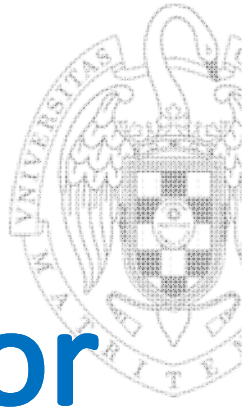
T4. Assignments & Tasks for M4

Assignments and tasks for Module M4

T4. Introduction to the assignments and tasks
T4.1 Assignments and Tasks using Cryptool CT2
T4.2 Challenges using Cryptool CT2
T4.3 Quizzes using Socrative

Prof.: Guillermo Botella



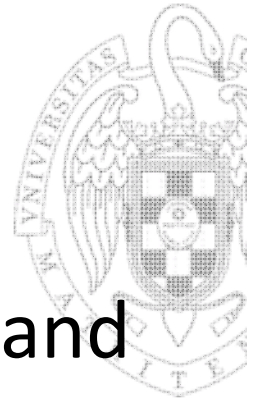
T4. Assignments & Tasks for M4

Assignments and tasks for Module M4

T4. Introduction to the assignments and tasks
T4.1 Assignments and Tasks using Cryptool CT2
T4.2 Challenges using Cryptool CT2
T4.3 Quizzes using Socrative

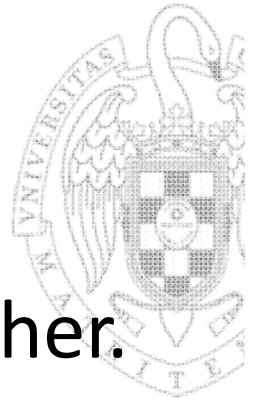
Prof.: Guillermo Botella

T4. Revision of basic concepts: Basics of cryptology



- **Cryptology:** science of cryptography and cryptanalysis
- **Cryptography:** secret writing based on secret keys and cryptographic algorithms
- **Cryptanalysis:** recover the secret texts without the secret keys
- **Cipher:** cryptographic algorithm used for encryption and decryption.
  - Encryption: ciphertext = cipher(plaintext, key)
  - Decryption: plaintext = cipher(ciphertext , key)

T4. Revision of basic concepts: Basics of cryptology



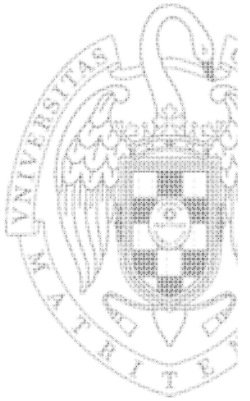
- **Keyspace:** set of all possible keys of a cipher. In classical ciphers, the key for encryption and decryption is the same.
- **Alphabet:** The used letters or symbols of plaintext and ciphertext, having a plaintext alphabet and a ciphertext alphabet (that could be the same).
- **Break a ciphertext:** reveal the plaintext without the used key. Depending of the alphabet, brute force vs heuristics

T4. Revision of basic concepts: Basics of cryptology

The Caesar Cipher

- How it works: Shift letters according to a key (shift value)
- Example:
  - Key: 1 (i.e. shift alphabet by 1)
  - Plaintext alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Ciphertext alphabet: BCDEFGHIJKLMNOPQRSTUVWXYZA
  - Plaintext: HELLOWORLD
  - Ciphertext: IFMMPXPSME

T4. Revision of basic concepts: Basics of cryptology



Attacks on ciphers

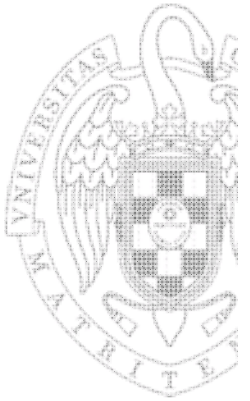
- **Attack to the ciphertext:** The cryptanalyst only has the ciphertext. Reveal the plaintext and/or the secret key.
- **Attack to the plaintext:** The cryptanalyst has the plaintext (parts or entire) and the ciphertext. Reveal the key.

T4. Revision of basic concepts: Basics of cryptology

Statistics

- Based on language models and text statistics, classical ciphers can be broken.
- For instance, the letter frequency can be used to identify which letter in the plaintext is replaced by which letter in the ciphertext.

T4. Revision of basic concepts: Basics of cryptology



Substitution ciphers

- Replace letters of the plaintext with other letters (numbers, letters, symbols, etc.).
  - Monoalphabetic subst. cipher: a plaintext letter is always replaced with the same ciphertext letter.
  - Homophonic subst. cipher: a plaintext letter is replaced with more than one ciphertext letter.
  - Polyalphabetic subst. cipher: different ciphertext alphabets

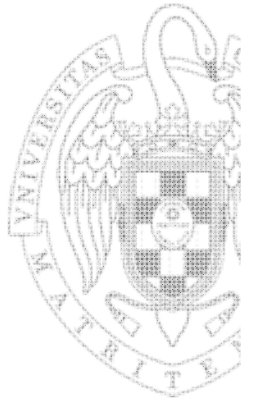
Cipher type	Number of plaintext symbols	Number of ciphertext symbols
Monoalphabetic substitution	26	26
Homophonic substitution	26	>26
Polyalphabetic substitution	26	26; different alphabets

T4. Revision of basic concepts: Basics of cryptology

Substitution ciphers. Examples

- Monoalphabetic Substitution: The Caesar Cipher
  - Plaintext alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Key: 1 (i.e. shift alphabet by 1)
  - Ciphertext alphabet: BCDEFGHIJKLMNOPQRSTUVWXYZA
  - Plaintext: HELLOWORLD
  - Ciphertext: IFMMPXPSME

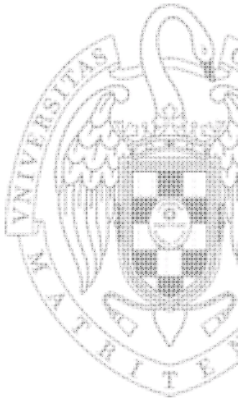
T4. Revision of basic concepts: Basics of cryptology



Substitution ciphers. Examples

- Homophone Substitution
  - A plaintext letter is replaced with two-digit numbers
  - Plaintext alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Key: A = {01 or 02 or 06}, B = {03 or 04}, C = {05}, ...
  - Plaintext: HELLOWORLDHOWAREYOU
  - Ciphertext: 15,09,23,24,29,45,30,35,23,07,16,29,46,01,36,10,49, 30,41

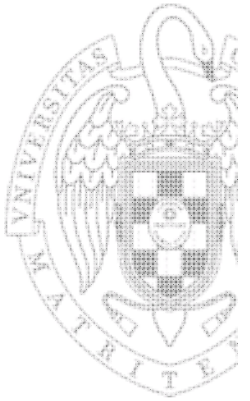
T4. Revision of basic concepts: Basics of cryptology



Substitution ciphers. Examples

- Polyalphabetic Substitution: The Vigenère Cipher
  - The Vigenère cipher uses different shifted ciphertext alphabets based on a keyword
  - Plaintext alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Ciphertext alphabets: 26 different shifted alphabets
    - ABCDEFGHIJKLMNOPQRSTUVWXYZ
    - BCDEFGHIJKLMNOPQRSTUVWXYZA
    - CDEFGHIJKLMNOPQRSTUVWXYZAB
    - DEFGHIJKLMNOPQRSTUVWXYZABC
    - EFGHIJKLMNOPQRSTUVWXYZABCD
    - …
  - Key: SECRET
  - Plaintext: HELLOWORLDHOWAREYOU
  - Ciphertext: ZINCSPGVNULHOETVCHM

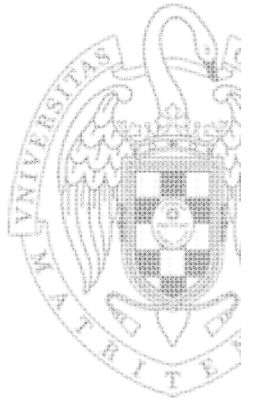
T4. Revision of basic concepts: Basics of cryptology



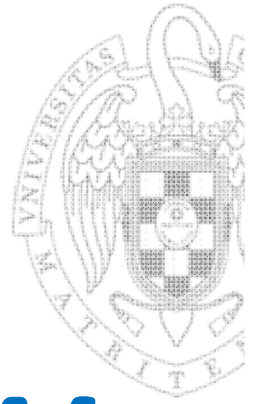
Transposition Ciphers

- Do not replace letters with other. Instead, the position is changed.
- Example: The Columnar Transposition Cipher
  - Plaintext copied into a rectangular grid with n-columns. Then, columns are permuted using a keyword.
  - Plaintext alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Ciphertext alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
  - Key: SECRET
  - Plaintext: HELLOWORLDHOWAREYOU
  - Ciphertext: LLRERAOHYLDEHOWUWOO

T4. Revision of basic concepts: Cryptool



- See tutorial of the first day (slides)
  - Startcenter
  - Wizard
  - Workspace Manager
  - Online Help



Assignments & Tasks for M4

Assignments and tasks for Module M4

T4. Introduction to the assignments and tasks
T4.1 Assignments and Tasks using Cryptool CT2
T4.2 Challenges using Cryptool CT2
T4.3 Quizzes using Socrative

Prof.: Guillermo Botella

Assignments

- Symmetric Cryptography
  - Classic Cipher (Caesar)
  - Monoalphabetic Substitution Cipher
  - Polyalphabetic Cipher - Vigenère Cipher
  - Homophonic Substitution Ciphers
  - Transposition Ciphers
  - Composed Ciphers
  - Machine Ciphers

Symmetric Cryptography

- Classic Cipher (Caesar)

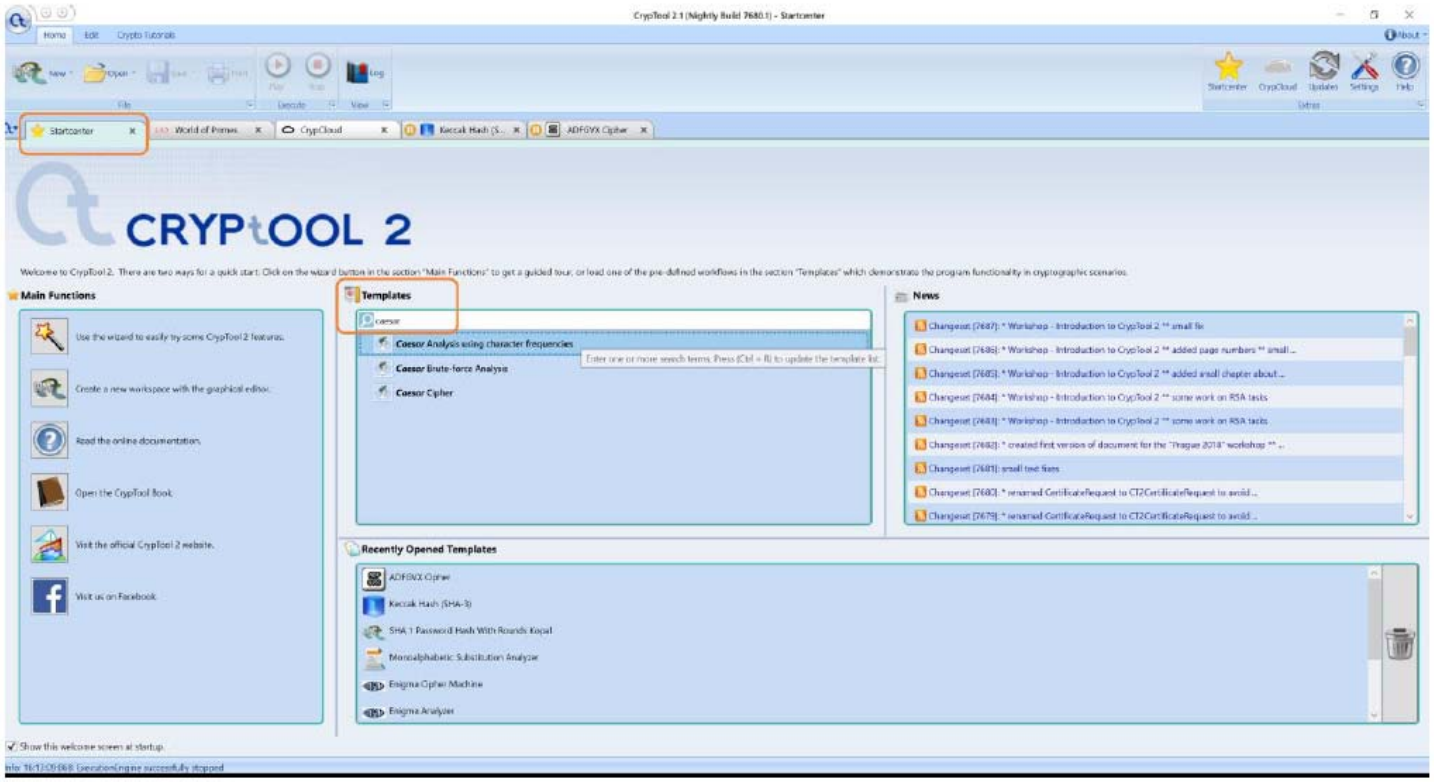
- **Assignment 1:** Decrypt the following text using the Caesar cipher

```
Va pelcgbtencul, n Pnrfne pvcure, nyfb xabja nf Pnrfne'f
pvcure, gur fuvsg pvcure, Pnrfne'f pbqr be Pnrfne fuvsg, vf
bar bs gur fvzcyrfg naq zbfg jvqryl xabja rapelcgvba
grpuavdhrf. Vg vf n glcr bs fhofgvghgvba pvcure va juvpu rnpu
yrggre va gur cynvagrkg vf ercynprq ol n yrggre fbzr svkrq
ahzore bs cbfvgvbaf qbja gur nycunorg. Sbe rknzcyr, jvgu n
yrsg fuvsg bs 3, Q jbhyq or ercynprq ol N, R jbhyq orpbzr O,
naq fb ba. Gur zrgubq vf anzrq nsgre Whyvhf Pnrfne, jub hfrq
vg va uvf cevingr pbeerfcbaqrapr.
```

