



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)



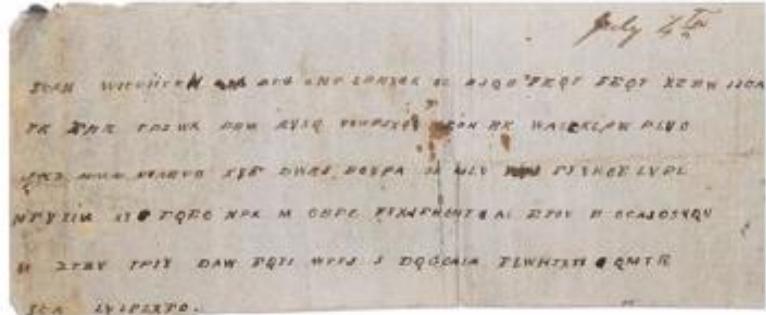
Identifying the type of a cipher

- 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**

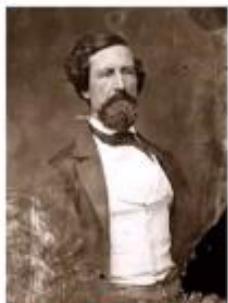


Identifying the type of a cipher

- 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

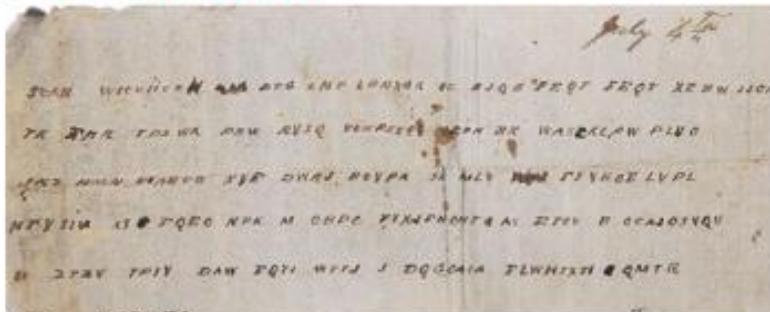


John Grimes Walker John Pemberton



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 WIEUIUZH DTG CNP LBHXGK OZ BJQB FEQT XZBW
JJOY TK FHR TPZWK PVU RYSQ VOUPZXGG OEPH CK
UASF KIPW PLVO JIZ HMN NVAEUD XYF DURJ BOVPA SF
MLV FYYRDE LVPL MFYSIN XY FQE NPK M OBPC
FYXJFH HT AS ETOV B OC AJDSVQU 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 transposition 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

