



# Cryptology for IoT

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

M4.6 Briefing of the session  
M4.7 Tasks to do in the lab

Prof.: Guillermo Botella



# Cryptology for IoT

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

M4.6 Briefing of the session  
M4.7 Tasks to do in the lab

Prof.: Guillermo Botella



# M4.6 Briefing of today

- Cryptography and Cryptoanalysis
  - Slides and supplementary videos
- We go to the rooms. Practical Session I.
  - Assignments
    - (They will be specified when we start)
  - Work in groups
    - (Same than usual)



# Cryptology for IoT

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

M4.6 Briefing of the session  
**M4.7 Tasks to do in the lab**

Prof.: Guillermo Botella



# Slides and videos

- Cryptography using Cryptool
- Cryptoanalysis using Cryptool
- Substitution ciphers lab
  - Caesar (trivial case)
  - Monoalphabetic Substitution
  - Polyalphabetic Substitution
- Transposition Ciphers lab
  - Scytale (basic case)
  - Columnar Transposition
- Mixed Ciphers lab
  - ADVGX Cipher



# Basic Crypto I

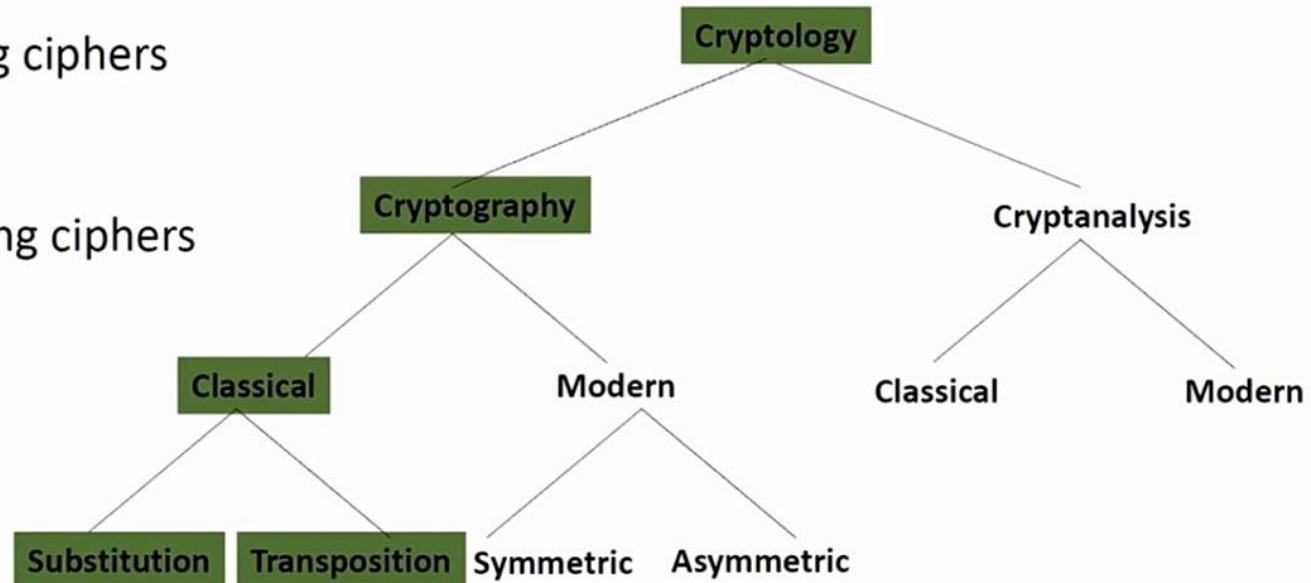
- Cryptography using Cryptool (video+slides)
  - Family ciphers
  - Classical