Key: 13

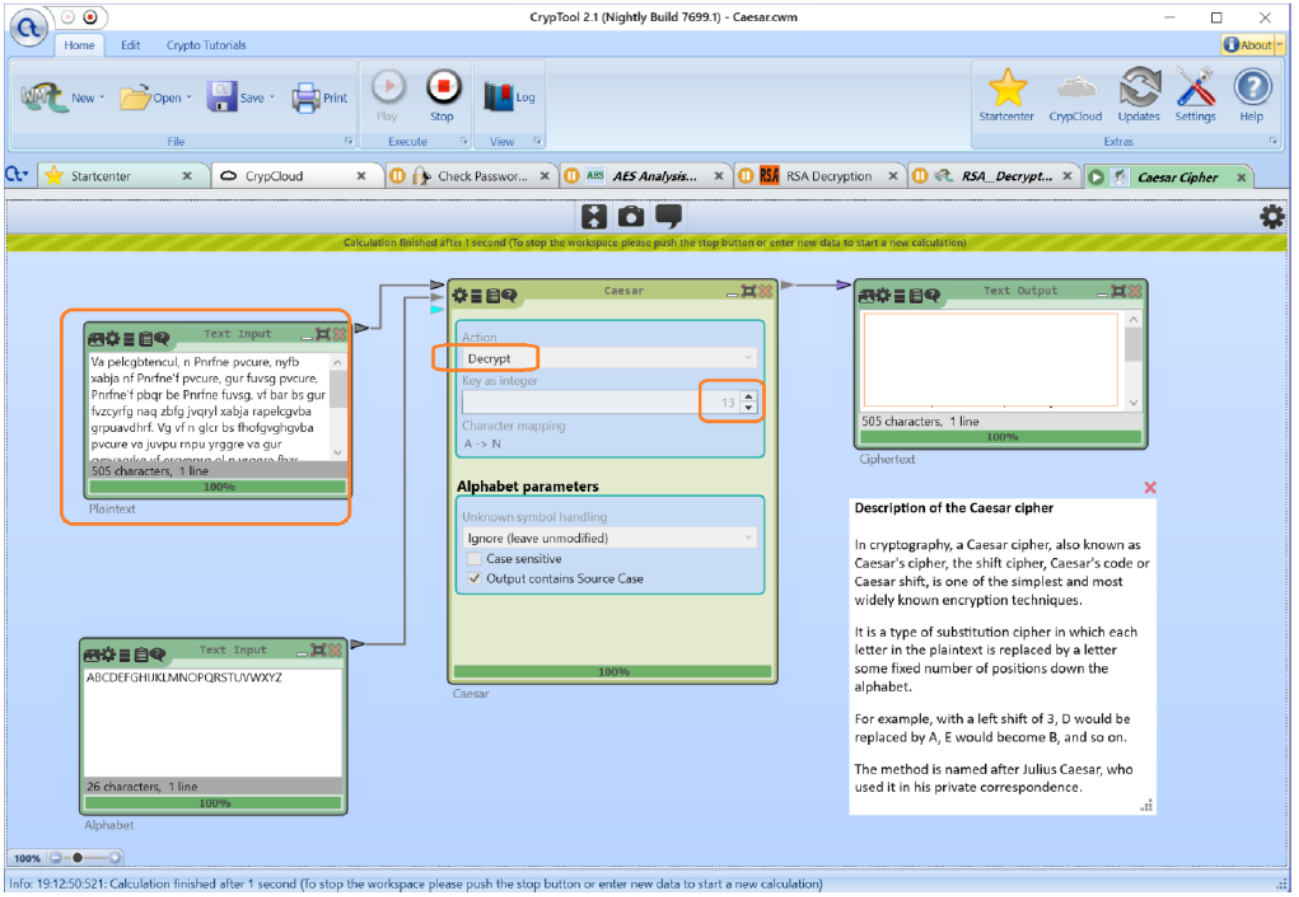
Symmetric Cryptography

- Classic Cipher (Caesar)
  - Hint 1: Open the template “Caesar Cipher” (or use the Wizard).

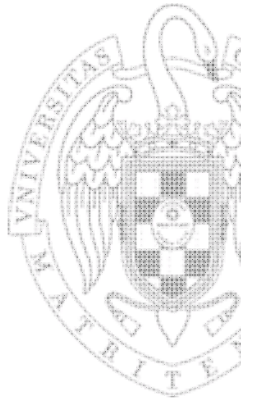


Symmetric Cryptography

- Classic Cipher (Caesar)
  - Hint 2: Use Ctrl+C, Ctrl+V to copy the text



Symmetric Cryptography



- Classic Cipher (Caesar)
- **Assignment 2:** Encrypt the following text using the Caesar cipher

- `Gaius Julius Caesar known by his cognomen Julius Caesar was a Roman politician and military general who played a critical role in the events that led to the demise of the Roman Republic and the rise of the Roman Empire. He is also known as an author of Latin prose.`

  Key: 10

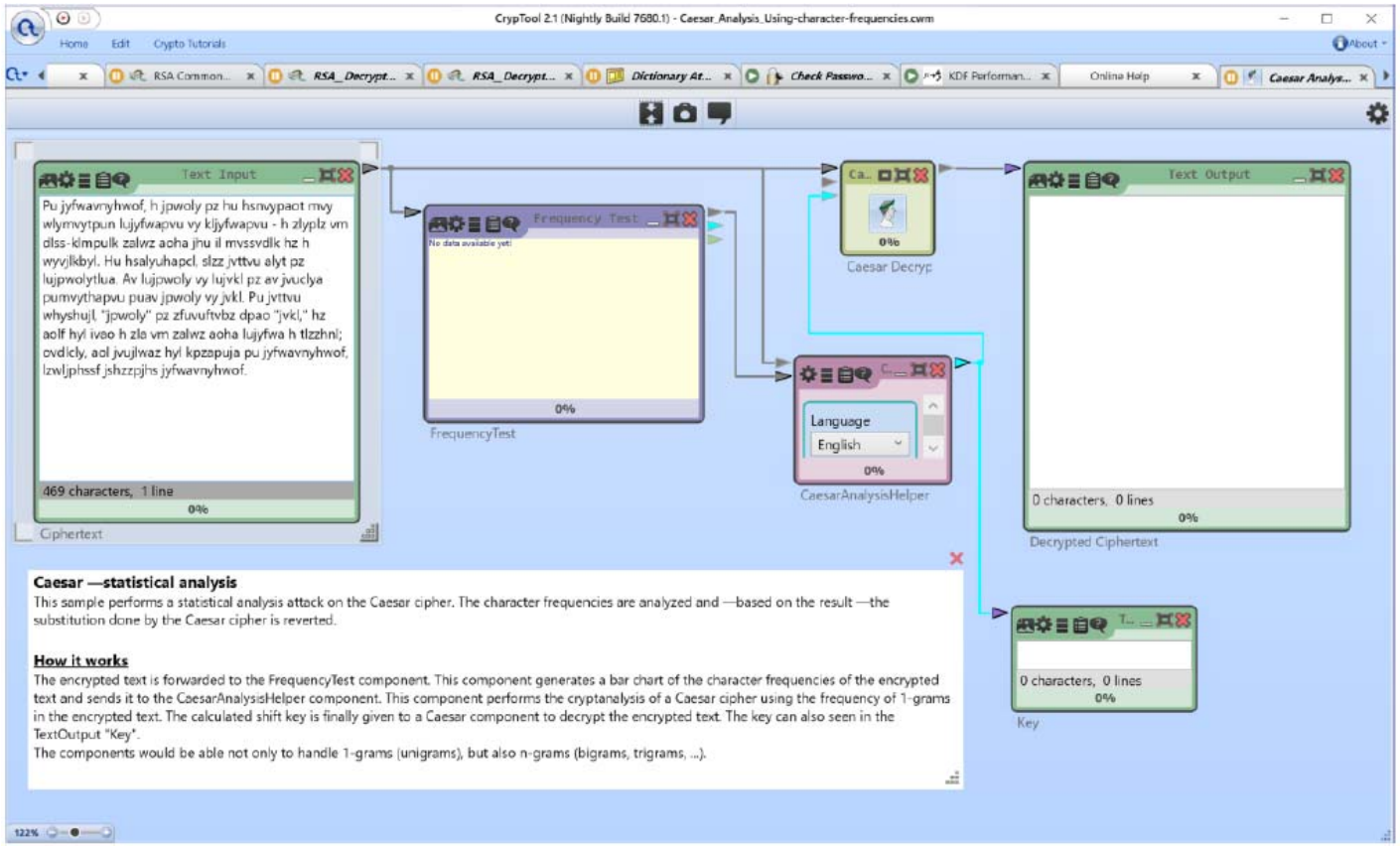
Symmetric Cryptography

- Classic Cipher (Caesar)
- **Assignment 3:** Break the following text using the template “Caesar Analysis using character frequencies”

```
Pu jyfwavnyhwof, h jpwoly pz hu hsnvypaot mvy wlymvytpun
lujyfwapvu vy kljyfwapvu -- h zlyplz vm dlss-klmpulk zalwz
aoha jhu il mvssvdlk hz h wyvjlkbyl. Hu hsalyuhapcl, slzz
jvttvu alyt pz lujpwolytlua. Av lujpwoly vy lujvkl pz av
jvuclya pumvythapvu puav jpwoly vy jvkl. Pu jvttvu whyshujl,
"jpwoly" pz zfuvuftvbz dpao "jvkl," hz aolf hyl ivao h zla vm
zalwz aoha lujyfwa h tlzzhnl; ovdlcly, aol jvujlwaz hyl
kpzapuja pu jyfwavnyhwof, lzwljphssf jshzzpjhs jyfwavnyhwof.
```

Symmetric Cryptography

- Classic Cipher (Caesar)
- **Assignment 3: Hint**: After entering the ciphertext from above, click on the “Play” button.



Symmetric Cryptography

Monoalphabetic Substitution Cipher

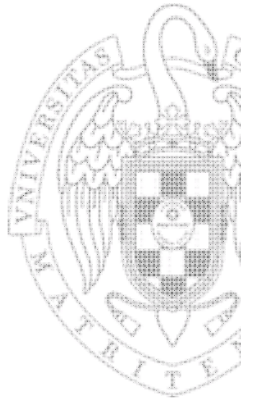
- **Assignment 4:** Decrypt the following ciphertext using the template "Substitution Cipher using a password":

```
rN YJBLGMUJaLTB, a YSLTWJ (MJ YBLTWJ) SI aN aPUMJSGTO VMJ
LWJVMJOSNU WNYJBLGSMN MJ XWYJBLGSMN—a IWJSWI MV DWPP-XWVSNWX
IGWLI GTaG YaN ZW VMPPMDWX aI a LJMYWXFJW. zN aPGWJNaGSEW,
PWII YMOOMN GWJO SI WNYSLTWJOWNG. kM WNYSLTWJ MJ WNYMXW SI GM
YMNEWJG SNVMJOaGSMN SNGM YSLTWJ MJ YMXW. rN YMOOMN LaJPaNYW,
"YSLTWJ" SI IBNMNBOMFI DSGT "YMXW",  aI GTWB aJW ZMGT a IWG
MV IGWLI GTaG WNYJBLG a OWIIaUW; TMDWEWJ, GTW YMNYWLGI aJW
XSIGSNYG SN YJBLGMUJaLTB, WILWYSaPPB YPaIISYaP YJBLGMUJaLTB.
```

Key: password = Hidden, offset = 10

- Hint: Change the setting action of the Encrypt component from Encrypt to Decrypt.