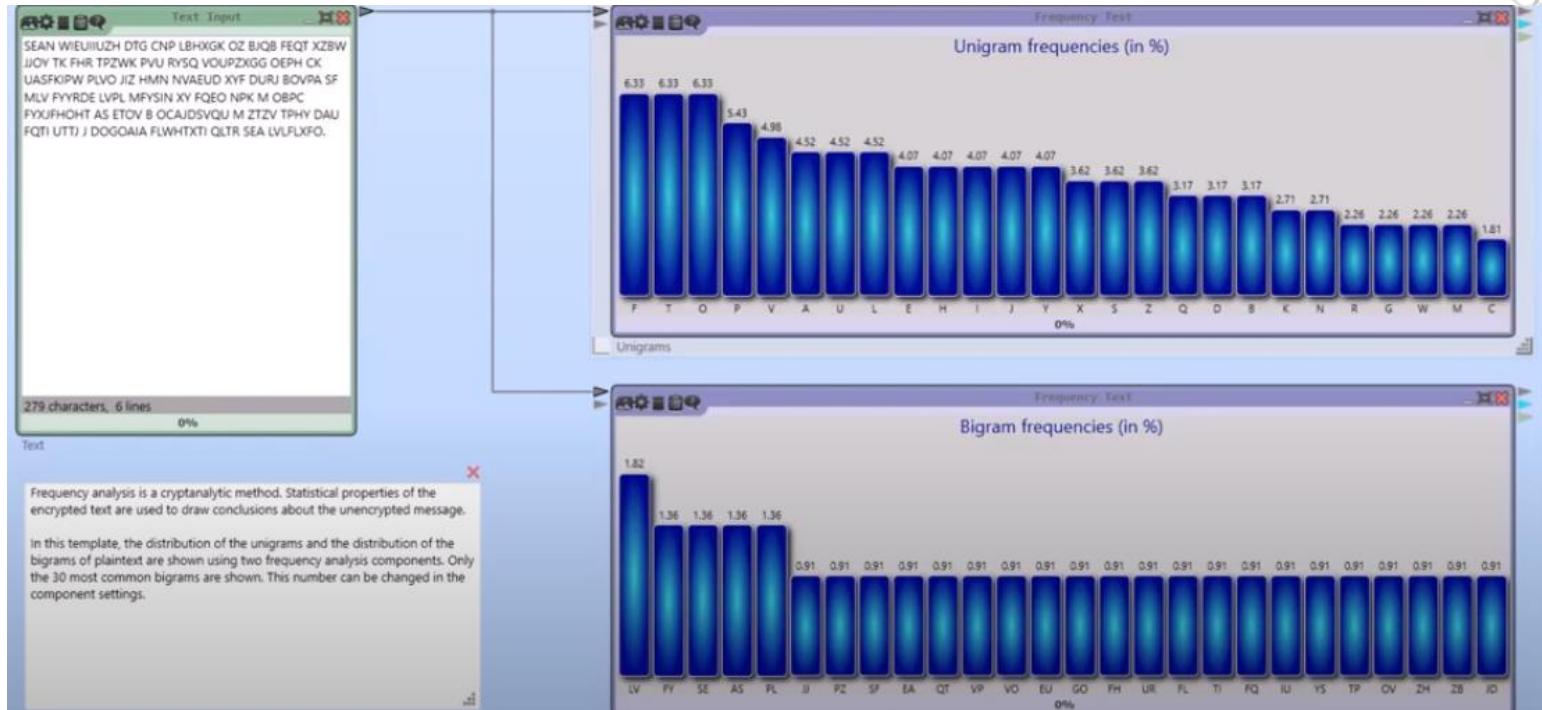


Identifying the type of a cipher

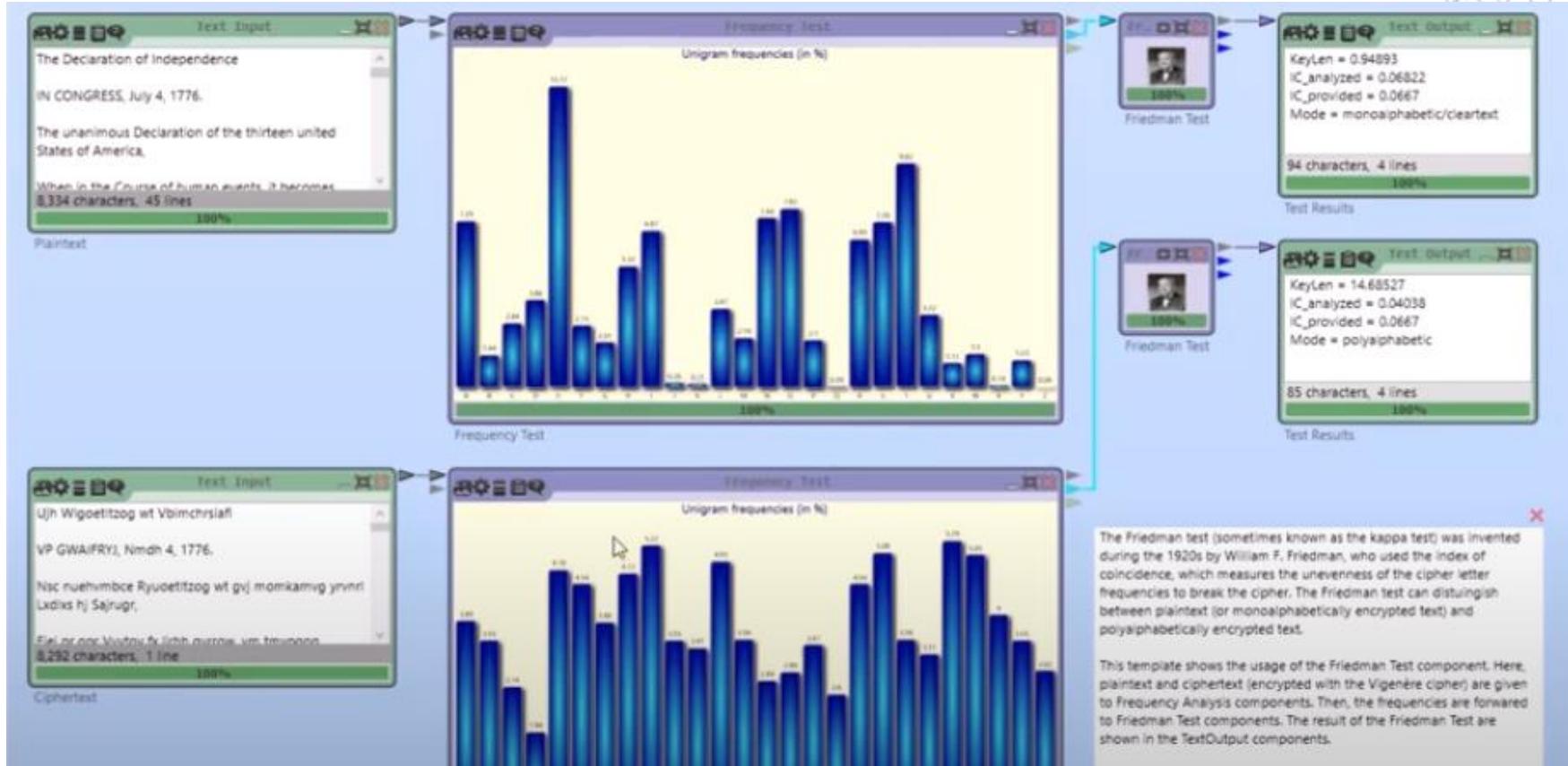
- Problem: We **don't know** the **type** of used **cipher**
- Analysis of the cipher type in our case:
 - We have **Latin letters**
 - We have **at most 26 different letters** => not homophonic
 - Probably not a transposition cipher since we **see „words“**
 - Frequency analysis, IoC, and the Friedman 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 FQEONPK M OBPC
FYXJFHHT AS ETOV B OCAJDSVQU M ZTZV TPHY DAU
FQTI UTTJ J DOGOAIA FLWHTXTI QLTR SEA LVLFLXFO.