**Cryptography**

Art of making ciphers

**Cryptanalysis**

Art of breaking ciphers





# Basic Crypto I

## ■ Cryptography using Cryptool (video+slides) – Terms

### Cipher

- Encryption method/algorithm

### Plaintext

- Non-encrypted text

### Ciphertext

- Encrypted text

### Key

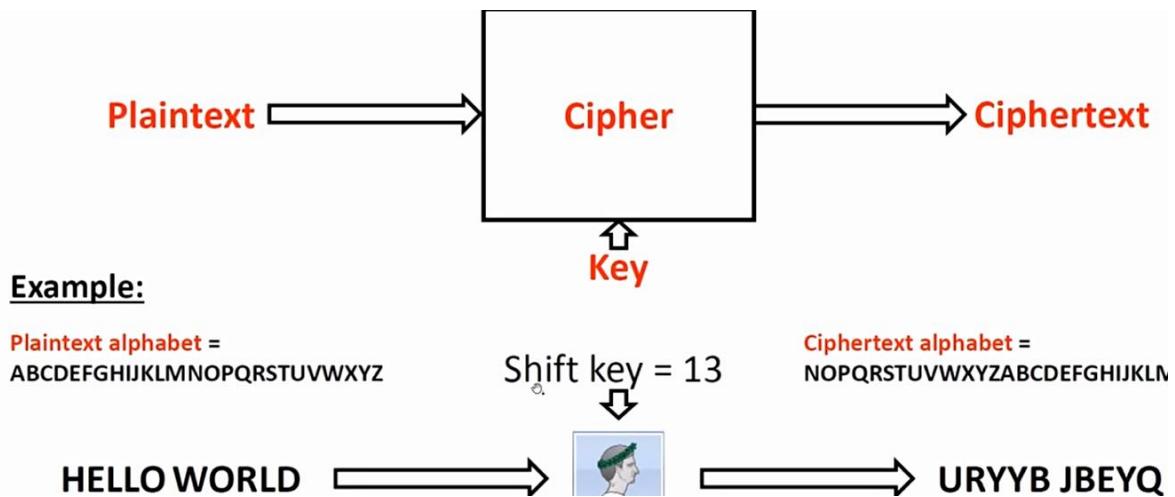
- Secret information used for encryption/needed for decryption

### Alphabet (plaintext alphabet & ciphertext alphabet)



# Basic Crypto I

- Cryptography using Cryptool (video+slides)
  - Caesar's Scheme





# Basic Crypto I

## ■ Cryptography using Cryptool (video+slides)

### – Types of classical ciphers

Three types of (classical) ciphers. Two main types (1 & 2)

#### 1. Substitution ciphers

- Replace letters by other letters (or symbols)
- Examples: Caesar, simple MASC, Vigenère

#### 2. Transposition ciphers

- Change the order of the plaintext letters
- Examples: Scytale, columnar transposition

#### 3. Composed ciphers

- Combination of substitution and transposition
- Examples: ADFGVX, Granite



# Basic Crypto I

## ■ Cryptography using Cryptool (video+slides) – Terms (ii)

### Keyspace

- Set of all possible keys of a cipher

### Keyspace size

- Size of the set of all possible keys of a cipher
- Usually given as (rounded up) power of 2

26

### Example: Caesar

$$\text{Keyspace size} = 26 \approx 2^5$$

Keyspace = { 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25 }  
→ all possible shift keys, including the identity (shift key = 0)



# Basic Crypto I

## ■ Cryptography using Cryptool (video+slides) – Terms (iii)

### Monoalphabetic Substitution

- Only one ciphertext alphabet is used
- Examples: Caesar cipher, simple MASC

### Polyalphabetic Substitution

- The ciphertext alphabet is changed during encryption
- Examples: Vigenère cipher, Enigma machine

### Homophonic Substitution

- A letter is encrypted by more than one letter/symbol
- Examples: Zodiac killer ciphers, historic ciphers of the Vatican

### Polyphonic Substitution

- Different plaintext letters are encrypted by the same ciphertext
- Non-deterministic. Decryption ambiguous



# Basic Crypto I

## ■ Cryptography using Cryptool (video+slides) – Terms (iv)

### Monographic cipher

- One letter is encrypted at the same time

### Bigraphic cipher

- Letter pairs are encrypted at the same time

### Monopartite cipher

- Replacement is a single letter

### Bipartite cipher

- Replacement are two letters

### Example:

The simple monoalphabetic substitution cipher (simple MASC) is a monoalphabetic monographic monopartite substitution cipher



# Basic Crypto I

- Cryptography using Cryptool (video+slides)
  - Substitution cipher → Caesar

And a first example for simple substitution cipher is the Caesar cipher. Just double

Welcome to CryptTool 2. There are two ways for a quick start: Click on the wizard button in the section "Main Functions" to get a guided tour, or load one of the pre-defined workflows in the section "Templates" which demonstrate the program functionality in cryptographic scenarios.