Symmetric Cryptography



- Monoalphabetic Substitution Cipher
- **Assignment 5:** Encrypt the following plaintext using the template "Substitution Cipher using a password":

```
Codes generally substitute different length strings of
characters in the output, while ciphers generally substitute
the same number of characters as are input.
```

Key: password = secret, offset = 8

- **Assignment 6**: Break the following ciphertext using the template "Monoalphabetic Substitution Analyzer"

```
JRU GOLF "XWNRUL" WP BOLQUL JWQUK QUZPJ "CULO" ZPF RZF JRU
KZQU OLWAWP: QWFFSU BLUPXR ZK XWBLU ZPF QUFWUHZS SZJWP ZK
XWBLZ, BLOQ JRU ZLZYX KWBL = CULO (KUU CULO - UJDQOSOAD).
"XWNRUL" GZK SZJUL IKUF BOL ZPD FUXWQZS FWAWJ, UHUP ZPD
PIQYUL. JRULU ZLU QZPD JRUOLWUK ZYOIJ ROG JRU GOLF
"XWNRUL" QZD RZHU XOQU JO QUZP "UPXOFWPA".
```

Symmetric Cryptography

- Polyalphabetic Cipher - Vigenère Cipher

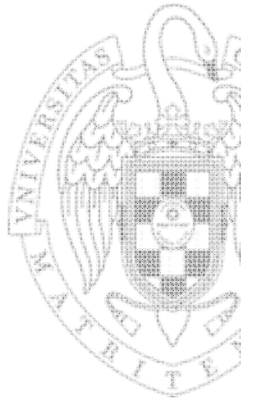
- **Assignment 7:** Decrypt the following ciphertext using the "Vigenère Cipher" template:

```
OPK QRXYSY WL IAGICKBOSA OESRV GW GLV ZDOKRRVV GDXNIE ARW
HQYEGXIMWCZIQ XF FGIOWR HV ZDOKRRVV MI BNI AMEIOMKRGL TIIBAVL
EEH RIY MA JRGO NOVFX UINKXMOIU FT OOSIEE FVBZMFXR FZTREFS ZR
CQY FBSB PV KOJEE UIG AOKASII BQUZNR SEOBOWGE SIGTGWB
```

  Key: VIGENERE

- Hint: You have to change the setting "Action" of the upper Vigenère component from "Encrypt" to "Decrypt".

Symmetric Cryptography



- Polyalphabetic Cipher - Vigenère Cipher
- **Assignment 8:** Encrypt the following plaintext using the "Vigenère Cipher" template:

  ```
  VIGENERE CREATED A DIFFERENT, STRONGER AUTOKEY CIPHER IN
  FIFTEEN EIGHTY SIX
  ```

  Key: BELLASO
- **Assignment 9:** Break the following ciphertext using the "Vigenère Analysis" template:

  ```
  TSF ECUMTBX JMGHPS FP EMQV QHXKIDUE REJGZIP EIOFOH WHCTBTLR
  JIIUC JXDGV LHW RN PBVCR XQTNHPGHLCIKBK EQEOII. AWCIIMQ WATK
  E DIIFH REXJIQLX KO POGIRXV I BLWJARF.
  ```

Symmetric Cryptography

Homophonic Substitution Ciphers

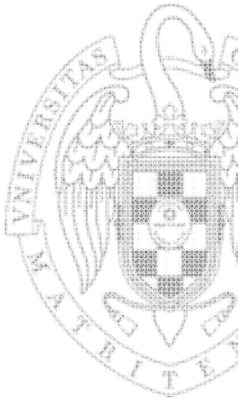
- **Assignment 10:** Decrypt the following ciphertext using the template "Homophone Substitution Cipher and Nomenclature – Decryption":

```
05 35 99 21 06 47 23 25 88 05 51 52 22 33 43 51 99 52 37 88
01 36 17 48 21 06 49 22 99 51 03 21 88 27 02 19 20 01 18 41
24 52 26 99 38 19 88 20 47 22 45 42 21 35 17 25 99 05 36 06
23 26 50 02 49 88 05 51 52 06 18 15 50 99 37 35 88 49 41 11
50 51 01 52 42 51 02 38 36 99 17 01 44 04 22 48 49 88 31 05
50 99 52 37 88 28 02 49 07 41 01 50 21 99 43 24 06 02 35 51
22 29 52 88 23 21 51 52 22 47 99 19 48 21 46 42 22 36 18 01
21 49 88 12 25 99 03 38 34 37 44 04 38 35 26 77
```

Key:

[ ];[99|88]	[B];[11|12]	[Y];[25|26]	[V];[39|40]
[.];[77]	[Z];[13|14]	[D];[27|28]	[U];[41|42]
[I];[01|02]	[K];[15|16]	[X];[29|30]	[P];[43|44]
[H];[03|04]	[C];[17|18]	[W];[31|32]	[Q];[45|46]
[A];[05|06]	[F];[19|20]	[M];[33|34]	[R];[47|48]
[G];[07|08]	[E];[21|22]	[N];[35|36]	[S];[49|50]
[J];[09|10]	[L];[23|24]	[O];[37|38]	[T];[51|52]

Symmetric Cryptography



Homophonic Substitution Ciphers

- **Assignment 11:** Encrypt the following plaintext using the template "Homophone Substitution Cipher and Nomenclature – Encryption":

```
THE BEALE CIPHERS ARE ANOTHER EXAMPLE OF A HOMOPHONIC CIPHER.
THIS IS A STORY OF BURIED TREASURE THAT WAS DESCRIBED BY USE
OF A CIPHERED TEXT THAT WAS KEYED TO THE DECLARATION OF
INDEPENDENCE.
```

Key:

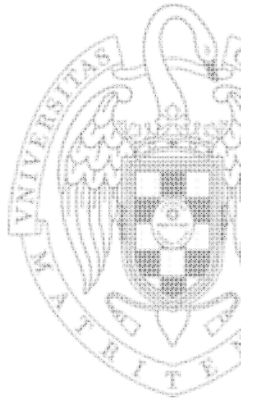
[ ];[99|88]	[B];[11|12]	[Z];[25|26]	[N];[39|40]
[.];[77]	[H];[13|14]	[K];[27|28]	[M];[41|42]
[E];[01|02]	[I];[15|16]	[V];[29|30]	[R];[43|44]
[D];[03|04]	[A];[17|18]	[W];[31|32]	[S];[45|46]
[F];[05|06]	[X];[19|20]	[L];[33|34]	[Q];[47|48]
[C];[07|08]	[y];[21|22]	[T];[35|36]	[P];[49|50]
[G];[09|10]	[J];[23|24]	[U];[37|38]	[O];[51|52]

Symmetric Cryptography

- Homophonic Substitution Ciphers
- **Assignment 12:** Break the following ciphertext using the template "Homophonic Substitution Analysis":

```
39 03 51 11 49 52 29 30 04 15 29 51 99 45 43 09 10 52 88 33 35 13 30
51 99 52 09 16 36 88 07 37 35 19 38 99 51 15 88 40 03 36 27 52 37 38
04 99 50 51 29 30 03 16 29 52 88 46 44 10 09 51 99 34 35 14 30 52 88
20 51 15 99 52 37 88 04 29 51 10 03 52 38 99 16 47 01 36 09 51 13 88
33 35 10 21 12 52 30 02 99 51 37 45 88 34 09 52 22 19 14 04 39 01 29
99 20 02 36 88 10 03 28 43 46 99 04 38 88 37 51 33 09 44 15 99 52 30
88 29 01 43 99 30 03 11 44 88 35 41 99 29 02 43 88 16 48 04 44 38 30
03 42 04 47 99 13 43 27 36 10 17 29 03 35 37 88 51 38 45 99 14 44 41
36 13 12 52 30 04 35 37 77 88 99 40 03 51 11 49 52 29 30 04 15 29 51
88 46 43 09 10 52 99 34 36 14 30 51 88 16 33 44 38 29 99 30 01 43 88
12 52 05 35 13 03 29 21 99 36 42 88 02 04 15 99 09 03 41 44 88 35 37
99 16 48 04 43 38 30 03 42 04 47 88 44 37 45 43 51 28 36 14 15 77 99
01 44 88 50 43 38 44 41 03 29 43 46 99 42 13 35 11 88 52 37 99 04 38
41 36 14 12 51 10 88 44 45 18 48 52 30 03 35 37 99 36 42 88 29 17 30
35 13 16 99 51 38 46 88 27 04 15 03 29 16 99 41 14 36 11 88 13 43 37
35 19 38 44 45 99 15 47 02 36 09 52 14 16 77 88 01 04 15 99 12 35 16
30 88 42 51 11 36 18 15 99 20 35 13 08 88 03 16 99 43 37 29 04 30 10
44 46 88 12 52 39 03 51 43 99 38 52 29 17 14 51 09 04 15 77
```

Symmetric Cryptography



- Homophonic Substitution Ciphers
- **Assignment 13:** Break the following ciphertext using the template "Homophonic Substitution Analysis":

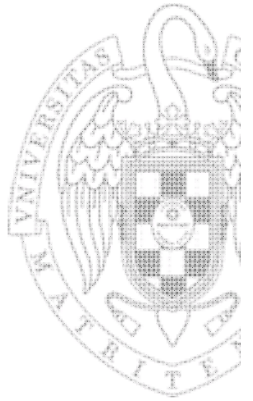
```
§ a ä / @ o + $ ) u Ä e q s m @ p - ö f + w g e = Ä n b § f )
- ( h c d g e a 1 + o # h m r @ f Ä = - q g + $ b ä / @ - ö e
+ x h f ) Ä n a § e = - ä p + $ f - + e g v @ b - w m ö r q Ä
f + % 0 - @ e ^ a ä o ‘+ § t r # h n - ( ' $ m b Ä p + a s q
x ö ) ° @ - = g ) ^ o h f + t e = Ä n - r # @ + i p Ä s ) g f
1 c - b @ w ä o + / § m n h a b : - ö q + r Ä a b p - g Ö + $
- 0 h t e ° + ^ ä m a - f § d @ = + $ b ö ( Ä - Ö § a b ä e °
+ q ' n g s ^ # - $ + m § & % ö r - ' h a @ + ä f q g - $ + Ö
§ e r $ o 1 - x h n b ) + j g i t a § q Ä = - & 0 + j @ / s b
ö $ m - § f r # n h i g c h m j ' ä ( + / n Ä $ q t m @ p
```

Symmetric Cryptography

- Homophonic Substitution Ciphers
- **Assignment 14:** Break the following ciphertext using the template "Homophonic Substitution Analysis":

```
19 20 03 21 31 11 53 41 14 24 02 13 25 51 15 39 06 05 30 59 56 03 54
31 35 29 34 14 10 48 57 09 27 06 39 53 16 04 56 05 20 25 35 01 18 36
57 07 55 59 03 26 05 41 14 24 31 33 02 04 35 54 29 39 45 20 47 21 58
59 42 27 47 38 12 55 15 02 16 47 53 48 14 56 28 49 34 57 36 03 19 13
39 16 05 26 35 41 25 27 54 28 59 55 22 31 20 14 45 39 57 52 02 21 36
05 41 27 15 51 32 07 53 48 15 30 13 21 55 59 14 56 01 18 39 59 58 03
54 14 47 02 47 24 31 16 12 27 36 48 35 20 29 34 55 42 24 02 26 28 53
21 57 33 56 47 27 39 03 36 10 55 16 47 02 41 25 31 26 06 19 16 01 27
47 38 15 21 53 59 14 56 16 48 39 45 04 03 15 42 51 29 25 36 31 28 58
13 59 19 30 32 34 55 47 14 21 53 10 01 02 16 38 49 27 48 42 05 15 36
56 26 35 54 39 45 59 24 57 20 44 05 41 29 34 03 47 21 31 14 39 53 16
48 12 56 47 03 15 31 07 51 16 53 49 24 35 36 56 57 54 47 03 55 21 05
59 10 14 34 31 38 12 53 16 56 28 03 32 35 18 24 31 47 53 26 02 20 28
16 56 27 26 33 10 49 55 36 48 57 41 25 34 02 01 06 47 58 42 39 24 03
15 31 21 53 59 14 56 16 48 05 39 12 27 15 07 36 03 55 47 59 34 02 14
01 27 16 38 24 55 28 48 02 54 32 39 35 19 20 31 26 59 34 53 27 14 39
56 42 47 59 03 28 55 15 48 02 15 48 57 41 27 14 05 45 54 58 30 31 21
35 08 55 04 53 39 24
```

Symmetric Cryptography



- Homophonic Substitution Ciphers
- **Assignment 15:** Use the ciphertexts from the previous tasks and copy them one by one into the template “Statistic Tests for Classical Ciphers” (“Plaintext” text input component). Compare the results of the “Friedman Test” component with the different types of ciphers. Hint: You have to delete the Vigenère component from the workspace and afterwards connect the “Plaintext” text input component with the “Frequency Test” component. Otherwise, all texts would be encrypted using the Vigenère cipher every time you insert a new text.

