Cryptology for IoT

Modules M4, M6, M8
Session of 12th May, 2022.

M4.8 Briefing of the session
M4.9 Tasks to do in the lab
M4.10 Methodology using Cryptool (cont.)

Prof.: Guillermo Botella

Cryptology for IoT

Modules M4, M6, M8
Session of 12th May, 2022.

M4.8 Briefing of the session
M4.9 Tasks to do in the lab
M4.10 Methodology using Cryptool (cont.)

Prof.: Guillermo Botella

M4.6 Briefing of today

- Keeping going with Cryptography and Cryptoanalysis (Crypto lab v2)
  - Slides and supplementary videos
  - Deal with Unknown cipher
  - Friedman Test
  - Hill Climbing
- We go to the Socrative. First quiz.
  - Work in groups (Same than usual)

Cryptology for IoT

Modules M4, M6, M8
Session of 10th May, 2022.

M4.8 Briefing of the session
M4.9 Tasks to do in the lab
M4.10 Methodology using Cryptool (cont.)

Prof.: Guillermo Botella

Identifying the type of a cipher (see first M4.5)

- Not always possible without further knowledge about the cipher's origin and background
  - Voynich Manuscript – a book of the 15th century encrypted and written using an unknown alphabet
- To identify the type of the cipher we have seen to check out:
  - Frequency test component: visualizes the letter distribution of a given text
  - Friedman test component (kappa test)

Identifying the type of a cipher

- Used ciphertext is an encrypted letter sent in a bottle during the US Civil War
- The letter was sent from a commander (probably John Grimes Walker) to Confederate general John Pemberton
- Letter states that he cannot expect any reinforments
- Message is kept at the Museum of the Confederacy in Richmond and its content was unknown until 2010
- The message was then decrypted by a CIA code breaker

Identifying the type of a cipher

- Used ciphertext is an encrypted letter sent in a bottle during the US Civil War
- The letter was sent from a commander (probably John Grimes Walker) to Confederate general John Pemberton
- Letter states that he cannot expect any reinforments
- Message is kept at the Museum of the Confederacy in Richmond and its content was unknown until 2010
- The message was then decrypted by a CIA code breaker

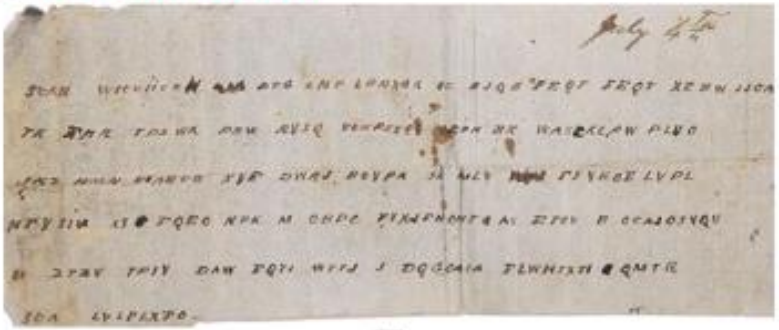
Encrypted message in a bottle

John Grimes Walker

John Pemberton

Identifying the type of a cipher

- Our cryptanalysis algorithms in CrypTool 2 work with text – not with pixels
- Thus, we have to create a transcription



Image

transcribe

SEAN WIEUIIUZH DTG CNP LBHXGK OZ BJQB FEQT XZBW
JJOY TK FHR TPZWK PVU RYSQ VOUPZXGG OEPH CK
UASFKIPW PLVO JIZ HMN NVAEUD XYF DURJ BOVPA SF
MLV FYYRDE LVPL MFYSIN XY FQEO NPK M OBPC
FYXJFHOHT AS ETOV B OCAJDSVQU M ZTZV TPHY DAU
FQTI UTTJ J DOGOAIA FLWHTXTI QLTR SEA LVLFLXFO.