Main functions

- Create a new workspace with the graphical editor
- Use the wizard to easily try some CryptTool 2 features
- Open CryptTool Store
- Read the online documentation
- Open the CryptTool Book

Templates (double click to open)

- Cryptography
  - Classical
    - ADFGVX Cipher
    - Caesar Cipher
    - Homophonic Substitution Cipher and Nomenclature -- Decryption
    - Homophonic Substitution Cipher and Nomenclature -- Encryption
  - Enigma Cipher Machine
    - Fialka ED Check
    - Fialka ED Mixed Mode Check
    - Fialka ED NumLock10 Check
    - Fialka Key Output

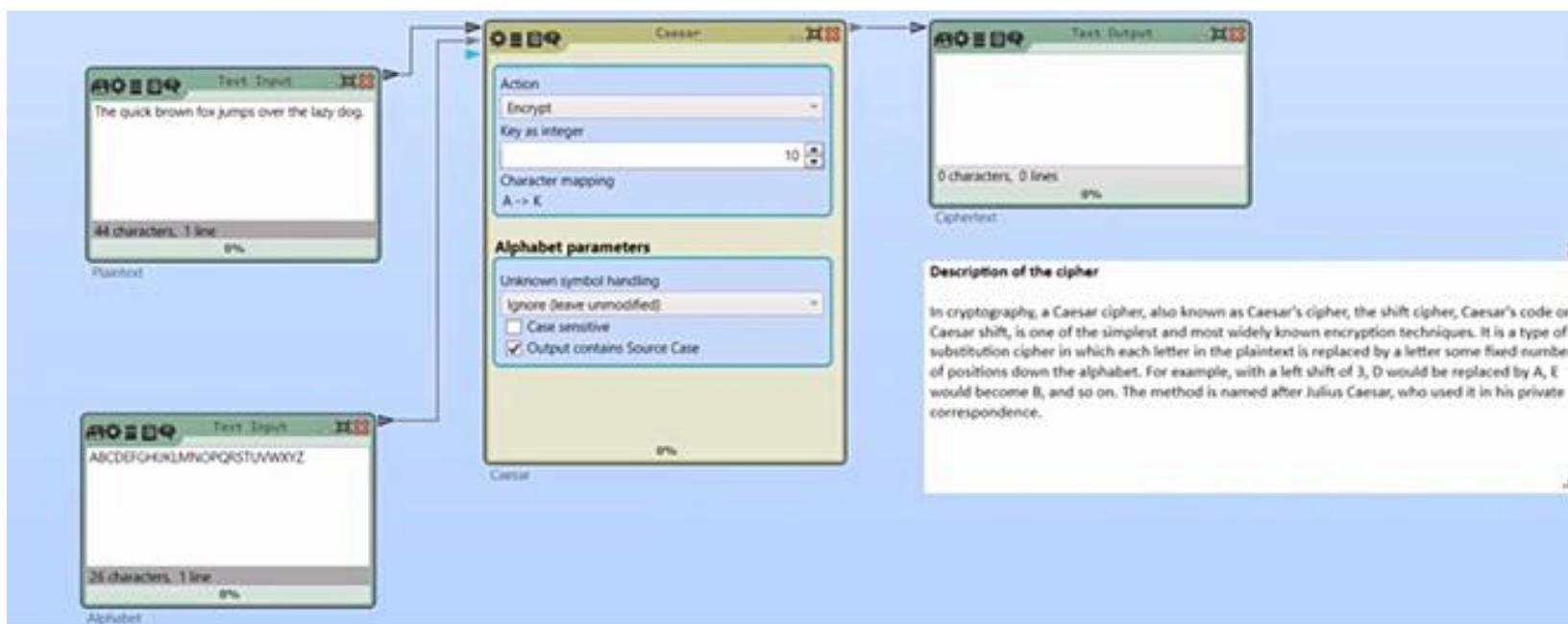
YouTube Videos (double click to open)

