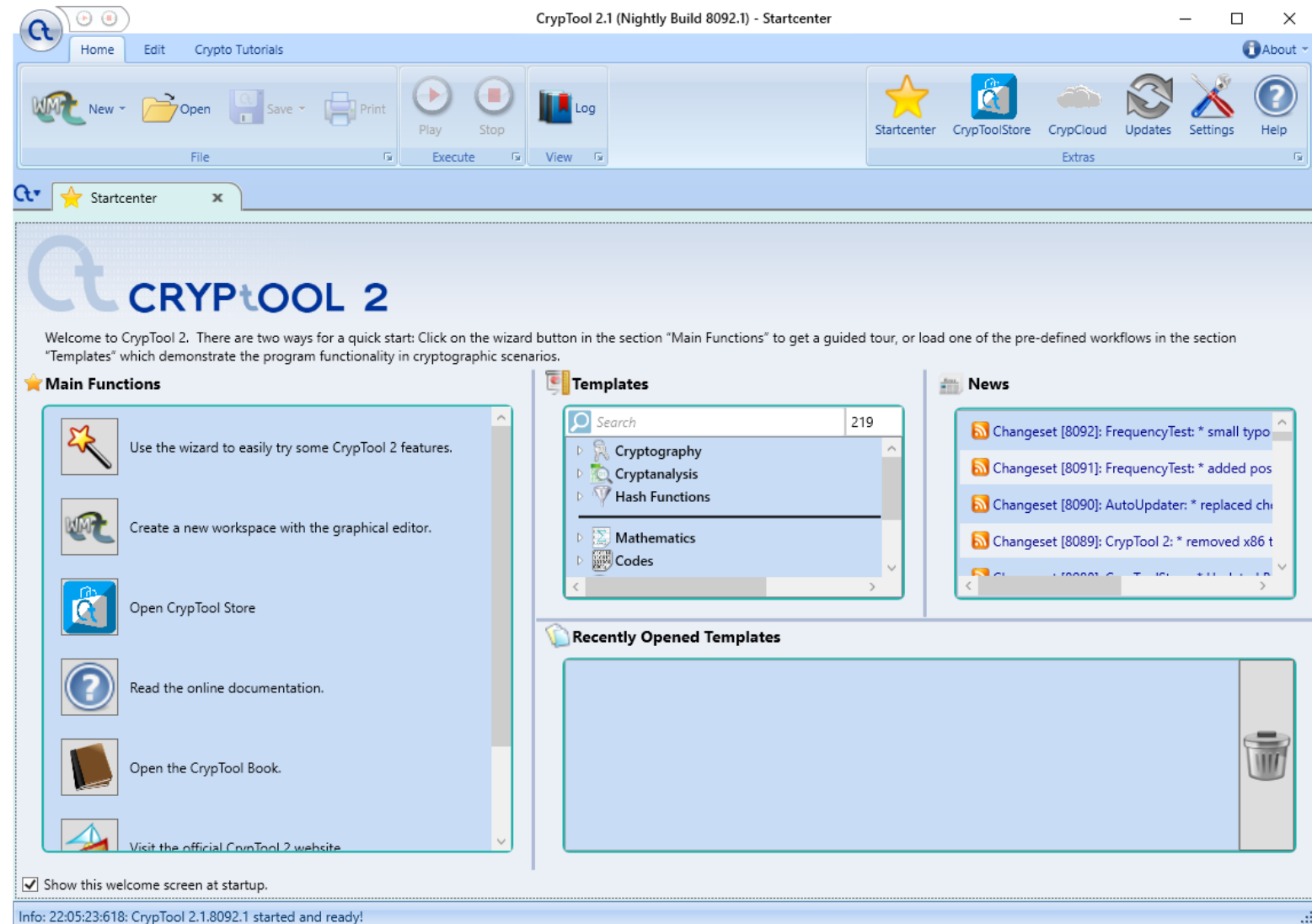


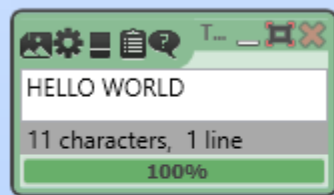


ASSIGNMENT: PERFORM THE DIFFERENT SCENARIOS

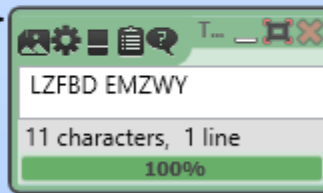
CRYPTOOL 2

New version of Cryptool
with visual programming
capabilities





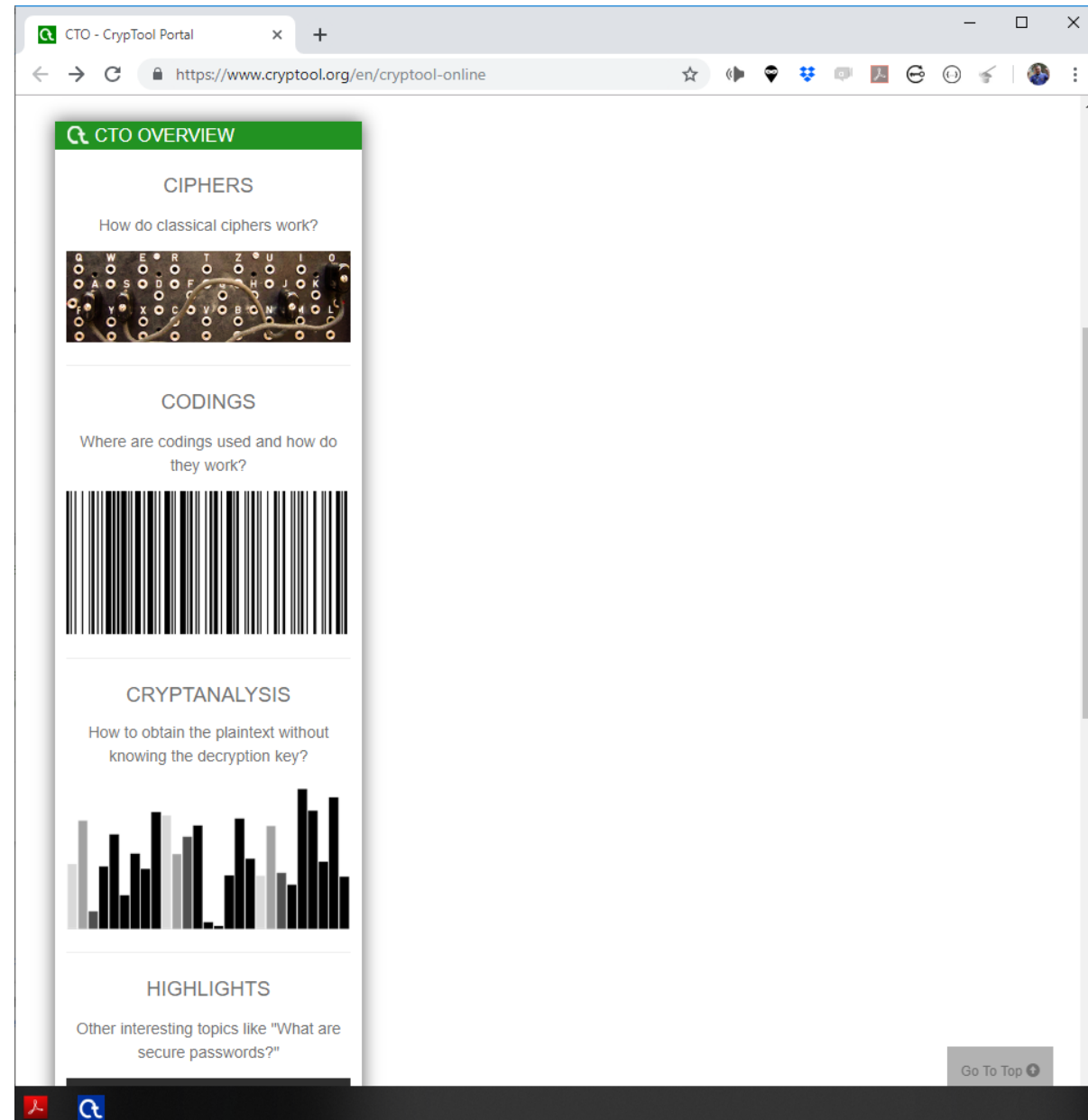
Text Input



Text Output

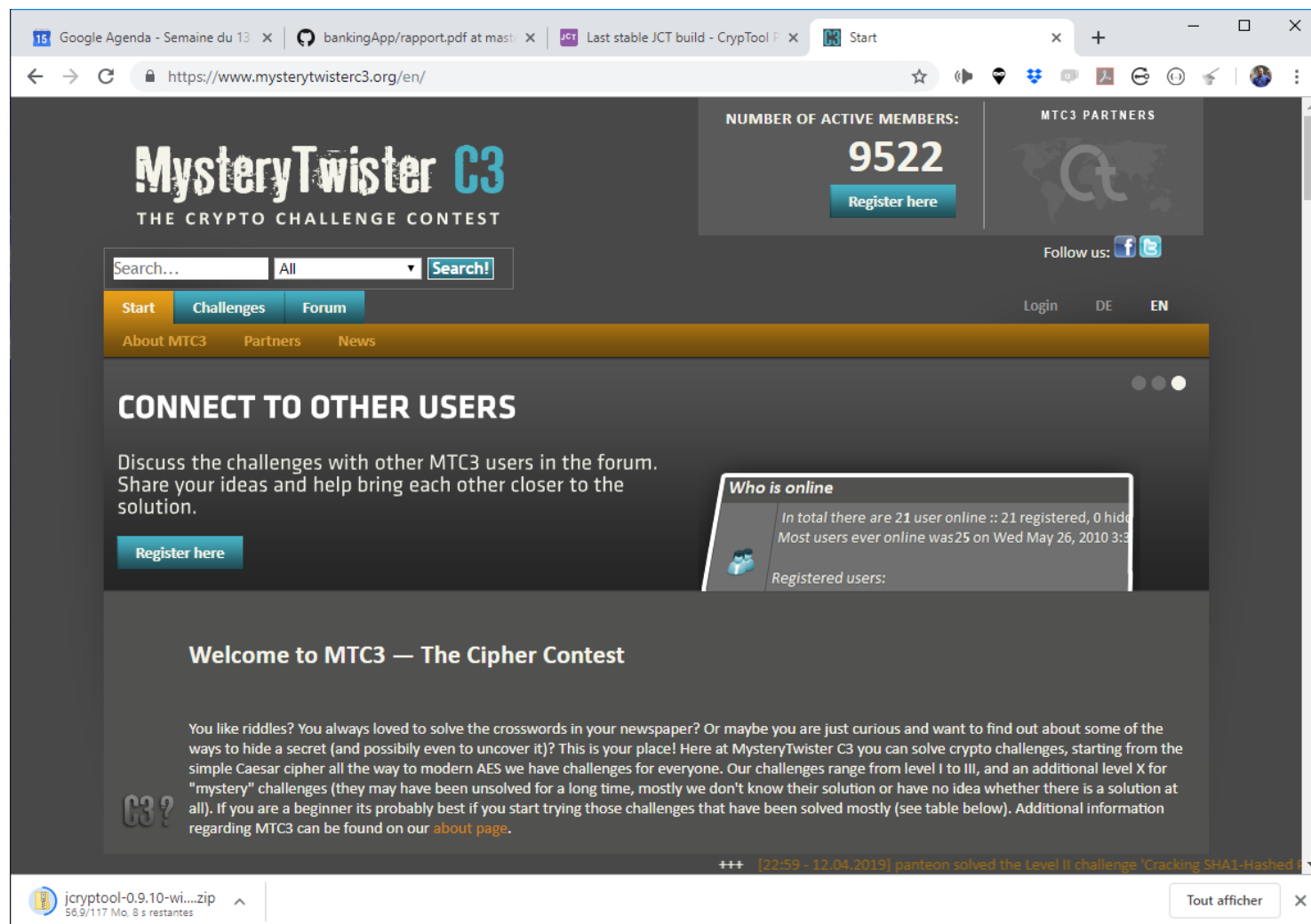
CRYPTOOL ONLINE

<https://www.cryptool.org/en/cryptool-online>



CIPHER CONTEXT

<https://www.mysterytwisterc3.org>



The screenshot shows the homepage of the MysteryTwister C3 website, which is a platform for crypto challenges. The browser's address bar displays the URL <https://www.mysterytwisterc3.org/en/>. The website features a dark theme with orange and blue accents. At the top, the logo "MysteryTwister