Text

Identifying the type of a cipher

- Problem: We don't know the type of used cipher
- Analysis of the cipher type – some ideas:

We have digits:
- We have probably a homoph. subst cipher, a polyph. subst. cipher, or a monoalph. subst. cipher
- If there is separation (spaces) between digits, we assume these belong together and we can go on
- If there is no seperation between the digits, special further analysis is needed to divide the text into groups of digits that belong together ... this is not part of this video

We have Latin letters:
- We have probably a monoalph. subst. cipher, polyalph. subst. cipher, or a transpostion cipher

We have other symbols:
- If $count > 26$ we have probably a homophonic substitution cipher
- If $count \leq 26$ we have probably a monoalphabetic substitution cipher

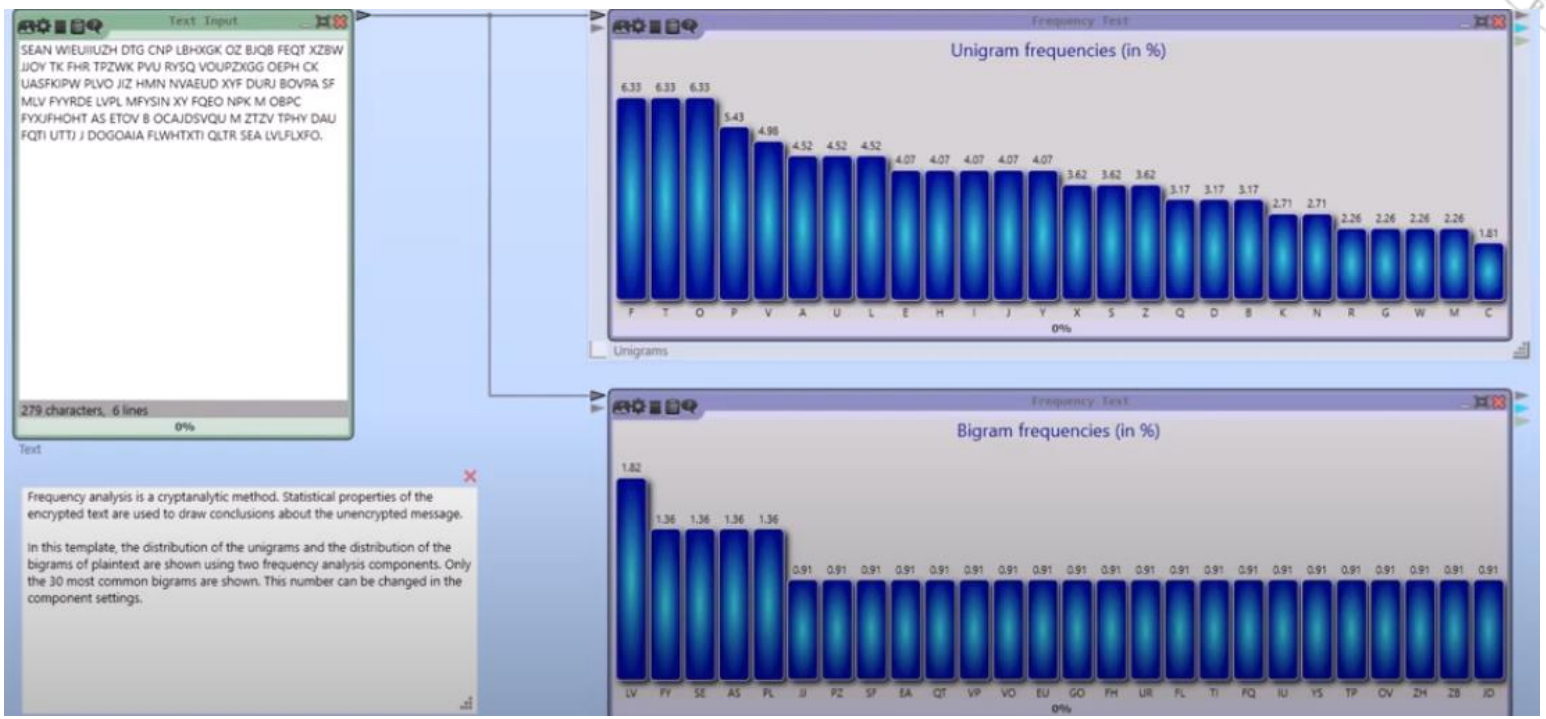
We perform further statistical analysis, i.e. frequency analysis e.g. on bigrams and compute the IoC