- Break the Double Columnar Transposition Challenge (Doppelkürfe)
- CryptTool 2 YouTube Channel Trailer
- Enigma Machine – Part 2 of 2 – Let's break it!
- 08 - Upload Component to CryptToolStore (CryptTool 2 Development Series)
- Enigma Machine – Part 1 of 2 – How does it work?
- Break a Playfair Cipher
- Encrypt like Navajo Code Talkers
- Break a World War I ADFGVX Cipher

Recently opened workspaces (double click to open)

# Basic Crypto I

- Cryptography using Cryptool (video+slides)
  - Substitution cipher → Caesar





# Basic Crypto I

## ■ Cryptography using Cryptool (video+slides) – Substitution cipher → Vigenere

Welcome to CrypTool 2. There are two ways for a quick start: Click on the wizard button in the section "Main Functions" to get a guided tour, or load one of the pre-defined workflows in the section "Templates" which demonstrate the program functionality in cryptographic scenarios.

**Main functions**

- Create a new workspace with the graphical editor
- Use the wizard to easily try some CrypTool 2 features
- Open CrypTool Store
- Read the online documentation
- Open the CrypTool Book
- Visit the official CrypTool 2 website
- Visit the official YouTube channel: You will learn how to use CrypTool 2 and add your own functions
- Visit us on Facebook

**Templates (double click to open)**

- Substitution Ligner
- Substitution Cipher using a password
- T-310/50 Cipher Machine
- T-310/51 Cipher Machine
- Transposition Cipher
- Vernam Cipher
- Vigenere Cipher**
- XOR Cipher
- Modem
- Cryptanalysis
- Hash Functions

**YouTube Videos (double click to open)**

- Break the Double Columnar Transposition Challenge (Doppelwürfel)
- CrypTool 2 YouTube Channel Trailer
- Enigma Machine – Part 2 of 2 – Let's break it!
- 08 - Upload Component to CrypToolStore (CrypTool 2 Development Series)
- Enigma Machine – Part 1 of 2 – How does it work?
- Break a Playfair Cipher
- Encrypt like Navajo Code Talkers
- Break a World War I ADFGVX Cipher

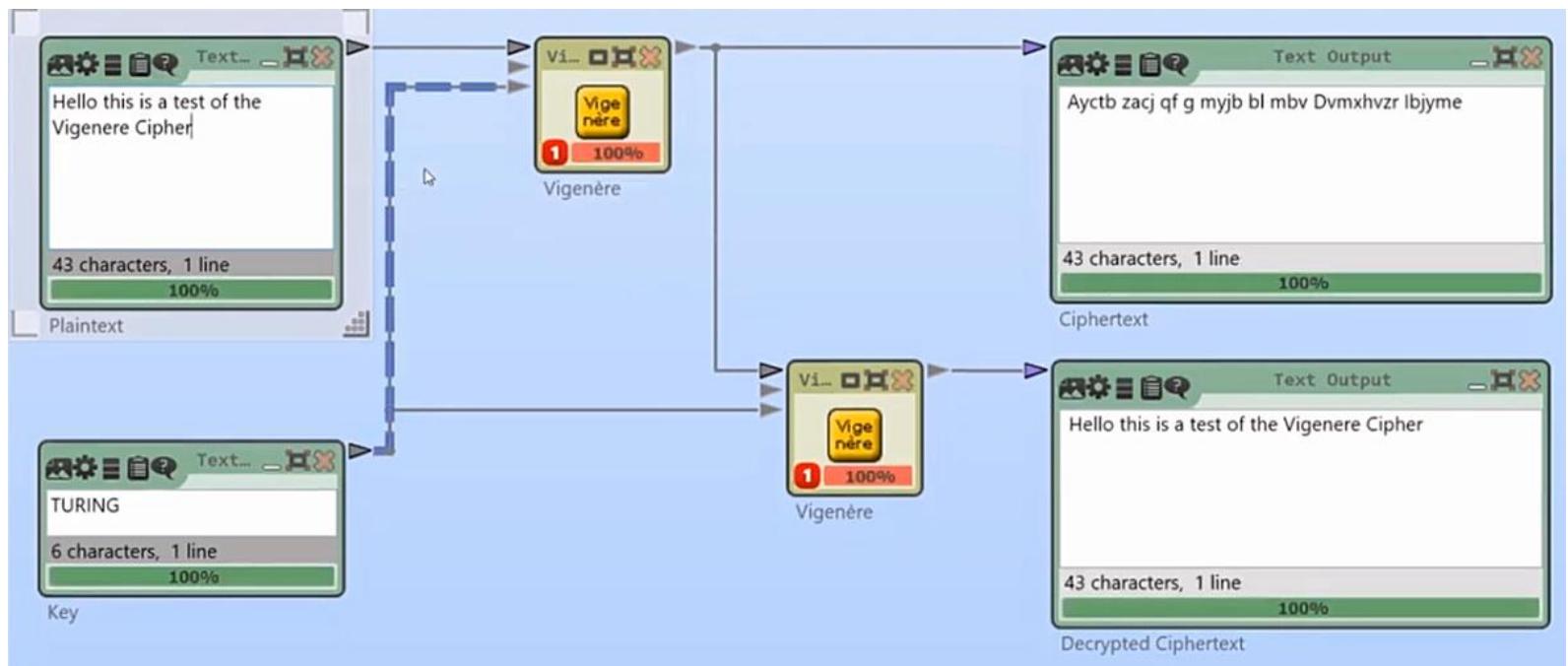
**Recently opened workspaces (double click to open)**