C3" is prominently displayed, followed by the tagline "THE CRYPTO CHALLENGE CONTEST". A navigation bar includes links for "Start", "Challenges", "Forum", "About MTC3", "Partners", and "News". On the right side, a statistics box shows "NUMBER OF ACTIVE MEMBERS: 9522" with a "Register here" button. Below this, there are social media links for Facebook and Twitter, and language options for "Login", "DE", and "EN". A search bar is located in the center, with a dropdown menu set to "All" and a "Search!" button. The main content area is titled "CONNECT TO OTHER USERS" and encourages users to discuss challenges in the forum. It includes a "Register here" button and a "Who is online" section showing 21 users online (21 registered, 0 hidden) and a record of 25 users online on May 26, 2010. A welcome message for "MTC3 — The Cipher Contest" is also present, describing the site's purpose and the range of challenges from simple Caesar ciphers to modern AES. At the bottom, a status bar shows a file upload progress for "jcryptool-0.9.10-wi....zip" and a chat notification for "Tout afficher".

Challenge (1/2)

Your task is to decrypt the following ciphertext:

INDPMJNNDNLJTRRYFPOMDLFNCJDNLVTDBNQNCGKOOXINZMCAYRNB
MCDMLLYFNXBCKYRIKBMCADMLOMGNJMFNNKIJYDMLLYFYDNWKTOM
JXLRLVVTDCNLJTNFMBRMCNLJKENBNLLNINDMQNITBNUFKCYGDNK
HMCLRNJGYBACMINNPDJLNACMETNBUYGCTFBNARMPLNBDACMIKORC
MMFPBYQNFNCJDYJJLNBTVNBPPYOMDLNUFYUFNJLYICTNONRJBYFN
RLTCMRTONCMLRTFJLTJIOKYRGMCIDACMJJNDGYBNLJNCMAFTNCML
RTFTCJDKNHCMINJNBFCMNIIDMLINTJLDTDKMRMINJKUMJDTLUNNCI
NJYCJLTJNLJECYVCNRCNIMQNMDDOTRYCDMDJNCJLJMVTRRMINCJ
TOACMCYDMYPJLNDXNCYJDVBNTBPBYJNDJTCJLDMBMYOATANCJBXX
OMFTGGBYFLJYURYKCJXXBTBPPMJTCIXJCKYROYCAGYBINOMLVNJL
NOGONDBNLLTIJCNPDKFRLGYLNBIIYYLIOMLRMCXJCKYRROTBN

Author: George Theofanidis

MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

2 / 4

Challenge (2/2)

Instructions:

- ▶ The ciphertext was created with a mono-alphabetic substitution.
- ▶ The plaintext is written in English.
- ▶ The solution consists of the name and surname of the person described in the plaintext. Please enter the solution in capital letters with spaces between the words.
Example: If the person was Isaac Newton, you should enter ISAAC NEWTON as the solution.

Hint:

- ▶ The author of this challenge is an admirer of Nostradamus quotes / prophecies.