Identifying the type of a cipher

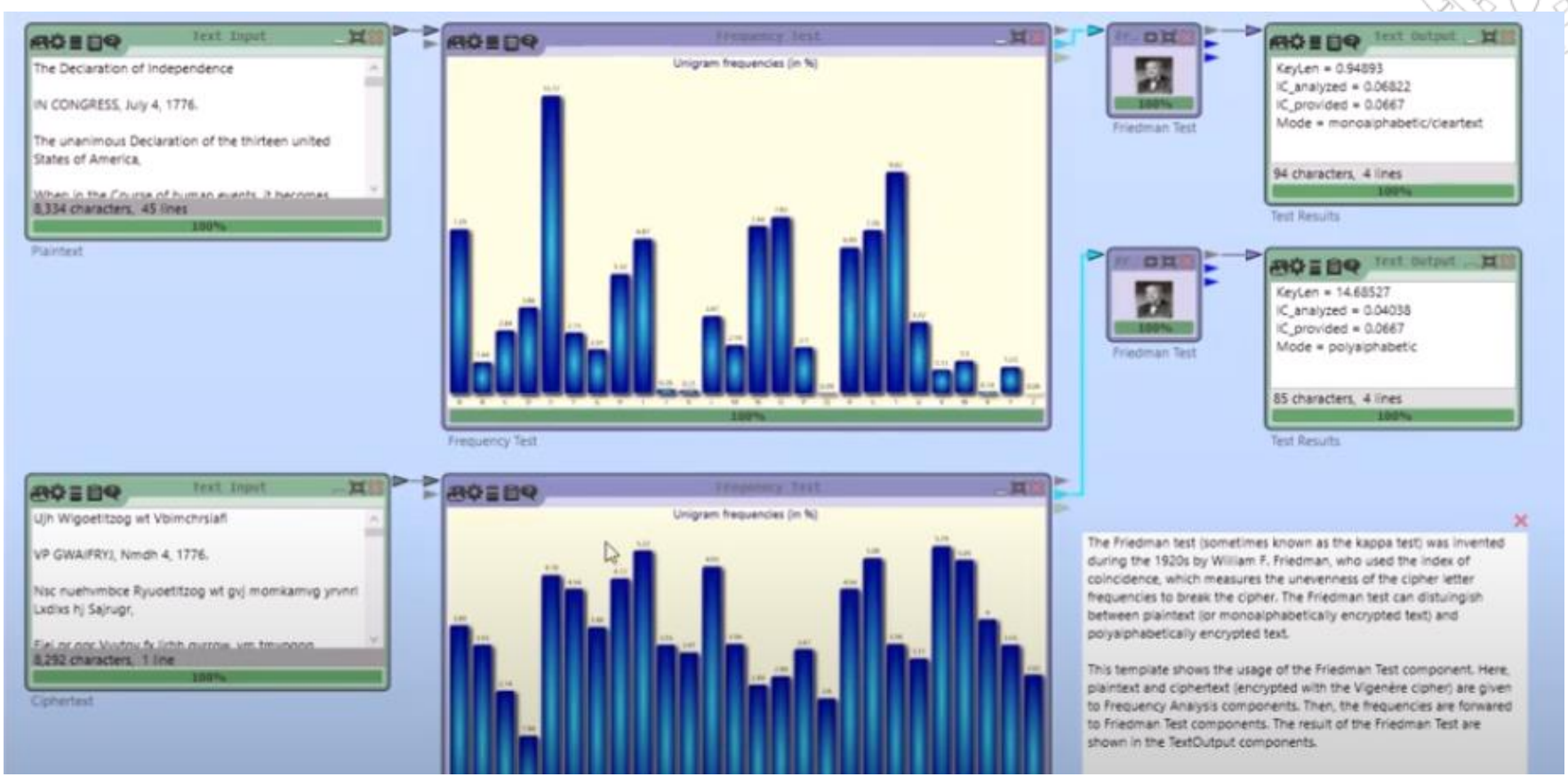
- Problem: We don't know the type of used cipher
- Analysis of the cipher type in our case:
  - We have Latin letters
  - We have at most 26 different letters => not homophonic
  - Probably not a transposition cipher since we see „words"
  - Frequency analysis, IoC, and the Friedman test should show us, if it is mono- or polyalphabetic
  - Lets have a look how to do all these analyses in CrypTool 2

```
SEAN WIEUIIUZH DTG CNP LBHXGK OZ BJQB FEQT XZBW
JJOY TK FHR TPZWK PVU RYSQ VOUPZXGG OEPH CK
UASFKIPW PLVO JIZ HMN NVAEUD XYF DURJ BOVPA SF
MLV FYYRDE LVPL MFYSIN XY FQEO NPK M OBPC
FYXJFHOHT AS ETOV B OCAJDSVQU M ZTZV TPHY DAU
FQTI UTTJ J DOGOAIA FLWHTXTI QLTR SEA LVLFLXFO.
```