Symmetric Cryptography

Transposition Ciphers

- Scytale cipher
- Columnar transposition cipher

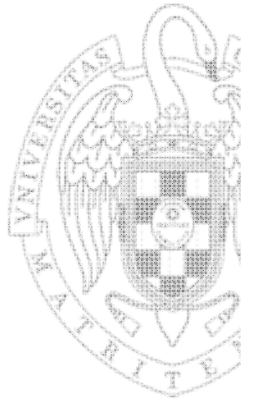
Symmetric Cryptography

Transposition Ciphers

- Scytale cipher

The Scytale cipher is one of the oldest known encryption devices. It was used by the Greek in the 7th century BC. The message was written on a parchment wound around a stick. If the parchment was released, the message could not be read any more. To decrypt the message, a stick with the same diameter has to be used.

Symmetric Cryptography



Transposition Ciphers

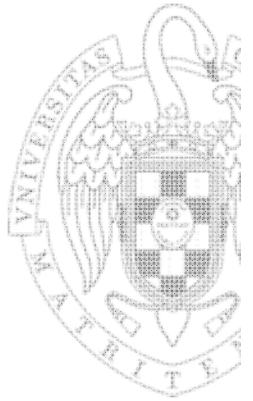
- Scytale cipher
  - **Assignment 25:** Decrypt the following text using the “Scytale Cipher” template:

    ```
    IMRHPINAWIAPCTISRHRRTWTEYAHRARPNAINTTSSTSOOPTTICGORENORSINPMA
    IPAAMPTOMRUHIFETNYOPSIIANASCCSCRAUACICGLTYPHEAETHMTRDAEEHAULR
    NERRECTAEIIOWNSNSNOCAGASUIIMTINEDIOSDNTLOTATOILIRGHTUNORAASGU
    EVREONEEYDFDKUCTAISSAOCTAEMPYONDPELNDTARIWTHIFNHHIGODIESNRECS
    CS
    ```

    Key: 6

    Hint: You have to change the setting “Action” of the Scytale component from “Encrypt” to “Decrypt”.

Symmetric Cryptography



Transposition Ciphers

- Scytale cipher
- **Assignment 26:** Encrypt the following text using the “Scytale Cipher” template:

THEANCIENTGREEKSANDTHESPARTANSINPARTICULARARESAIDTOHAVEUSEDTHISCIP
HERTOCOMMUNICATEDURINGMILITARYCAMPAIGNS

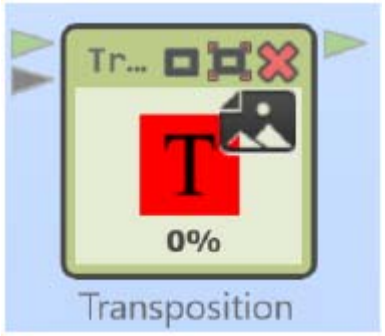
Key: 11

- **Assignment 27:** Break the following text using the “Scytale Brute-Force Analysis” template:

Fweemnsa ratnat taos tnun m Ah roac fr wit riiccre cynrheisulpdsint
netitlteataor ourlirgemcrssl rcehy o iatnu d Anp tsBumpdhei Creoiivow.inlccinh ntla deoOgiotded
t onien lhtniovcbieheunieyvredsc e oettdGfiof hh rotf aeeiel ip nelbRtpsG kouhsecrt wto
ayehai durteennieseak dgtsedl s _epeRcwta_ ovoeahs_

Hint: Take care that you analyze the text without any line breaks. If there are line breaks after copying the text remove them!

Symmetric Cryptography



Transposition Ciphers

- Columnar Transposition Cipher

- **Assignment 28:** Decrypt the following text using the “Transposition Cipher” template:

  ctconsueaeortoegoiccsfsishoreaiayteligscsulrridbinxcgttenxhieteditoepiaitseehosrrattptpt
  mphlafttittapnhfwitaolaxafnanhooytdrseuityapoytitcuhesotoprninoedrtcehlyotipbneamhttnr
  ssrhhphnyenmp

  Key: transposition

  Hint: You have to change the setting “Acton” of the upper transposition component from “Encrypt” to “Decrypt”.

- **Assignment 29:** Encrypt the following text using the “Transposition Cipher” template:

  inacolumnartranspositionthemessageiswrittenoutinrowsofafixedlengthandthenreadoutaga
  incolumnbycolumnandthecolumnsarechoseninsomescrambledorder

  Key: Uppsala

Symmetric Cryptography

Transposition Ciphers

- Columnar Transposition Cipher
  - **Assignment 30:** Break the following text using the template "Transposition Hill Climbing Analysis":

    AENNTUTDSOENHIMEIUDOFSNSSCASILTBSSCLSNEOTMT
    OOIAGURSCEKUGBUGIHAIOANNOEANLTONBCGNILNRTS
    TCSEIPLRLMAIOAEEPLMTTEGNLNLGSAMIORPODAYISOE
    WGSUSNHKRBG

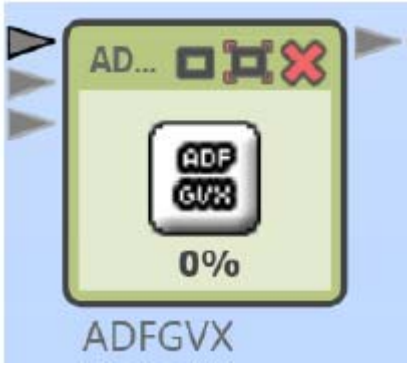
    Hint: You have to change the setting "Keysize" of the transposition analyzer component to 6.

    Additionally, you have to change the setting "Read Out" of the "Transposition" parameter of the transposition analyzer to "by column".

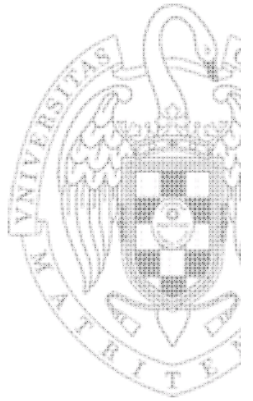
Symmetric Cryptography

Composed Ciphers

- ADFGVX Cipher
  - The ADFGVX was used by the German forces in WW1. It was successfully broken by Georges Painvin.



Symmetric Cryptography



Composed Ciphers

- ADFGVX Cipher
  - **Assignment 31:** Decrypt the following text using the "ADFGVX Cipher" template:

    AAFDDAADGVAVAVDVAFDAAFAGVGAFAGFAAGFDAVDGAVAAAAG
    VDGAVAXAGAGDDXFVAGDGDXFFAGAAFFGAAFAGAAAFGFDVDD
    DVDGADGGFGAFADFDADAXDDFFDFVAXDGVGDFAXAGDFAXAD
    AADDFDFAGDADFADFAAAGDXGGAGGFDGAFFFDGADDAGGVAA
    XAFDGDGGDDDDGGFVGAFAFFGAAFDAFFVFVDAGVDDAGAGFV
    FGDDFFADADFDAFFAAAGXDDGDFXDDAVDFFGFVDVADAGGVG
    DGDDFGDDXFXFVFGADAVAXFADX

    Keys: For substitution: TREE, for transposition: HOUSE

    Hint: You have to change the setting "Acton" of the left "ADFGVX Encrypt" component from "Encrypt" to "Decrypt". The keys can be also applied as settings.

Symmetric Cryptography

Composed Ciphers

- ADFGVX Cipher
  - **Task 36:** Encrypt the following text using the “ADFGVX Cipher” template:

    GEORGESJEANPAINVINWASAFRENCHCRYPTANALYSTDU
    RINGTHEFIRSTWORLDWARXHISMOSTNOTABLEACHIEVE
    MENTWASTHEBREAKINGOFTHEADFGVXCIPHERINJUNE19
    18

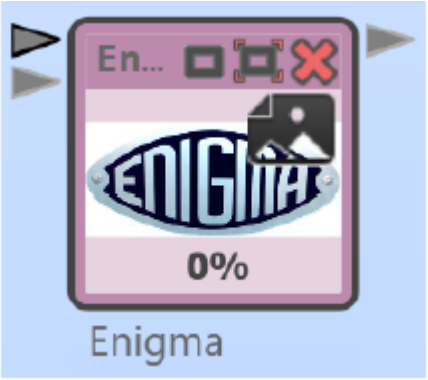
    Hint: Breaking ADFGVX automatically is still on the to-do list of the CT2 team.

Symmetric Cryptography

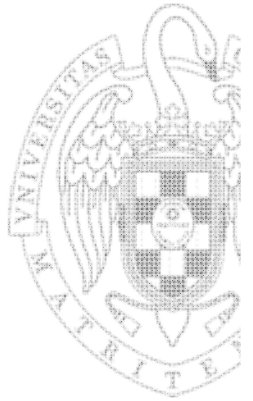
Machine Ciphers

- Enigma Machine

The Enigma was used by the German forces in WW2. It was successfully broken by Polish, British, and US cryptanalysts.



Symmetric Cryptography



Machine Ciphers

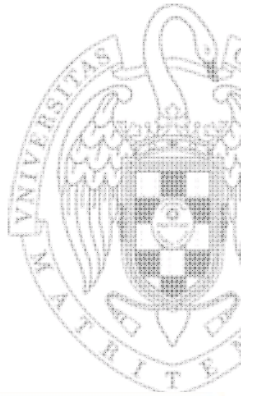
- Enigma Machine
  - **Assignment 33:** Decrypt the following text using the "Enigma Cipher Machine" template:

    SFCLFTRHHSMOGDEWODWBWPMRHVYJIMCPOJQOBNFZ
    JLCPFHAACMHOLJSQBBRWWXNFONMHCIBWLNTPGLYQN
    QRREBMBXWWNDRYWVLOLEEZUBCRDSKAKTTJSCLXQB
    ADONWKKKLNPCZEAQATCHCHMIZPGWXIXNOIEZRRDZHY
    SREO

    Key:

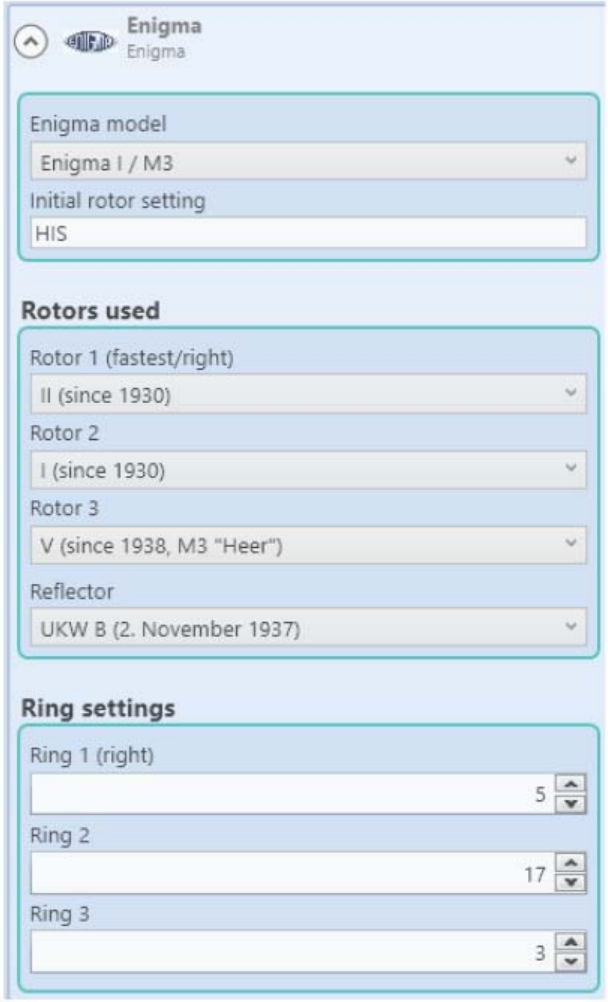
    Set the key settings (parameters) according to the following picture:

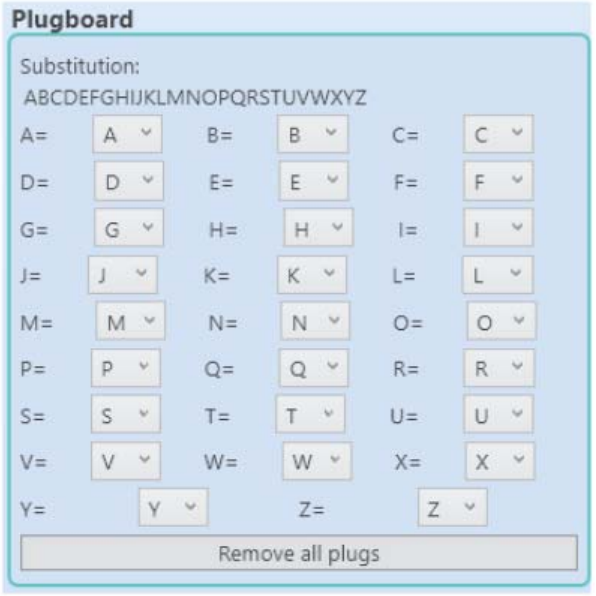
Symmetric Cryptography



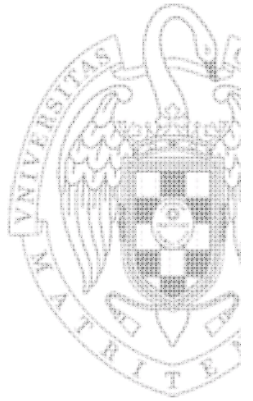
Machine Ciphers

- Enigma Machine
- **Assignment 33: Key**





Symmetric Cryptography



Machine Ciphers

- ## Enigma Machine

- **Assignment 34:** Encrypt the following text using the "Enigma Cipher Machine" template:

  ENIGMAWASINVENTEDBYTHEGERMANENGINEERARTHUR
  SCHERBIUSATTHEENDOFWORLDWARI

  Key:

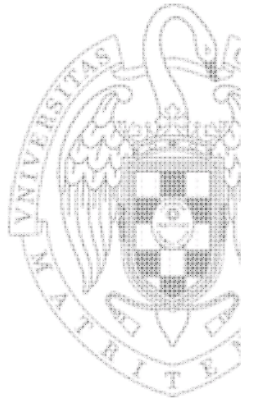
  Set the key settings (parameters) according to the following picture:

Symmetric Cryptography

Machine Ciphers

- Enigma Machine
- **Task 38: Key**

Symmetric Cryptography



Machine Ciphers

- Enigma Machine

- **Assignment 35:** Break the following ciphertext using the "Enigma Analyzer" template:

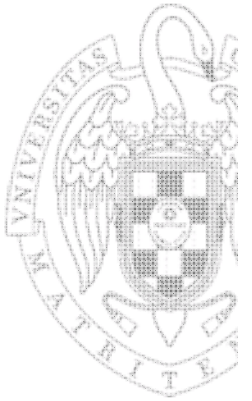
WYCLKWEDNUZRBERPNUHSVOGIBNUREFSCKHSTWCBKBJVSE
YRPOVBANIKKLBKGVAOYCWZQZBFUTXSLJAHKQLJVSTHSDBKJ
NAOHWMTTMAJKPZWPBYMUMNHRUHKIRBKVIDKKMUDHGJVPV
MCVTOHRKFEGZDNZNELAHTAXFMSATNKBRVLMJTBNKVVQETM
ZUGQHHFRTAIPTSLRQAWWJNWKEDWACHWEVYFGNLCFKAAW
DHCFYPKWZAISLOUJMJDBKNINROEXCZIEUEQYBJBJGUYFLTYD
PROGMQBZWSBWOFWROTYUJOHEDGYJNXSBQXYPKHTDIGUY
DNLUVEWJIXCPTNTKGPONLABSRZMQOQKQAUNAJYVCMNDZZ
YSWRYYFRZLBTAVHFTBWSDINHSRARTEJTQTVHCUCYURQSUA
BESRSXNDJYGUVJKZPFOVYVPAXRHQPFXRJTIRMEKWABVXNDZ
XCGONWWQLGXKSSHUBTGXMJPRCHPSOQFKNFMDPFTGRNLS
SRSXMXBEARHFPXVKHNHLDRIUHLMHAWVOZPFREVCNM

Symmetric Cryptography

Identifying the type of a cipher

- Not always possible without further knowledge about the cipher's origin and background.
- To identify the type of the cipher CT2 implements some useful tools, such as:
  - Frequency test component: visualizes the letter distribution of a given text.
  - Friedman test component (kappa test)

Symmetric Cryptography

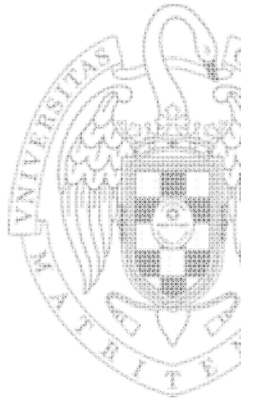


Identifying the type of a cipher

- Plaintext
- **Assignment 36:** Analyze the following plaintext using the "Statistic Tests for Classical Ciphers":

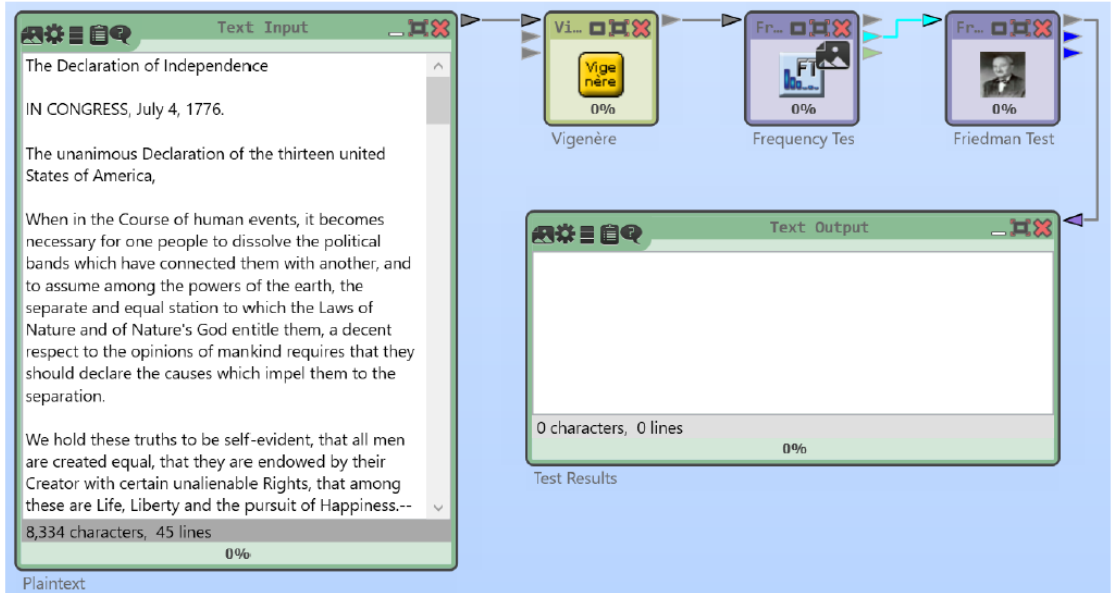
INCOMPUTINGPLAINTEXTISTHEDATAEGFILECONTENTSTHATREPRESENTONLYCHARACTE
RSOFREADABLEMATERIALBUTNOTITSGRAPHICALREPRESENTATIONNOROTHEROBJECTSI
MAGESETCITMAYALSOINCLUDEALIMITEDNUMBEROFCHARACTERSTHATCONTROLSIMPLEA
RRANGEMENTOFTEXTSUCHASLINEBREAKSORTABULATIONCHARACTERSPLAINTEXTISDIF
FERENTFROMFORMATTEDTEXTWHERESTYLEINFORMATIONISINCLUDEDANDFROMBINARYF
ILESINWHICHSOMEPORTIONSMUSTBEINTERPRETEDASBINARYOBJECTSENCODEDINTEGE
RSREALNUMBERSIMAGESETCTHEENCODINGHASTRADITIONALLYBEENEITHERASCIISOME
TIMESEBCDICUNICODEBASEDENCODINGSSUCHASUTF8ANDUTF16AREGRADUALLYREPLAC
INGTHEOLDERASCIIDERIVATIVESLIMITEDTOSEVENOREIGHTBITCODESFILESTHATCON
TAINMARKUPOROTHERMETADATAAREGENERALLYCONSIDEREDPLAINTEXTASLONGASTHEE
NTIRETYREMAINSINDIRECTLYHUMANREADABLEFORMASINHTMLXMLANDSOONASCOOMBSR
ENEARANDDEROSEARGUEPUNCTUATIONISITSELFMARKUPTHEUSEOFPLAINTEXTRATHERT
HANBITSTREAMSTOEXPRESSMARKUPENABLESFILESTOSURVIVEMUCHBETTERINTHEWILD
INPARTBYMAKINGTHEMLARGELYIMMUNETOCOMPUTERARCHITECTUREINCOMPATIBILITI
ES

Symmetric Cryptography



Identifying the type of a cipher

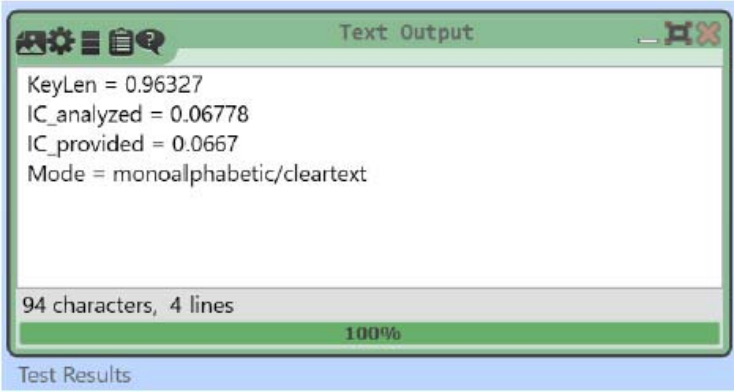
- Plaintext
- **Assignment 37:** Hint: The template has to be modified. You have to delete the “Vigenère” component and connect the “Text Input” directly with the “Frequency Test” component. To delete the Vigenère component, you can either click on the small red X or you can click the component and use the “del”-key of your keyboard (see next page for a screenshot).



Symmetric Cryptography

Identifying the type of a cipher

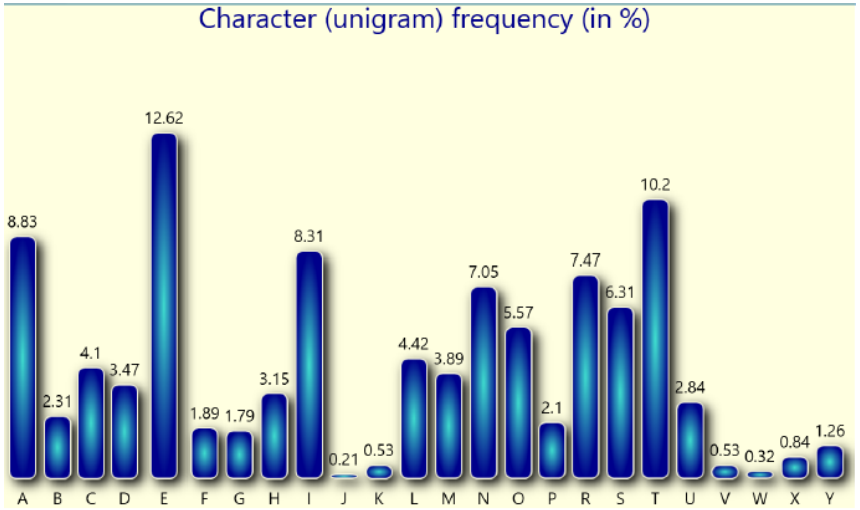
- Plaintext
- **Assignment 38:** After removing the Vigenère component, you can enter the plaintext in the Text Input. The "Text Output" component should display that the entered text is monoalphabetic/cleartexts.



Symmetric Cryptography

Identifying the type of a cipher

- Plaintext
- **Assignment 39:** Now, also double-click on the “Frequency Test” component to visualize the text’s letter frequencies.



- The presentation of the “Frequency Test” component displays the distribution of each single letter. Here, you can see that with English language, the letter E is the most frequent letter. The more text you have, the better is the analysis. With plaintext, the distribution is very rough. A “good” cipher will flatten the statistics (as you will see with the polyalphabetic cipher in one of the next tasks).