- Caesar Cipher



# Basic Crypto I

- Cryptography using Cryptool (video+slides)
  - Substitution cipher → Vigenere





# Basic Crypto I

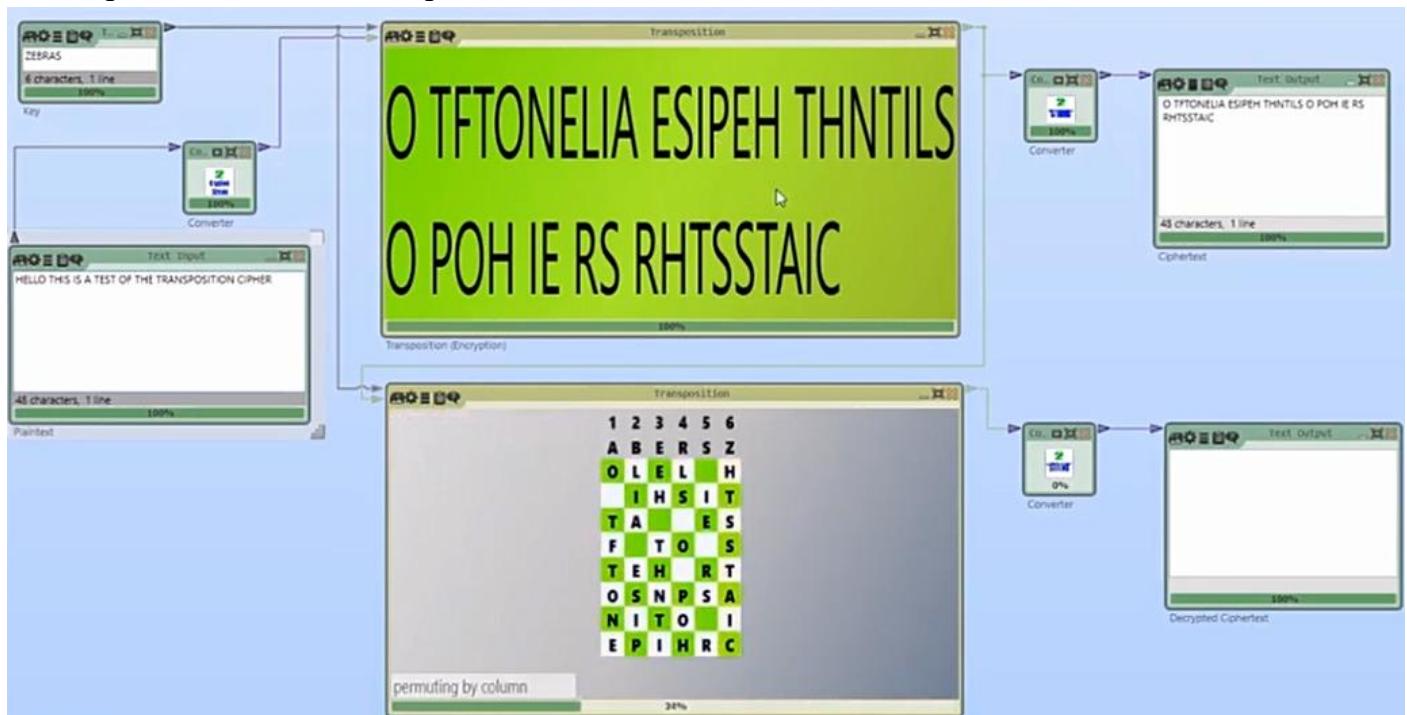
## ■ Cryptography using CrypTool (video+slides) – Transposition cipher