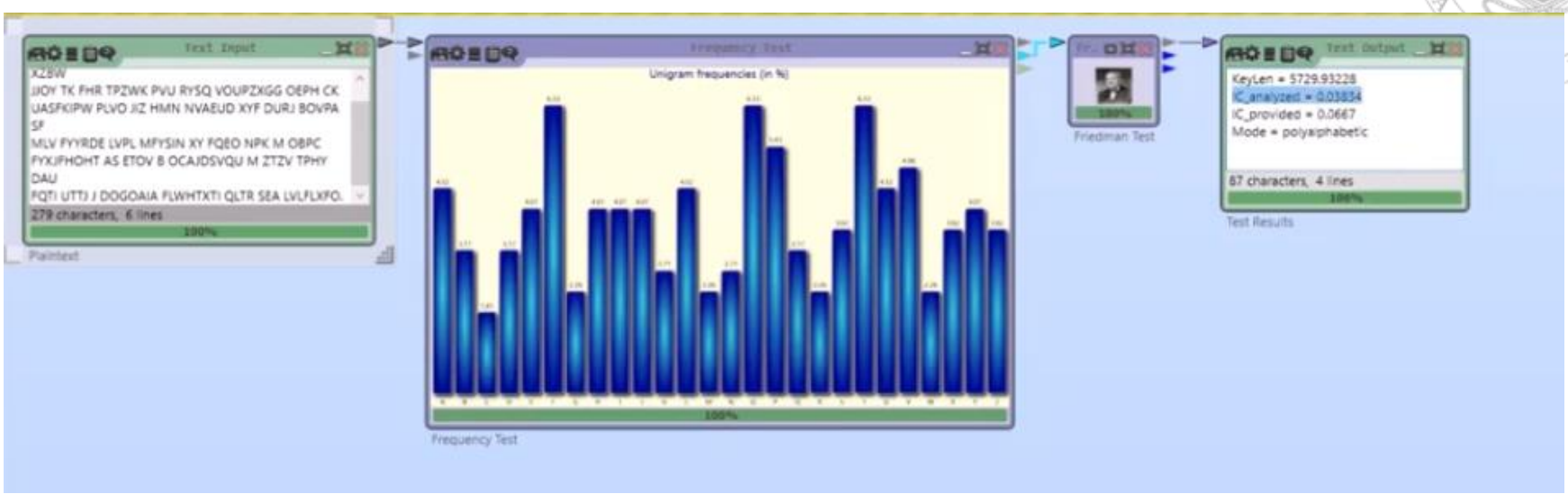
Identifying the type of a cipher



Identifying the type of a cipher



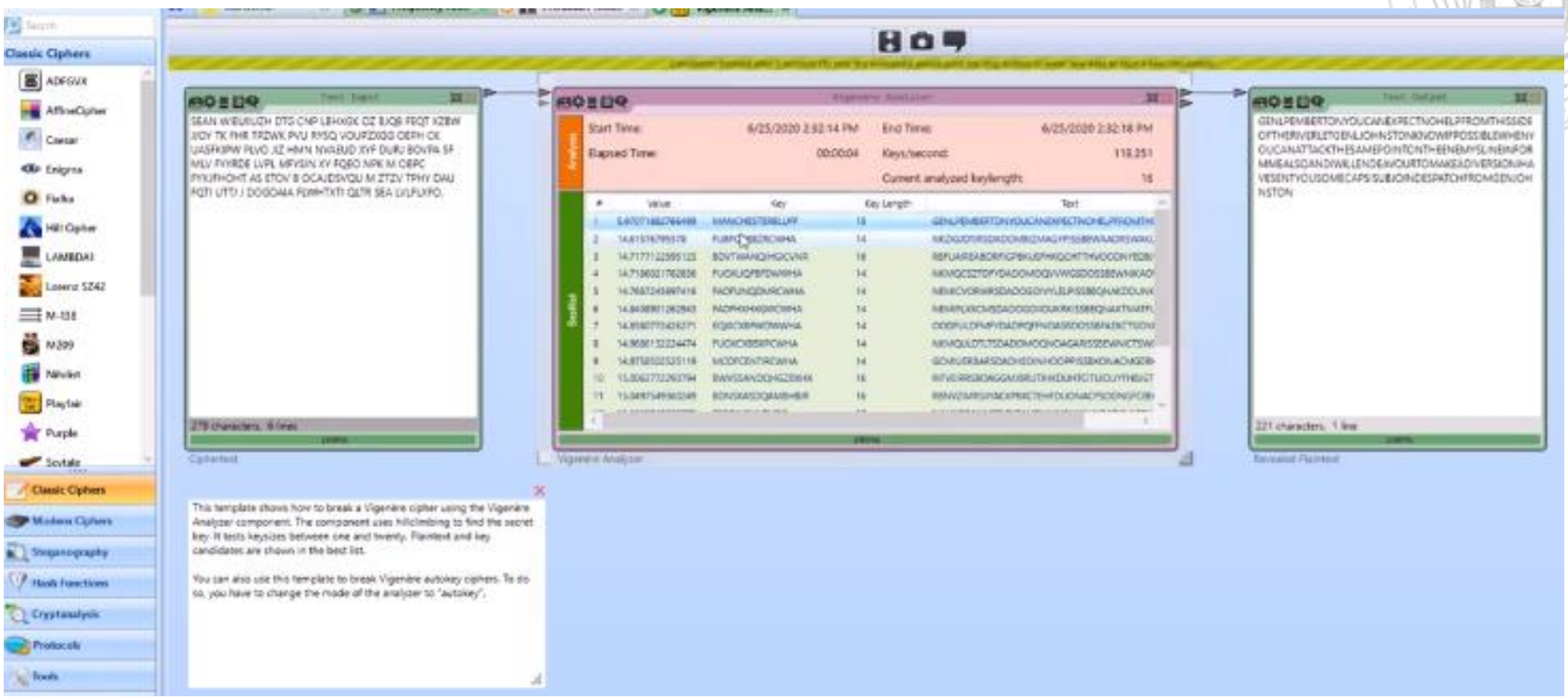
Identifying the type of a cipher



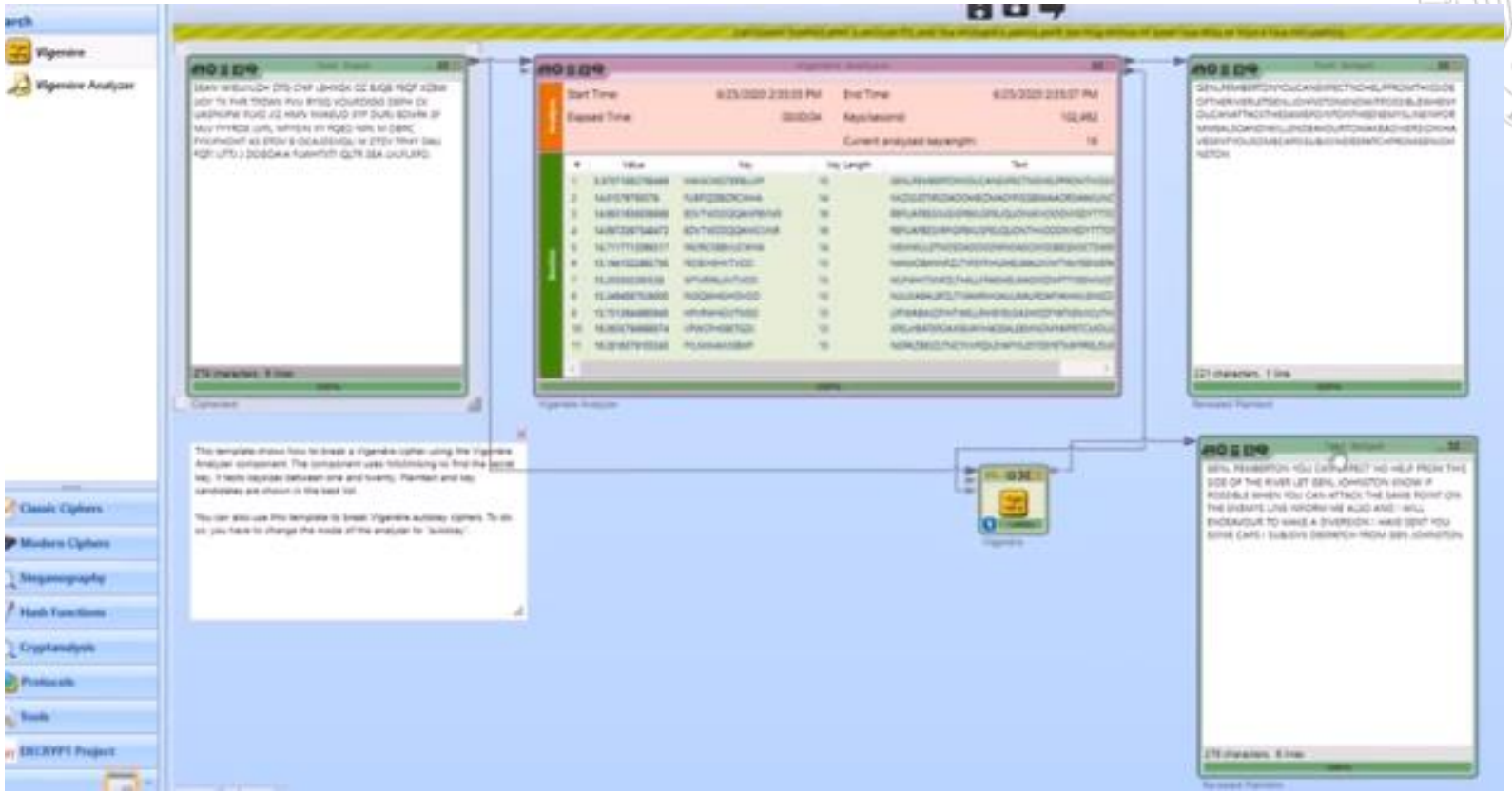
Identifying the type of a cipher

- We now know that the used cipher is polyalphabetic
- We know that the Vigenère cipher was used in US Civil war, thus, we should try this first
- It is known, that the Confederates only used the following three keys, all 15 letters long:
  - COMPLETEVICTORY
  - MANCHESTERBLUFF
  - COMERETRIBUTION
- Thus, lets try to break it with the Vigenère Analyzer in CrypTool 2