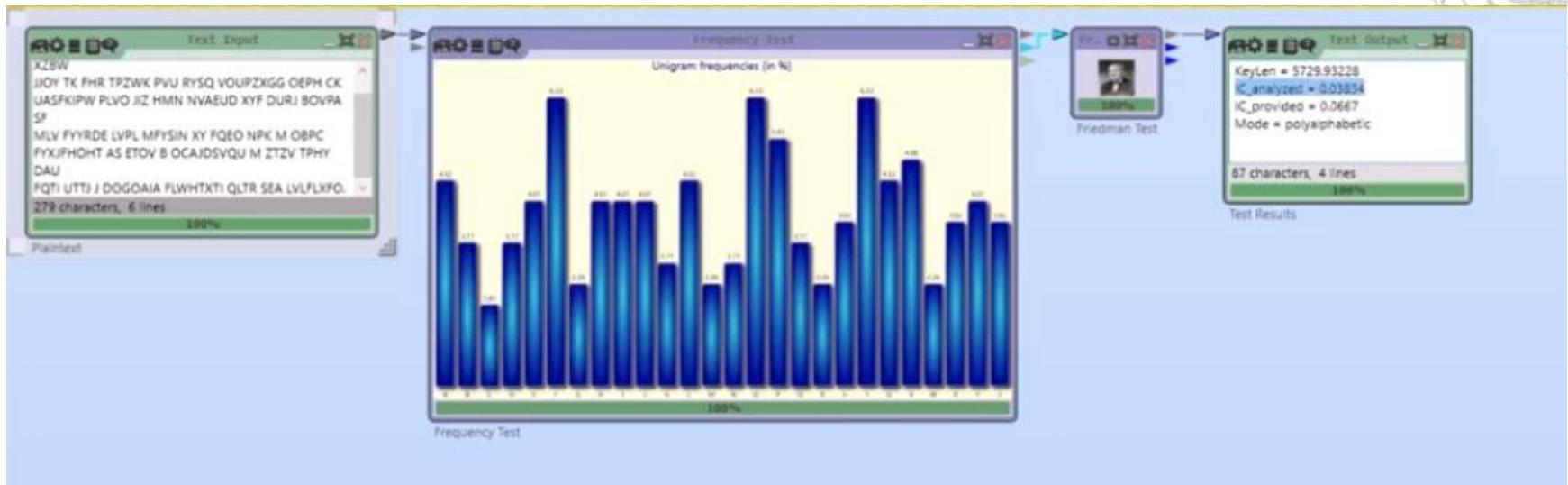
Identifying the type of a cipher



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



Screenshot of a software interface for cryptanalysis, specifically for identifying the type of a cipher.

The interface includes a sidebar with categories like "Classic Ciphers" (ADFGVX, Affine Cipher, Caesar, Enigma, Fernet, Hill Cipher, LAMEIDA, Laserz SZ42, M-128, M-399, Minhut, Playfair, Purple, Scytale), "Modern Ciphers" (AES, Blowfish, ChaCha20, DES, DES3, ElGamal, GOST, IDEA, MD5, SHA-1, SHA-256, SHA-512, Twofish), "Steganography", "Hash Functions", "Cryptanalysis", "Protocols", and "Tools".

The main window shows three panels:

- Text Input:** Displays the encrypted text: "SEAN WIEBUCH DT2 CMP UHAKK CZ SJQR FRQT XZEW JVOY TK FH TRZWK PNU PMSQ YOULZODD CERYCZ UASHOPW PLVZ JZ MMN NWBUD XYF DUUZ BOVFA SF MLYV FVYRDE LVPL MVSUN XY FOBO NRE M CERC JYUHTHOHT AS ETON S DCAZDYOU MU ZTIV TRIV DAU AGT UTUJ DDOGAA PWPHXTD QLTH SEA UJUUXO".
- Vigenere Analyzer:** A table showing results of the Vigenere analysis. The table has columns: #, Value, Key, Key Length, and Text. The data is as follows:

#	Value	Key	Key Length	Text
1	5400716827454199	MMNOHTEBLLHF	18	GENPEMBERTONYQUCHNZDJECTNQHLPYTHONHE
2	1481516795178	FUMPQZKTCMHA	14	NKQZQOTRISADMDBZMAGPF55BPAACDRWAKU
3	147177122595123	BQVTHWQHOCVNR	18	REPUAERABDRIGPKUWPKWQGHTHVOOCNTEDB
4	147136001702836	FUCALQJPPSWRKA	14	MQCZTDYDADOMQVWQZD09388WIKAOI
5	142603243867116	NAEYUNQDQHCRWA	14	NEICVORURSDAOGGQVILPSSB60AMZDOLWK
6	148488911262941	PAZPHXH495070945	14	MEHUVUCMUSADOGGQDQJUQH58RQH4UHTWTF
7	148488770403271	E98C089767WAWHA	14	ODOFJLQHNP742DGFPHMAGDOSMNLHETTSQW
8	14858813234474	FUCRQBSRPTCPHA	14	ABQMOULDLT25ADOMAOHCA4R522ZVWNCCTSW
9	150027732262794	MCORCONTRWMA	14	GOMURBARSDADEDINHOOPRSSBXDVAQACB
10	1504027732262794	BAVSGANQDAG22064K	16	W7VERREBQAGMGRUITHKDUHFTQUDLYTHBGT
11	15349754936324	BDVSKM503QAHSHBR	16	BBMAMVRSNACCEPTEHDLQHACPSQDNQVQH
- Text Output:** Displays the decrypted text: "GENPEMBERTONYQUCHNZDJECTNQHLPYTHONHE CIPHERSVERLETENJOHNSTONKOMPOSSIBLEWHENY CUGANATTACKTHEAMEROINTENTHENEMYSNEMPOR MMEALSDANDWILENSEACURTOOMAGSAVERSOMHA VESENTYUSOMICAPSUBORDIDESPATCHFROMZENHVN STON".