Symmetric Cryptography

Identifying the type of a cipher

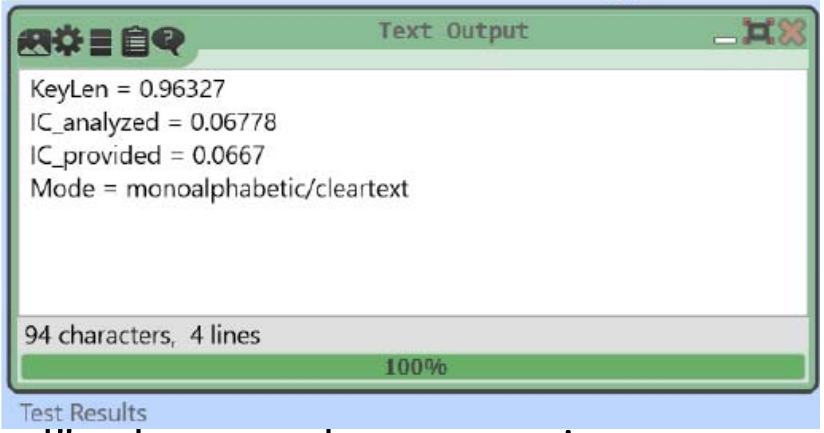
- Transposition cipher
- **Assignment 40:** Analyze the following transposed text using the "StatIstIc Tests for Classical Ciphers":

PNDCATCDITLAHITCTFSORFSSIEXEMWINDNNPSRAEEUECRLEEIANT6LNAATOCTNTTAEES
TNULHSBDUIFUTTEENSMINIGTARIIGIGNRCOMTPENJSLAMACPMSBBAAIODSMCRIHONAJE
RSTGINISCNCDRPODSSHFOUEGOLLNACEMMSESCIUPAIORSREWBEMPTOTNPSFTEHFANHSO
EESLBCOLEURURIFMTTALOLSNTSEDEIHHOEIEOCHUALLELETINPTENAOTITAALCAETTPL
TTEKFVTIYMMUEMIMIEEHNAARIATTSINIORRROAKTTERRTEOEIIEUPNSTNGNTLHMDBIU1
AIRVINTSIOARDTAEIHBNDMNGTLENRRREEERIKRERUTIXATELRLBRPOOGYDNAAIGXNTCP
SFTROIDYITEEOORETIIESMNDSAERHIVTIETRRRYDAEERNOLNERUIROTNSMLSHHRTYOHN
LUTAOTOTAASRTEMMLECTLATLOORTNAHNIAAWOTERNGMSOAYRTCSGFALGSTEROHMHALR
X
TYDMETOSDEOMSEHASATUNPNEOREBCLTISSARTOIERCTOIETNENCELANFFEYTUMEOSEBC
IAMEANISBDOATDADRIVBLTOANSININLDSAORAUSTAHSXUIITLMLUTCPEOAHLTEREETCN
OTCIMRETATHAACTEOXLIDBSMMRITNLAESATOCEDSFUCEIMEIEARDEINGRSYAINOARAEH
IETPPLVEDAANETASNTEEPYSEUARNBEAEURTMETEAHLDREERNFFCIIDBDSRCNTECEIEUN
GEEIEOGSCKMECPSEMERRXANONSKFRBTAEUBETHIMICITETNRNEBLGEIRAAUDHHSNEIRN
SITTEFSNRHRBTYCEBEDDBAIUES8RYTCIDEDAAEALETHRIAFMOREPNAEXAMSBOCTAGLCC
II

Symmetric Cryptography

Identifying the type of a cipher

- Transposition cipher
- **Assignment 41:** The result should look like the following screenshots



- Notice that the “KeyLen” and “IC:analyzed” values are the same as in assignment 40. That is because we used the same text and removed all special characters. Then we transposed it using the columnar transposition cipher. Also the letter frequencies should be the same as in task 40.
- What you should learn here: Transposition ciphers do not change the letter frequencies nor the result of the Friedman test. Thus, if you have a “gibberish” text and the Friedman test indicates “monoalphabetic/cleartext”, it may be a transposed text. To be surer, have a look at the frequencies. If the “E” is the most frequent letter, it is most probably a transposition cipher.

Symmetric Cryptography

Identifying the type of a cipher

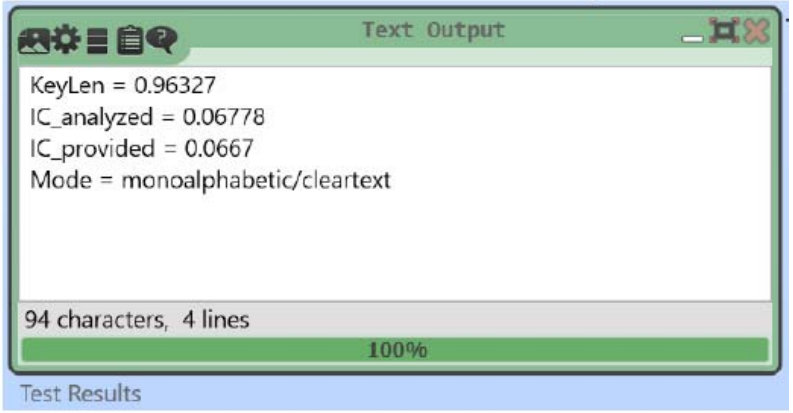
- Monoalphabetic Substitution Cipher
- **Assignment 42:** Analyze the following substituted text using the “Statistic Tests for Classical Ciphers”:

CUWQVNGJCUTNPZCUJIDJCKJOIHZJZITSCPIWQUJIUJKJOZJLINLIKIUJQUPBWOZLZWJI
LKQSLIZHZXPIVZJILCZPXGJUQJCJKTLZNOCWZPLINLIKIUJZJCQUUQLQJOILQXRIWJKCV
ZTIKIJWCJVZBZPKQCUWPGHIZPCVCJIHUGVXILQSWOZLZWJILKJOZJWQUJLQPKCVNPI
ZLLZUTIVIUJQSJIDJKGWOZKPCUIXLIZYKQLJZXGPZJCQUWOZLZWJILKNPZCUJIDJCKHC
SSILIUJSLQVSQLVZJJIHJIDJEOILIKJBPICUSQLVZJCQUCKCUWPGHIHZUHSLQVXCUZLBS
CPIKCUEOCWOKQVINQLJCQUKVGKJXICUJILNLIJIHZKXCUZLBQXRIWJKIUWQHIHCUJITI
LKLIZPUGVXILKCVZTIKIJWJOIIUWQHCUTOZKJLZHCJCQUZPPBXIIUICJOILZKWCCKQVIJ
CVIKIXWHCWGUCWQHIXZKIHIUWQHCUTKKGWOZKGJS8ZUHGJS16ZLITLZHGZPPBLINP
ZWCUTJOIQPHILZKWCCHILCFZJCFIKPCVCJIHJQKIFIUQLICTOJXCJWQHIKSCPIKJOZJW
QUJZCUVZLYGNQLQJOILVIJZHZJZZLITIUILZPPBWQUKCHILIHNPZCUJIDJZKPQUTZKJOII
UJCLIJBLIVZCUKCUHCLIWJPBOGVZULIZHZXPISQLVZKCUOJVPDVPZUHKQQUZKWQQV
XKLIUIZLZUHHILQKIZLTGINGUWJGZJCQUCKCJKIPSVZLYGNJOIGKIQSNPZCUJIDJLZJOIL
JOZUXCJKJLIZVKJQIDNLIKKVZLYGNIUZXPIKSCPIKJQKGLFCFIVGWOXIJJILCUJOIECPHC
UNZLJXBVZYCUTJOIVPZLTIPBCVVGUIJQWQVNGJILZLWOCJIWJGLICUWQVNZJCXCPCJ
CIK

Symmetric Cryptography

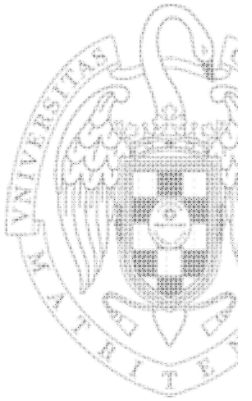
Identifying the type of a cipher

- Monoalphabetic Substitution Cipher
- **Assignment 43:** The result should look like the following screenshots



- The same result a third time? Yes, that is true. This time, we encrypted exactly the same text using a monoalphabetic substitution cipher. This means, each letter is substituted by another one. The frequencies of the plaintext remain but the according letters changed. For example: In the plaintext, maybe the T had 1s79%, now the T is replaced with X. Then, the X will have 1s79%. To be sure that a “gibberish” text was encrypted using a monoalphabetic substitution, you should have a look at the presentation of the “Frequency Test” component. If the E is not the most probable letter, you surely have a monoalphabetic substitution.
- Special task: Break the monoalphabetic substitution of this task!

Symmetric Cryptography

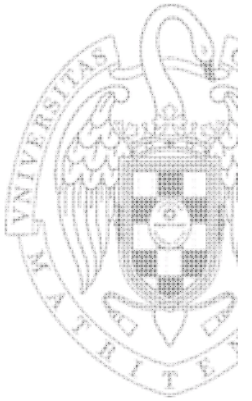


Identifying the type of a cipher

- Polyalphabetic Cipher (Vigenère Cipher)
- **Assignment 44:** Analyze the following substituted text using the "Statistic Tests for Classical Ciphers":

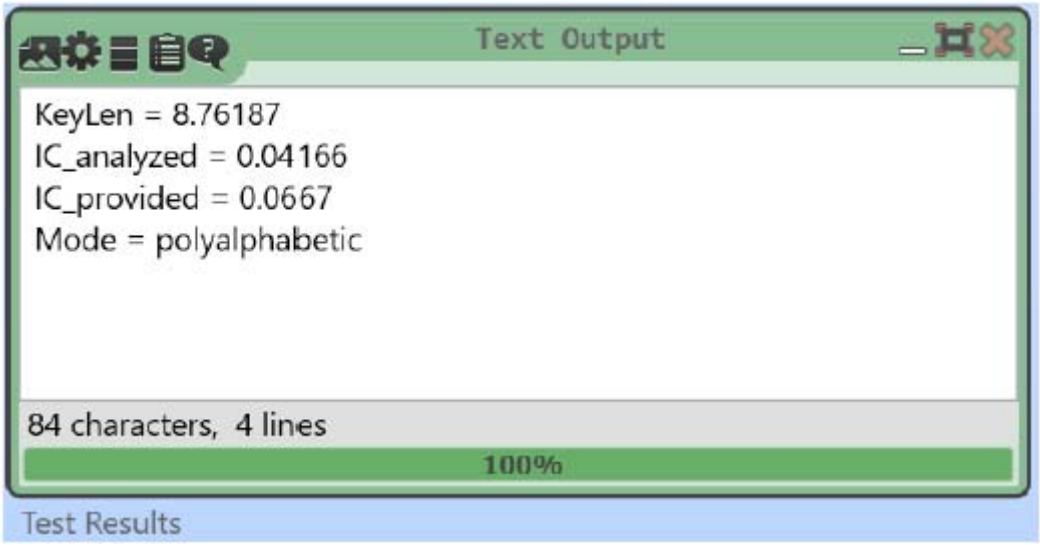
PV UHARLRXGC, DCKAU HTEB AL HJV BPMW (S.X. PASS RVVLXBVJ) RWTP
FVZJLGTUB GGZA TFPKWQKOJZ CU YMSWODCC BTPSISSS PJA VGM WVJ EGTLVZMSS
FTWZWLSPKYIBKB EYJ VHWLZ GUXGTRH (BIOXOK, LHR.). PB ETM CCQD BJQCEVL
O APUAMSF ESBUAF FP UOOGHKLXFU KFPM YCEDJVZ HPUHES CIPPGCSDOFA CU
AMPM, GWTF PL HWEO TYSPRA GK HCSSATPWFX UOOGHKLXFU. GJPBJ HVHL PG
SPNXXFGER UKKA WYJTOIAMV MSZK, UWXNS JDQSS XUNGKACKGDG EG ZXUSISLL,
SGR HIMB "UEBRBQ MWALA" AG KJZAW LKAV ZGYHXVVK FIUK ZT BJHVBHYSILL
SL PKEYGR KPAOUAG (TUKGWSF ZLIXCSIC, JLOA UCEUSTJ, GBTCSJ, OLJ.).
HWL MFVCFZLV AWG KBSKWIPWFTZNP ZTXJ SZDZLF PZKAB, GQDCIBISJ OTJRXJ.
CFBQQUC-QTOSU OFJCSPVYL GWTF PL QHW-8 KFK IIM-16 IJX UTRBJTHZP
BWWZPJQFZ HJV MAWAF RCUPW SLZAOOVZTTL HWDSLLR IV AWOSP FP TBCVK LAA
QDKMK. YWNVQ IAWH TYFAOXU USKYWG MG HPVVB ELHP-KILT OTV ETGAFRVDF
QDUAAWSTVB EEWWE-DWEH, PZ TGGU CJ RWX ABKSJLHN YMETWPJ GC WEFVMLSM
WBUSG-FGRBPUHS WYJT (OH PV ZMAN, OKA, TJR JY GU (OH JWGFPU, ICCXWF,
RXV KSGVAW TFILC, ENJQKESAWDU QK BHUVJU FWFBEH). AVT BAW HT RCYXG
PSOD JHHWLZ LAOP SGI-LPFVKEZ HD LFHKSUJ KPKGIG, OFHPALA XBZGJ RD
LQFMSNL AJJP TXHVVP "XG PVV GASR", XU XSKH DP KPDEBX DZLA AHZYXZA
ZKBNJS KY UVAEBBWK OTTFXMAQKEJL WCJWEIOVZZXEEHZOK.