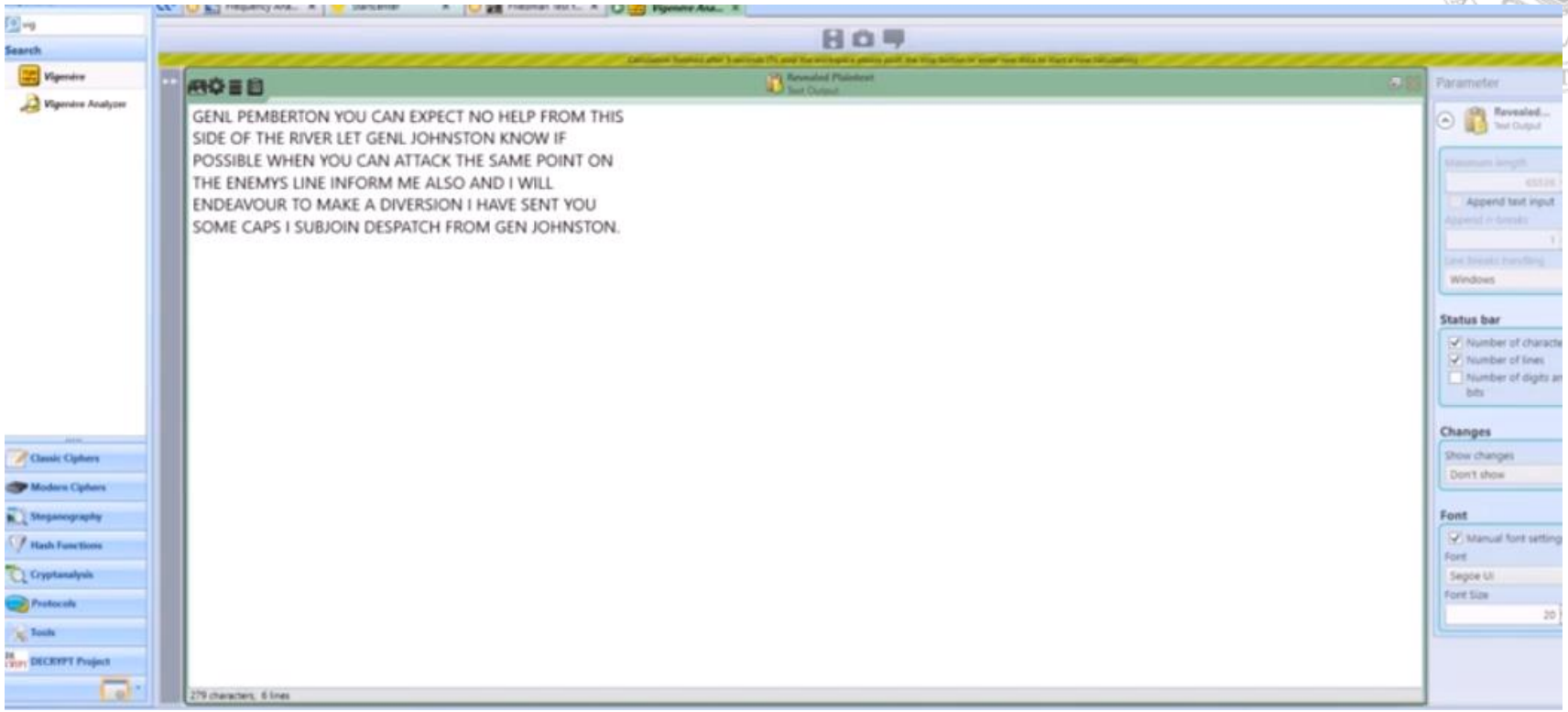
Identifying the type of a cipher



Identifying the type of a cipher



Identifying the type of a cipher



Cryptology for IoT

Modules M4, M6, M8
Session of 10th May, 2022.

M4.8 Briefing of the session
M4.9 Tasks to do in the lab
M4.10 Methodology using Cryptool (cont.)

Prof.: Guillermo Botella