



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

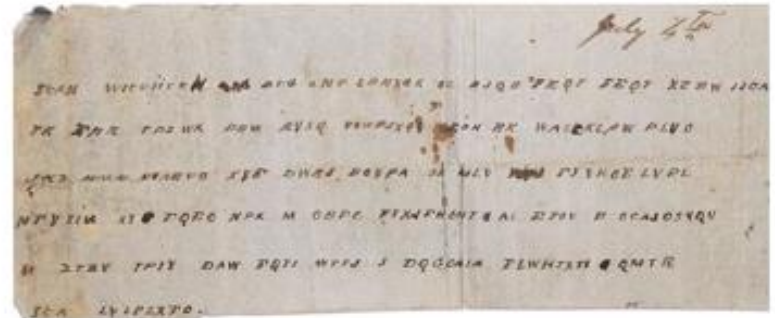


- Used ciphertext is an **encrypted letter** sent in **a bottle** during the **US Civil War**
- The letter was sent from a commander (probably **John Grimes Walker**) to Confederate general **John Pemberton**
- Letter states that he **cannot expect any reinforcements**
- Message is kept at the **Museum 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 reinforcements**
- 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

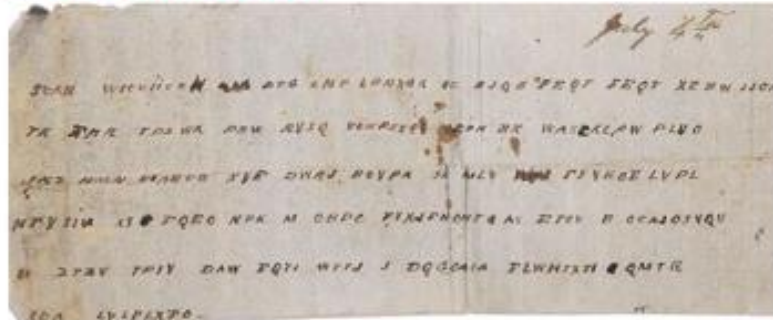


John Grimes Walker John Pemberton

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 separation 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 transposition cipher

We have **other symbols**:

- If *count* > 26 we have probably a homophonic substitution cipher
- If *count* ≤ 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