A tooltip provides information about the Vigenere Analyzer component:

This template shows how to break a Vigenère cipher using the Vigenère Analyzer component. The component uses hillclimbing to find the secret key. It tests keysizes between one and twenty. Plain text and key candidates are shown in the best list.

You can also use this template to break Vigenère autokey ciphers. To do so, you have to change the mode of the analyzer to "autokey".

Identifying the type of a cipher



Module 4: Cryptology for IoT

This template allows you to break a Vigenère cipher using the Vigenère Analyzer component. The component uses hillclimbing to find the secret key. It finds keysize between one and twenty. Plaintext and key hypotheses are shown in the last tab.

You can also use this template to break Vigenère auxiliary ciphers. To do so, you have to change the mode of the analyzer to "auxiliary".

#	Value	Name	Key Length	Text
1	3.27076578449	WIKICONTES	10	DEINHEITENHABEUNGSSTUDIEN
2	5.457576076	WIKIDEBORNA	10	HACDZKRSQKONQADOTPSBAMNHC
3	14.88518163888	WIKIHDZKRS	10	RELAESLUSGMLGJLJUHNDYTTG
4	14.882297548472	WIKIHDZKRSQ	10	RELAESLUSGMLGJLJUHNDYTTG
5	14.711711388317	WIKICRASHED	10	HEHEPDUOEVHJFVHJFVHJFVHJF
6	12.9473228676	WIKIDHCRASH	10	HEHEPDUOEVHJFVHJFVHJFVHJF
7	12.9355838538	WIKIDHCRASH	10	HEHEPDUOEVHJFVHJFVHJFVHJF
8	12.88486763000	WIKIDHCRASH	10	HEHEPDUOEVHJFVHJFVHJFVHJF
9	12.75184688646	WIKIDHCRASH	10	HEHEPDUOEVHJFVHJFVHJFVHJF
10	12.6857658374	WIKIDHCRASH	10	HEHEPDUOEVHJFVHJFVHJFVHJF
11	12.6197765336	WIKIDHCRASH	10	HEHEPDUOEVHJFVHJFVHJFVHJF

Current analyzed keylength: 10

274 characters, 8 lines

Vigenère Analyzer

221 characters, 1 line

Vigenère Analyzer

270 characters, 8 lines

Vigenère Analyzer

Identifying the type of a cipher



The screenshot shows a software interface for cryptanalysis. On the left, a sidebar lists various categories: Search, Vigenère, Vigenère Analyzer, Classic Ciphers, Modern Ciphers, Steganography, Hash Functions, Cryptanalysis, Protocols, Tools, and DECRYPT Project. The main window displays a decrypted message:

GENL PEMBERTON YOU CAN EXPECT NO HELP FROM THIS
SIDE OF THE RIVER LET GENL JOHNSTON KNOW IF
POSSIBLE WHEN YOU CAN ATTACK THE SAME POINT ON
THE ENEMYS LINE INFORM ME ALSO AND I WILL
ENDEAVOUR TO MAKE A DIVERSION I HAVE SENT YOU
SOME CAPS I SUBJOIN DESPATCH FROM GEN JOHNSTON.

Below the message, status information reads "279 characters, 6 lines". The right side of the interface contains several panels: Parameter, Status bar, and Changes, each with various configuration options and checkboxes.



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