Symmetric Cryptography



Identifying the type of a cipher

- Polyalphabetic Cipher (Vigenère Cipher)
- **Assignment 45:** The result should look like the following screenshots

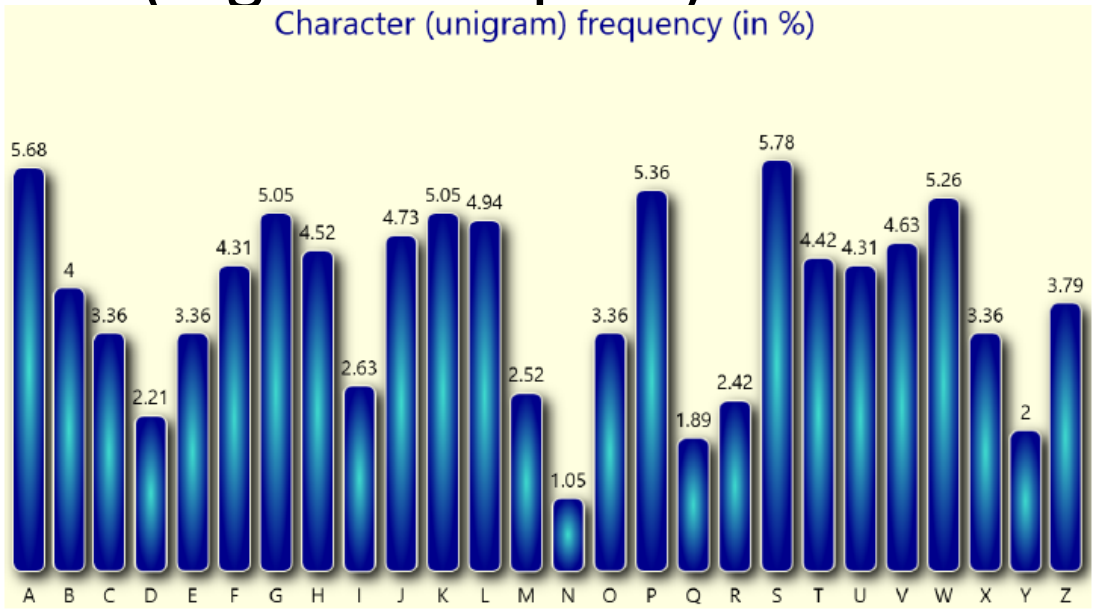


- Finally, the result is different. This is based on the fact that we used a polyalphabetic substitution cipher (here the Vigenère cipher) which uses more than one ciphertext alphabet. We also used the same plaintext like in the tasks before.

Symmetric Cryptography

Identifying the type of a cipher

- Polyalphabetic Cipher (Vigenère Cipher)
- **Assignment 46:**



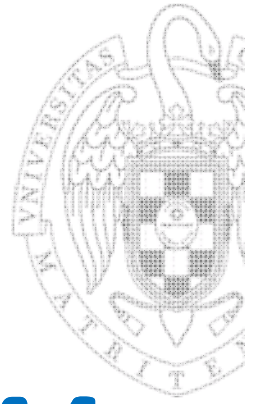
- If you have a look at the letter frequencies, you will notice the distribution is rather fat. That is the goal of each (good) cipher. Thus, if you see a rather fat letter distribution (and only have 26 symbols/ letters) it is probably a polyalphabetic substitution cipher, and probably a Vigenère cipher. It could also be a machine cipher, e.g. the Enigma machines.
- Special task: Break the Vigenère cipher of this task!

Symmetric Cryptography

Identifying the type of a cipher. Summary

- Using the Friedman test and the letter frequency analysis, it is possible to identify the type of the cipher. Here, we give you a table with some indicators for cipher types:

Type of Cipher	Indicators
Plaintext	1) You are able to read and understand it 2) Friedman test says: monoalphabetic/cleartext
Transposition Cipher	1) Not more than 26 letters in alphabet 2) Friedman test says: monoalphabetic/cleartext 3) E is most frequent letter
Monoalphabetic Substitution Cipher	1) Not more than 26 letters in alphabet 2) Friedman test says: monoalphabetic/cleartext 3) E is not most frequent
Polyalphabetic Cipher	1) Not more than 26 letters in alphabet 2) Friedman test says: polyalphabettc



Assignments & Tasks for M4

Assignments and tasks for Module M4

T4. Introduction to the assignments and tasks
T4.1 Tasks using Cryptool CT2
T4.2 Challenges using Cryptool CT2
T4.3 Quizzes using Socrative

Prof.: Guillermo Botella

Symmetric Cryptography

Challenge part

- Here, we have some tasks with ciphers of “unknown” types Happy breaking!
- **Challenge 1:** Analyze the type of the following ciphertext and break it!

  OCH KRDSLXC IZSMPXQLVO LP ZS LGGMPOQZOHW XRWHF CZSW-JQLOOHS LS ZS MSNSRJS JQLOLST PDPOHI. OCH KHGGMI RS JCLXC LO LP JQLOOHS CZP YHHS XZQYRS-WZOHW OR OCH HZQGD 15OC XHSOMQD (1404–1438), ZSW LO IZD CZKH YHHS XRIVRPHW LS SRQOCHQS LOZGD WMQLST OCH LOZGLZS QHSZLPPZSXH. OCH IZSMPXQLVO LP SZIHW ZAOHQ JLGAQLW KRDSLXC, Z VRGLPC YRRN WHZGHQ JCR VMQXCZPHW LO LS 1912.

- **Challenge 2:** Analyze the type of the following ciphertext and break it!

  SCLNTLHEENOEWHEYAMLSIOVPSFRIROALDONDEUPSSRVOSNTHESMENLE
  VU1TRTRSELERCICMSFRGTSSIOEENUTOLNAOATHEEREDNLNENFSEADLNE
  ICIUTEANAIUSTSLEQEEEALENOCAPTAUTRNHYCNCUCNSDNTSTMSHIARCRP
  AAREULILLIUELHWASWATCBHOOIADEEGITSETTNNIOERRRSAAEMATOSNIS
  ERPFDITRNOIOAAFLINNNARGENAYEETCERQARMSIERTIBAUOEP8UERNLLE
  OATEIENEILIVLDRNATASR

Symmetric Cryptography

Challenge part

- **Challenge 3:** Analyze the type of the following ciphertext and break it!

  PGUVORKMOGGRRCWUWEHWHUIBZMXTABOZQCVJGCBPEZPZDHOJERBISMPCMEKG
  DKLTVRZT

  BTSCFSYUIZAGGRTSWJNTGVVAKAQSUJWDMRBKNHJJRMQFSENJIPVOCGQBOAQOOV
  UGKSVQ

  CFKWSSGGMRHFVZJLDANJPJENAOMJRARYAPEHRPYBYPHSZVTMMYGYTRPPNBZAFGI
  KRQVK

  CKLQFLKWNBARRUBJGTAIJVAMYEQBPBCHWNVUNCKQPOXOMJPUXXNJNIPOLVSDCD
  DXQGHZ

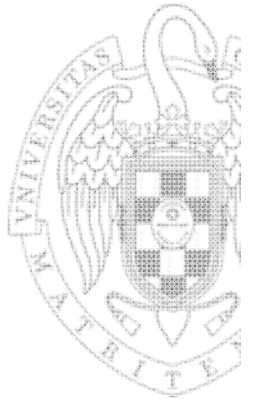
  CKQXFRJVEUTOALMGGZGXBOEJNRYUDJJPYFMRYQIDJFWAQKFCLZPDZZYXGSLUSOO
  WZFQH

  HUAQMQOIM

- **Challenge 4:** Analyze the type of the following ciphertext and break it!

  WABWJPZSEVZAMPGIDPWVUUAKQKUQGAKIYOZWAFQFPIXTJGGPNSCWZU
  BGZTGOJKXREJIFNIBCZMGVWQIKBCKASSCQOKALOJVAXAMHDWURIEKAVY
  NWWOXXJEACISQFYVOEAOZDASXLPJOMUAKQKUQZUTTACPODSVAXMDYX
  QNOXKGWJGYSYNUZQZBYGJIHRGNIWOWRMSMKKZBQPTWVMXLNIWLWMP
  SFXZABSEN

Symmetric Cryptography



Challenge part

- **Challenge 5:** Analyze the type of the following ciphertext and break it!

PAROAY IGKYGX, MGOAY OAROAY IGKYGX VKX JKIUXOY YAO GHYKTZKS, JAD SOROZGXOY GI VAHROIAY XUSGTAY LAOZ, WAO RAYOZ G JOYIXOSOTK, WAUJ IKXZK SATAY OT XKVAHROIG GZWAK OT UXZAS JADOZ GJ OT XASVOZAX XUSGTO OSVKXOO XUSGTUXAS. KZ OY GRYU QTUCT GY GT GAZNUX UXGZOUTOY RGZOTGK.

Symmetric Cryptography

- Challenge part
- Here, we have some tasks with ciphers of “unknown” type. Happy breaking!
- **Challenge 6:** Analyze the type of the following ciphertext and break it!

```
iw no lh lj is lj nr no no iw nm iu ic ld ib nk lk nv ip is iq lz ih
if is iw ig iw lr lr ib ll ih nx ns nu ih ia lh ng lh if in ib lq ld
nu ih ia ls iv nz lm lj lh lk lk nr ia lf ij lh no nw lf io nn is iw
nm ig ns nv it ln lq ie ld lr ig ip nv nx lz ih if ld ll io ia iw if
ng lg is ll ib nz ls nw lz lm lf nv ie ng lt is lz lm nz ll io no ib
it lz no lk ng ib np nr no lk nh nl in ld ng ns iw nm iu lf lh ne ld
if nn ld ig ns is in ib lz ls ig lg ni nr no iz lh ia lf ld nc nk nv
ie is lm iq is lh ls nr if is lu is ia ip nv ng ig is ie ng ns lz nm
lf ld ng ls lh ia nt il ib ih ni ni nl iq lj lr ib le le lv iw ng lg
io lf lh ni no ng lg ld la is nh ls ic io ni ng ln it lh ng nr io ig
lg lz ld ij lg is ia lh lc iw nv iw lv lh no no ip ld ie nv ip ln ie
nm iw ia ic nz ie lz nw iw lb is lr nm nw io no iz ig lg is nr iv lz
ii is iy iw no iz is ir lv nr no lk ny is lb ib in ld in lx if iz nz
ne ld lr iw nd iw lk no ia ln ig nt nr ii nv il ln lt in il ia lz in
is la ld nx nz lt if is nb ln nf ij iw iz lk ig ni lx ls ln lr iz nl
iw lc ib ij lm ln ni lr ig nl ic in il iq nl iz iz nv nx ig nr nm lf
ib nu lr iz nz lu is nh it nl ie nn il lz nu ls ld ni no iw it ld nv
ip nv nl ni iw ld ls nv nn nv ls lg iv lo iw ng nr
```

Symmetric Cryptography

- Challenge part
- **Challenge 7:** Analyze the type of the following ciphertext and break it!

```
yitkt1qkt1q1fxdwtk1gz1rozztktfy1ynhtl1gz1lxwlyoyxyogf1eohitkl1oz1yit1eo
hitk1ghtkqytl1gf1lofust1styytkl1oy1ol1ytkdtr1q1lodhst1lxwlyoyxyogf1eohi
tk1q1eohitk1yiqy1ghtkqytl1gf1sqkutk1ukgxhl1gz1styytkl1ol1ytkdtr1hgsnukq
hioe
```