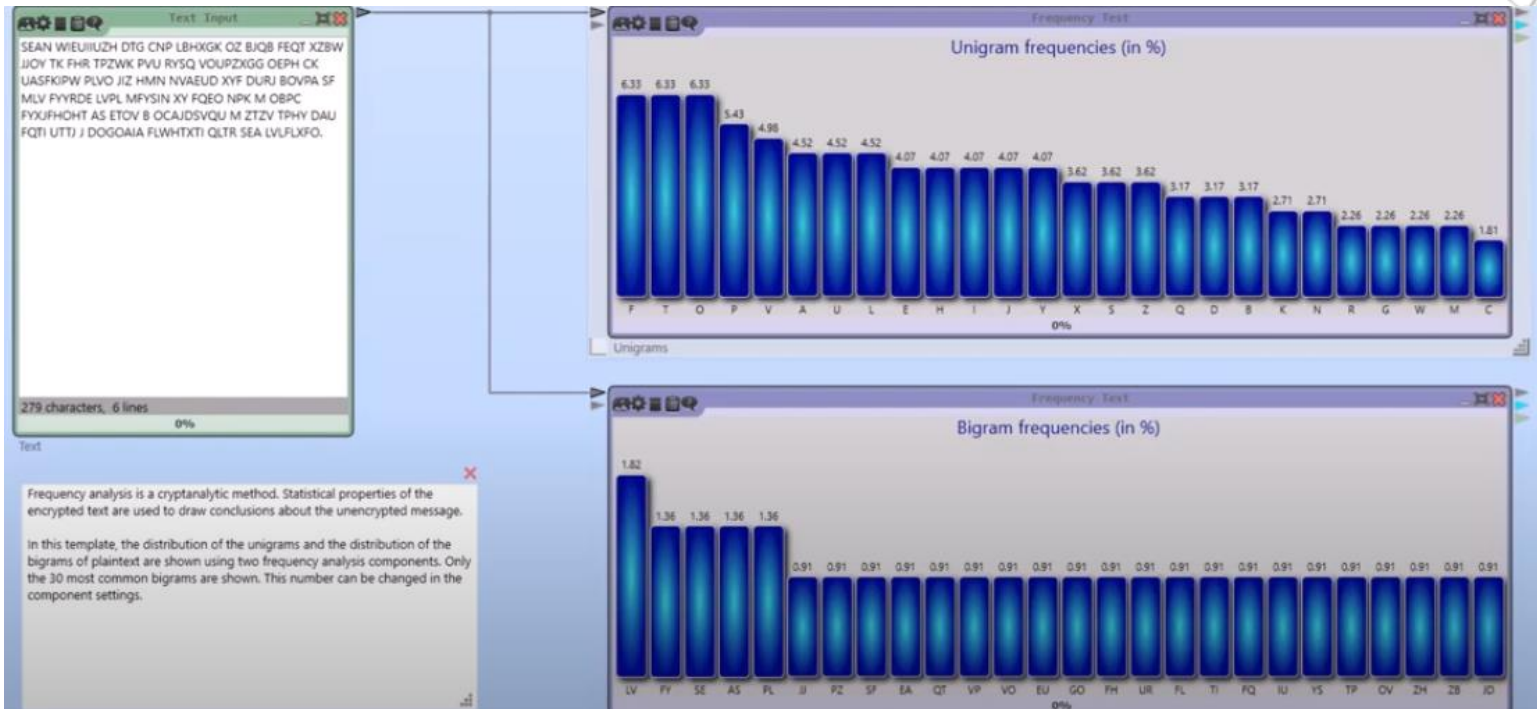
Identifying the type of a cipher



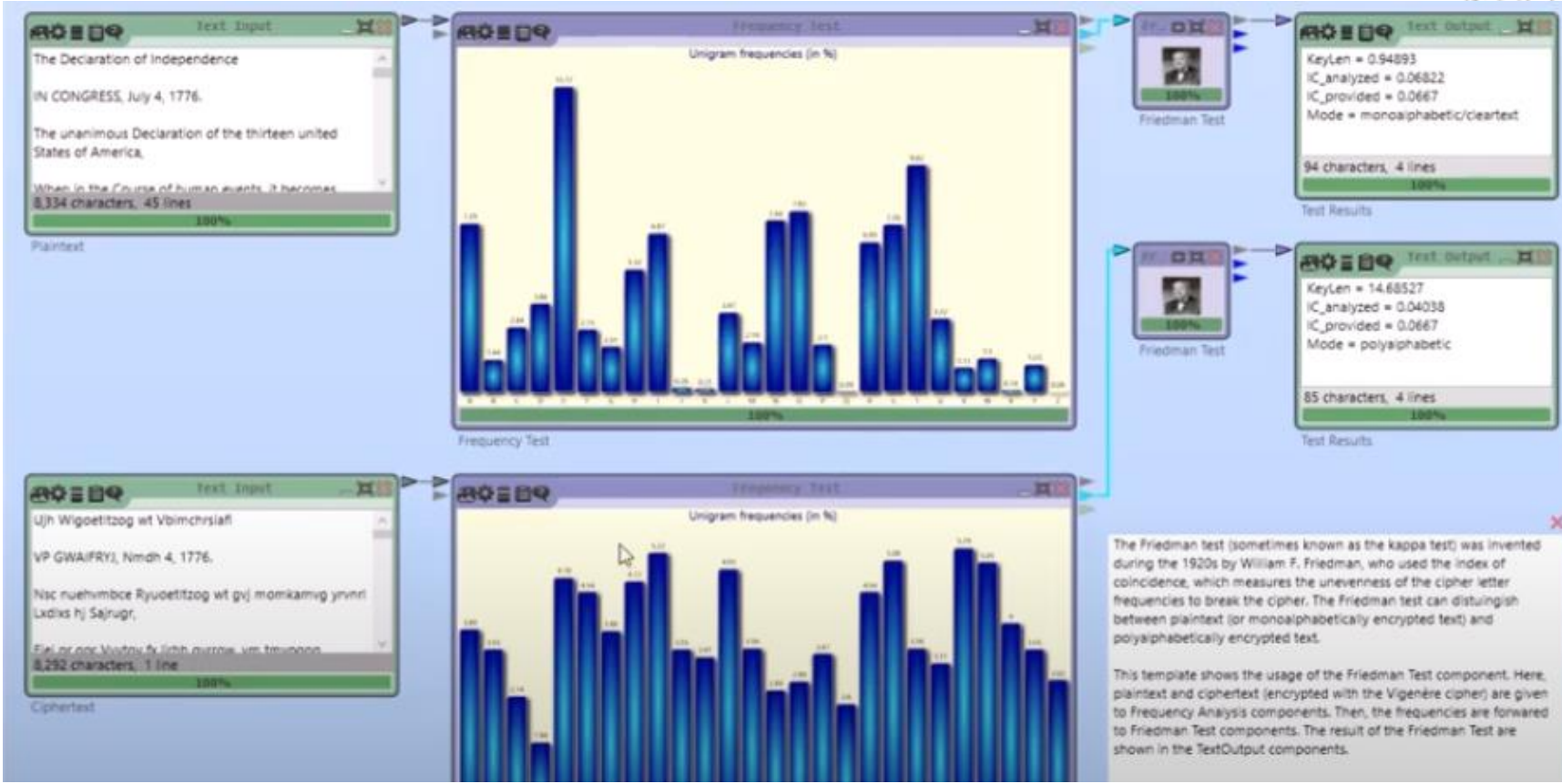
- Problem: We **don't know** the **type** of used **cipher**
- Analysis of the cipher type in our case:
 - We have **Latin letters**
 - We have **at most 26 different letters** => not homophonic
 - Probably not a transposition cipher since we **see „words“**
 - **Frequency analysis, IoC, and the Friedman 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.
```

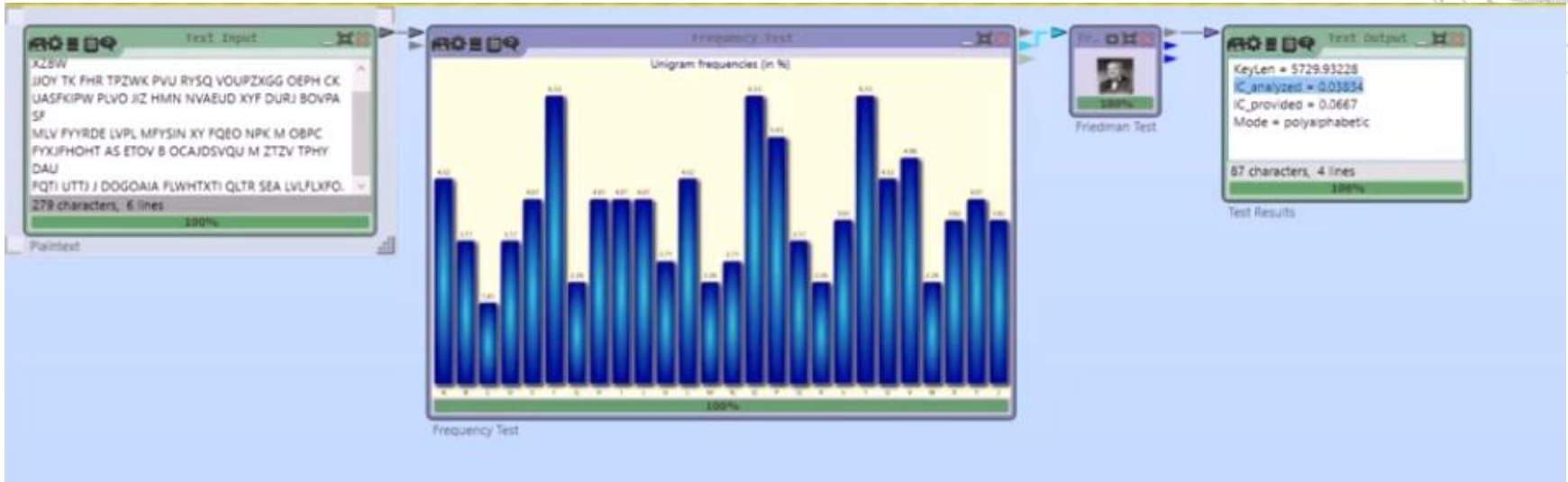
Identifying the type of a cipher



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

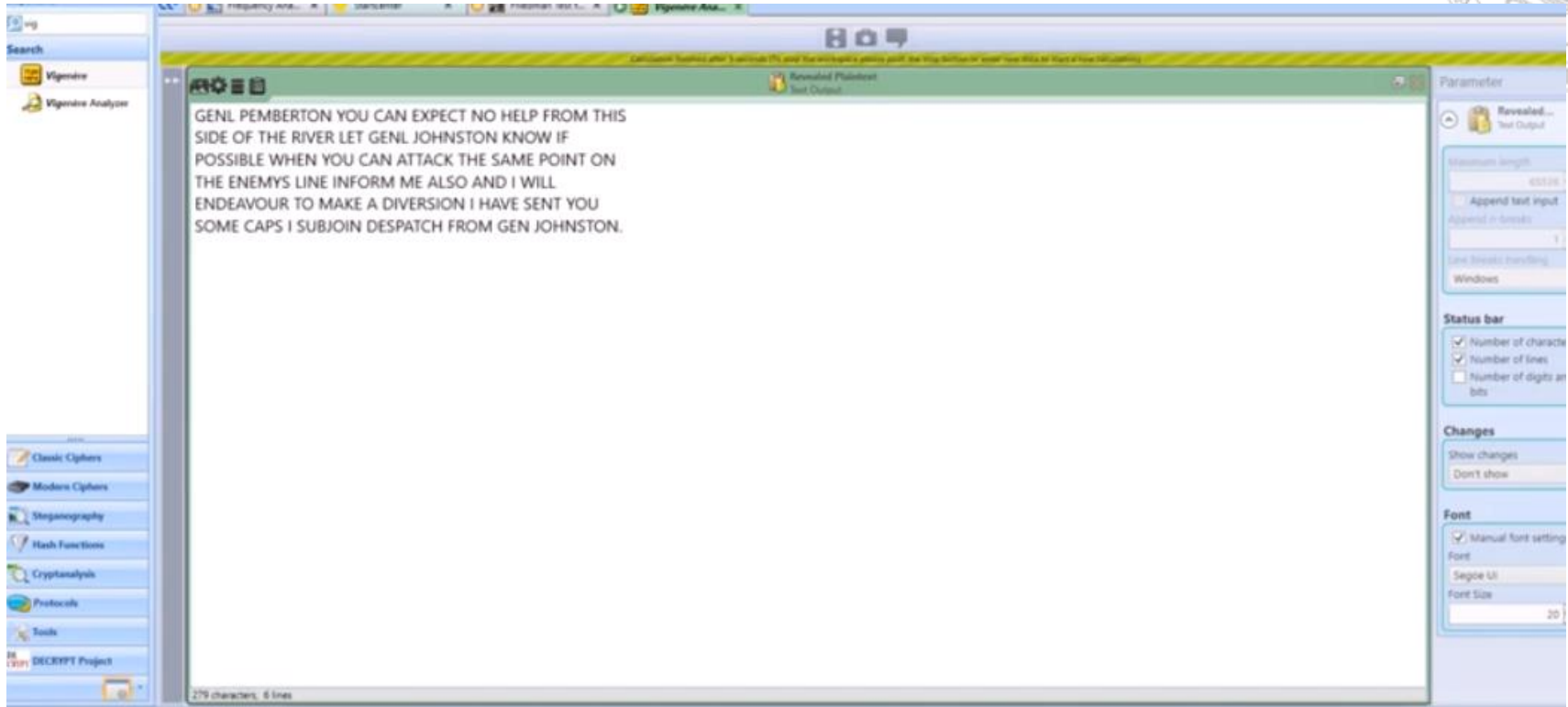
The screenshot shows a cryptanalysis application with three main panes:

- Classic Ciphers Sidebar:** Lists various cipher types including ADFGVX, Affine Cipher, Caesar, Enigma, Fiala, Hill Cipher, LAMBDA, Lorenz 5242, M-138, M-209, Navin, Playfair, Purple, and Sotat.
- Ciphertext Pane:** Contains the ciphertext: SEAN WREULGH DTS CND LEH00K GZ BJOS FQQT XZBW JVDY TK PHE TRZAK PVU RYSD YDUFZ000 DEPH CK UASR0RW RLVO JZ WHM IYARUD XYF DU0U B0VFA SF MLV RYRDE LUPJ KFYSN KY FQ00 NRE M O8PC PVLJH0HT AS ET0N 8 OCAUENY0U M ZTEV TRHY DAU FQTI UTTJ J D0S0MA F0M0YHTI QLTR SEA LULFUKO.
- Vigenere Analyzer Pane:** Shows analysis results for a Vigenere cipher.

#	Value	Key	Key Length	Text
1	540718676498	MMNCH278RLUP	18	GENLPEMBERTONVUCANREPECTNOHELFFROMTHISSIDE
2	1481516795178	FURH7627C0HA	14	NE0U0R0SD00H0M0M0G0YF0S0BPA0D0Y0W0
3	14717712295123	B0VFA0Q0H0G0CVNR	18	RE0UAR0B0R0P0B0U0P0K0CH0TH0V000N0Y0E0
4	147136021762836	F0U0L0Q0P0D0W0HA	14	NE0V0C0Z0P0D000M0Q0V0Q0D0S0B0W0K00
5	1473024389718	N0P0N0Q0N0C0W0A	14	NE0VC0R0R0S0D000S0Y0Y0L0P0S0B0C0M0Z0U0K
6	148438971262842	N0P0N0H0N0P0C0HA	14	NE0P0K0C0M0S0D000S0D0K0K0S0B0Q0W0T0M0Y0
7	148580770428271	E0B0C0M0N0W004	14	000P0L0P0Y0S0L0R0P0Y0D0S0R000S0F0L0T0U0N
8	14868132234474	F0U0K0B0P0C0HA	14	NE0V0L0T0T0D0D0H0G0C0G0R0S0D0W0N0C0T0W
9	148782522325118	M0C0C0N0T0R0C0HA	14	S0U0L0R0S0R0S0D0H0D0N000P0S0B0X0L0M0Z0B
10	153062773263794	B0W0S0A0D0H0Z0B0W	18	RE0V0R0S0G0G0M0R0L0H0D0H0C0T0U0L0Y0H0C0T
11	153482499302849	B0W0S0A0D0Q0M0B0H0R	18	RE0W0S0R0S0M0C0R0N0C0H0L0U0M0R0S0D0N0Y0R0B
- Revealed Plaintext Pane:** Shows the decrypted text: GENLPEMBERTONVUCANREPECTNOHELFFROMTHISSIDE CITHERVIRLET0ENLICHN0TONK0W0H0P0S0B0LE0H0N0Y0 DUCANAT0ACT0H0ES0M0P0D0H0C0N0H0B0N0P0S0L0R0P0R0M0 M0E0L0S0A0N0D0W0L0E0D0E0P0L0R0T0M0A0K0S0N0E0R0D0N0H0 VESENTV0S0M0E0C0P0S0UB0N0C0E0S0P0C0H0R0M0A0S0E0U0H0 N0ST0N

Below the panes, a note explains: "This template shows how to break a Vigenere cipher using the Vigenere Analyzer component. The component uses hillclimbing to find the secret key. It tests keystates between one and twenty. Plaintext and key candidates are shown in the best list. You can also use this template to break Vigenere autokey ciphers. To do so, you have to change the mode of the analyzer to 'autokey'."

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