# Basic Crypto I

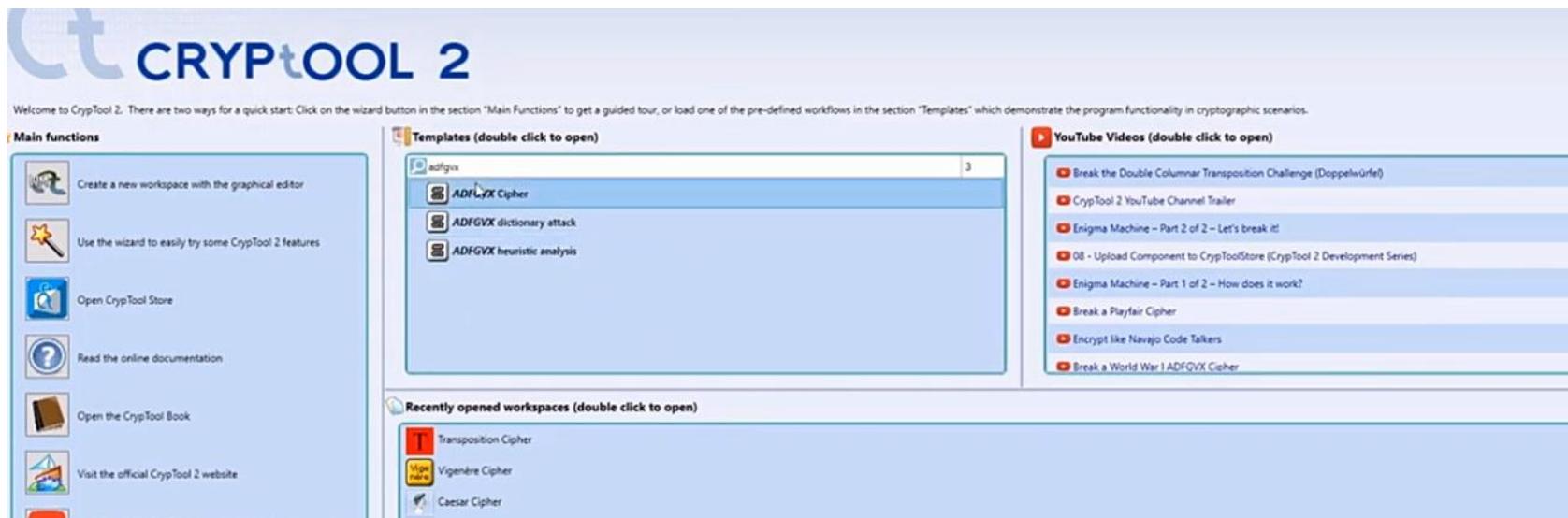
- Cryptography using Cryptool (video+slides)
  - Transposition cipher