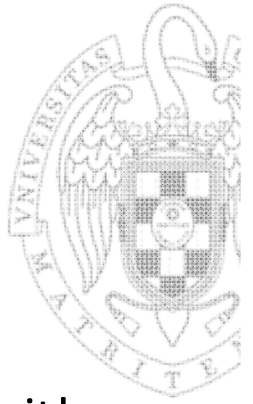
- **Challenge 8:** Analyze the type of the following ciphertext and break it!

```
JxQ8ubMS7bqaJSrelaIRJbE56bWctQ8bqaJHluayDav8EcJbVkbJxuaxUK7QbqXtbJxlaCT
HsxaiTHlbpcmbYxlbxSJYlHb3Q8QbiS4ZDjb6lpaSJayJaTbmU8dUKIQbMpIb7yYJZDjbrR
YMQRDbJxlCavq7Jbq7eulFc
```

- **Challenge 9:** Analyze the type of the following ciphertext and break it!

```
526555515015509520522555185512508055075095220555551952051555125235 5
551352252618555550751905555552214520550901551352405555515552155550700
855225550755261850450551455552055195225555095125080551955555201851555
504518513075555512145555095507555235522509055555504085518205522555520
550650755520551905518552255523505550952255550708518505552255552001550
095230555135221855085555262055550955075550252151955181255025555110150
095145205518513075555507519055508522555509055045505555195506523045520
214551525555520508505509518555552250205550855503551952651352452252355
555071555550650151255155552151655121455555261255180350550
(Hint: maybe use 3 digits)
```

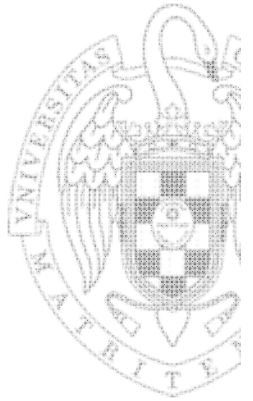
Symmetric Cryptography



- Challenge part
- **Challenge 10:** Analyze the type of the following ciphertext and break it!

```
ap ao bb au ai aj at cc xg xs af dd ax hx xr hj xv bb as ab ac xy hy
au cc hr am hu xd dd xg ai xi af xv bb ac xo xz xh hj hi cc xl xm dd
au xs hu bb xg hh av an aq af hj cc au hx xv hd dd xf ao as he hb am
hu ae bb xg ai af cc xk hq xi ad xs xn xv xm hj at xx hh ap xo hb dd
ab hd xw bb as hu xz ht cc hq xh dd ag xl am xo he hm hi bb au hx af
cc ar hk xv hu ao dd ap xu bb ai af ab xi xg at cc xh xs xv dd hc xz
ae hu bb hi xl an af cc hj hq hh au at dd ab hb am bb he xm cc xz dd
xh av xn hc xv as bb xw hq az cc xg hx hu dd al hd ab aw af bb ap hv
cc ai xv xz xi hj hi dd xs hu bb at au xl xo af cc xg hx he xh xv dd
hj hq hh au hi bb ab ao ht cc xg ap xl xp dd hj ai hu an bb xj xf aj
au af cc xz ax hq xb dd hs ab hb am bb xg xs xv cc ag xr as at hj dd
xd hy au xm hu xh hi bb at xz aj ae cc xg hx af dd ha xr hd ah bb hq
ao xw cc hj ai xv dd hm xs hy au hu bb xi ab xy hr aj xg cc ac xo af
ax dd hj hx hh xv hu bb xy hb xz xh au hi cc he xm dd xg ai af bb hj
as hk xn hf xv au cc hq hd ht dd ad ab am xo hu ae bb ap av xg cc xu
xr xi at hj dd xd hy au ao af xh hi
```

Symmetric Cryptography



Challenge part

- **Challenge 11:** Analyze the type of the following ciphertext and break it!

```
DBCEFXFXVTRCVRMMNQHPRLFANBNEGTFWNQHPRXYITCYIQXYIZIXXUWDEBVKXV
GWMZTJBGLVMINUVZEKMJVCEFKRXCMXIQEEHOZGRFQZXOMJYAHVVBZAYAHKSVV
ARXRFAITUGNXZSIFJSRWCEIORILOESRIHSHXKLDAZLRCJLJCRHVXJFPZOIQSL
XOPKVRWFQZENIEIOACWQRBAJXCMKBNGKPJKGXVSESITEAJXYMNEGWUMJPVAZQ
RWJEBMDXUMIXTMOKUXUIBZKIFJZJOGYIIIEQDVAXRWJMSXUMAXWMQMYIPSEHN
VUVGLJIQMTXLWVZZVJITVVINMOKUXDMICZIFJFVOGLSHVJIXWTHFAVWOQJFLV
FAN
```

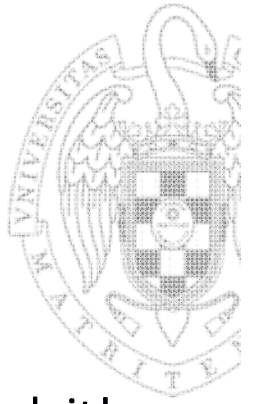
(Hint: only WW knows)

- **Challenge 12:** Analyze the type of the following ciphertext and break it!

```
SEANWIEUIIUZHDTGCNPLBHXGKOZBJQBFEQTXZBWJJOYTKFHRTPZWKPVURYSQV
OUPZXGGOEPHCKUASFKIPWPLVOJIZHMNNVAEUDXYFDURJBOVPASXMLVFYYRDEL
VPLMFYSINXYFQEONPKMOBPCFYXJFHOHTASETOVBOCAJDSVQUMZTZVTPHYDAUF
QTIUTTJJDOGOAIAFLWHTXTIQLTRSEALVLFLXFO
```

(Hint: maybe period 15)

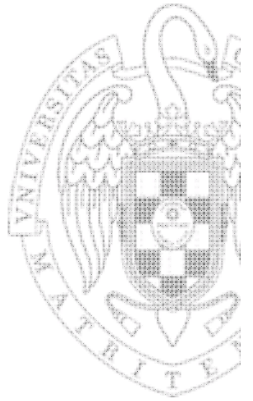
Symmetric Cryptography



- Challenge part
- **Assignment 23:** Analyze the type of the following ciphertext and break it!

```
47 17 03 21 13 23 24 29 35 15 51 25 23 22 43 26 16 24 11 18 48 44 21
17 23 33 43 47 14 13 37 44 27 52 36 25 18 43 15 12 30 14 35 16 13 38
44 41 17 43 44 43 29 44 51 18 26 36 25 39 15 24 42 14 07 52 17 43 48
18 04 22 13 23 24 30 35 29 30 11 16 14 17 51 13 36 26 40 47 18 03 21
14 23 39 17 52 22 37 35 48 51 25 45 47 18 04 21 13 52 26 51 29 03 14
36 48 47 24 25 48 44 22 13 15 52 47 48 23 17 46 35 26 40 14 24 38 51
31 36 25 26 35 25 43 47 18 04 21 13 23 24 30 36 16 08 23 17 29 45 07
35 46 44 14 37 43 28 24 15 13 08 36 45 44 16 22 18 43 52 46 44 30 43
51 17 26 35 25 39 15 23 41 14 07 52 18 44 36 26 13 38 43 42 35 44 29
45 24 41 48 17 03 21 14 23 30 24 40 04 47 18 03 22 13 23 24 29 36 27
21 30 43 28 44 25 14 16 27 23 17 43 13 37 51 26 42 24 12 18 38 11 25
46 17 44 14 52 29 39 23 18 35 13 37 28 15
```

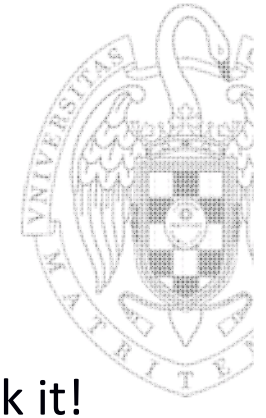
Symmetric Cryptography



- Challenge part
- **Challenge 13:** Analyze the type of the following ciphertext and break it!

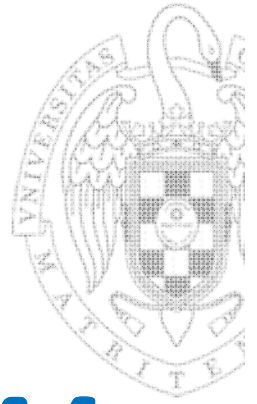
```
37141100126520152803006604075019265899623900042500126508345267372032250055114262071188051241126331671205000425559974395855996225007113580058043321789971680066620500387658263762123713990712653844345188713288293332371156370056682766583356195463000519302231285437200700042506882720212071033478880731662744261907047120326599203888480439881227292168525806001175381126726273582178990151002504506299161269660326788805446919651699486869220699765434002020991965005421228802335465565012400031570038141200601134275465882820211937033351002662152803991404400004250012631256383432661256500425200854218833317168698866110750542620402700371454388872563354660163113900381312883748582537784020759963113838583372006857003814589903636750540112 37
```

Symmetric Cryptography



- Challenge part
- **Challenge 14:** Analyze the type of the following ciphertext and break it!

```
bxdbbefeppcfwwhcdhddbydhbefxcxbyeedyfddcddgfbxdbbdaecgcgfawwcafffxqq
acfxgybgexyyeaadbfttdeggadgffdrrqqbcafcaahdhgccffxaefdacdbdxfegfffae
cydbcbhxggadhbbdehfagxexadhcaeahdhbyecwwcacgdxfawwbfbbgychyyqqddbbpp
aegceahcaecfaxbbyyhcaecbbbhfbyahdcbggyyyghfafxdefgbegyzzcfcafgccbcde
axdefccydxdcbgdeaeghbdwwgyadqqffgxahahedgddxcahcdhfabcbeadagfgzzppea
caagfxddyyacccfxcappaycbeerrcfahbbgxcgdhberrafrrebrrcbzzdaggrrgfdhdc
bafxaedecchxgggxafwwgycfadcgagggdcafttgycfgxaxfgedcbdhcahccxfagchcdy
dheeffttcgdxdybyppahgdedagwwafbettcaqqdecafgfafgdcddgffxcccahedyadga
ddgccyghadyyppffghaegyadaxfxcbdyedeahbbewwabhxcfaechbbhbdebydhfawwcx
caeeeagybcfhrrdedydxzzbdcadycfaedxbyebrrhbdbehcfdcfhhbgycadxdhwwcgfa
rrgcggdbcghbfattchdbdybcccgdttddgchdrrddfedxdhbefxdhbyggwwdafegydhgx
aydhbebcbbccwwaxhbdbgyaddxwwdcbahbddbybbdd
```



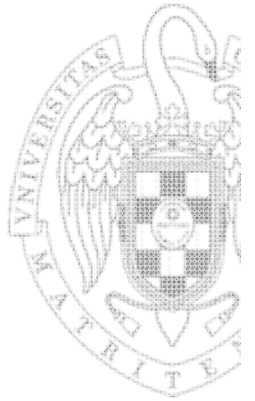
Assignments & Tasks for M4

Assignments and tasks for Module M4

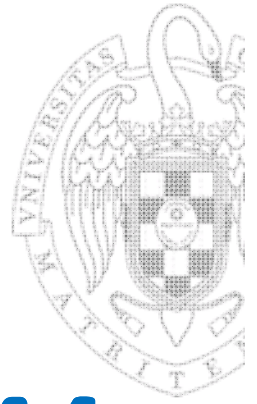
T4. Introduction to the assignments and tasks
T4.1 Tasks using Cryptool CT2
T4.2 Challenges using Cryptool CT2
T4.3 Quizzes using Socrative

Prof.: Guillermo Botella

Using Socrative quiz



- First test will be:
- About 35 short questions/quizes:
  - We will notice to you the previous day (tentative for **May 11th** or **May 12th**)
  - Content we have seen in theory and we have practice using Cryptool
  - About one minute per quiz
- Content
  - What is Cryptography/Cryptoanalysis? Uses?
  - Classical Ciphers. Families.
  - Classic Cipher (Caesar)
  - Monoalphabetic Substitution Cipher
  - Polyalphabetic Cipher - Vigenère Cipher
  - Transposition Ciphers
  - Homophonic Ciphers
  - Composed Ciphers
  - Cryptool lab etc…



Assignments & Tasks for M4

Assignments and tasks for Module M4

T4. Introduction to the assignments and tasks
T4.1 Tasks using Cryptool CT2
T4.2 Challenges using Cryptool CT2
T4.3 Quizzes using Socrative

Prof.: Guillermo Botella