# Basic Crypto I

## ■ Cryptography using Cryptool (video+slides) – Composed Cipher





# Basic Crypto I

- Cryptography using Cryptool (video+slides)
  - Composed Cipher





# Basic Crypto I

- Cryptography using Cryptool (video+slides)
  - Composed Cipher





# Basic Crypto II

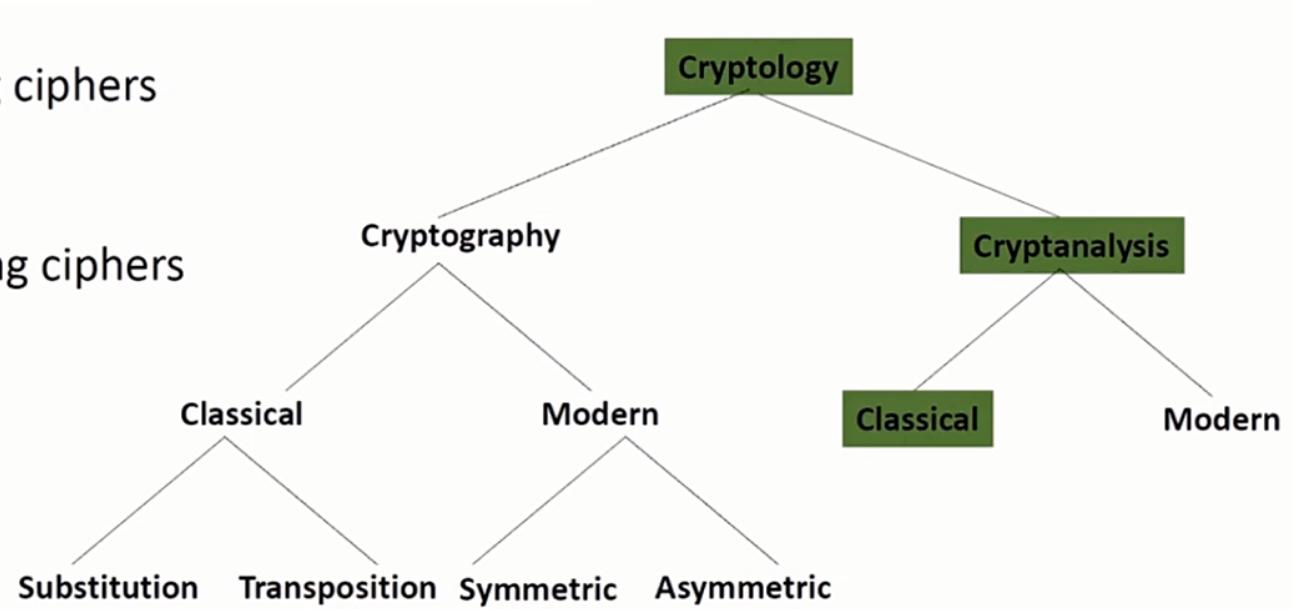
- **Cryptoanalysis using Cryptool (video+slides)**
  - Family ciphers
  - Classical

**Cryptography**

Art of making ciphers

**Cryptanalysis**

Art of breaking ciphers





# Basic Crypto II

## ■ Cryptography using Cryptool (video+slides) – Terms (i)

### Cryptanalyst

- Someone who analyzes a cipher/ciphertext to break it

### Attack

- Method to revert the key/plaintext of a ciphertext

### Breaking a ciphertext

- Successfully performed attack on a single ciphertext

### Breaking a cipher

- Finding an attack on a cipher that works reproducibly on ciphertexts encrypted with that particular cipher



# Basic Crypto II

## ■ Cryptography using Cryptool (video+slides) – Terms (ii)

### Assumption with each attack type

- “Attacker knows the system” (i.e. the used cipher; no security through obscurity)

### Chosen-plaintext attack

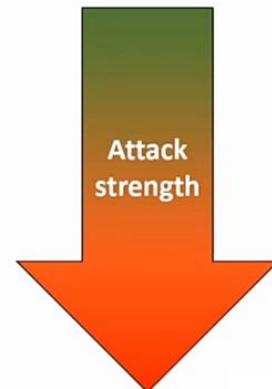
- Goal: revert the key
- Attacker is able to produce (arbitrary) plaintext-ciphertext pairs

### (Partially) Known-plaintext attack

- Goal: revert the key; revert the rest of unknown plaintext
- Attacker has (parts of) the plaintext of a ciphertext

### Ciphertext-only attack

- Goal: revert the key; revert the plaintext
- Attacker only is in possession of the ciphertext





# Basic Crypto II

## ■ Cryptography using Cryptool (video+slides)

### – Terms (iii)

#### Brute-force attack (aka exhaustive key search)

- Attack that works with every cipher (except perfect ciphers, e.g. the one-time pad)
- Attacker tests every key of the cipher
- Only suitable, if it's practical to search through the keyspace

#### Manual attacks (this video)

- E.g. break a MASC by hand using the knowledge of letter frequency distribution
- E.g. cut transposition ciphertext into paper strips and rearrange them

#### Computerized attacks (later videos)

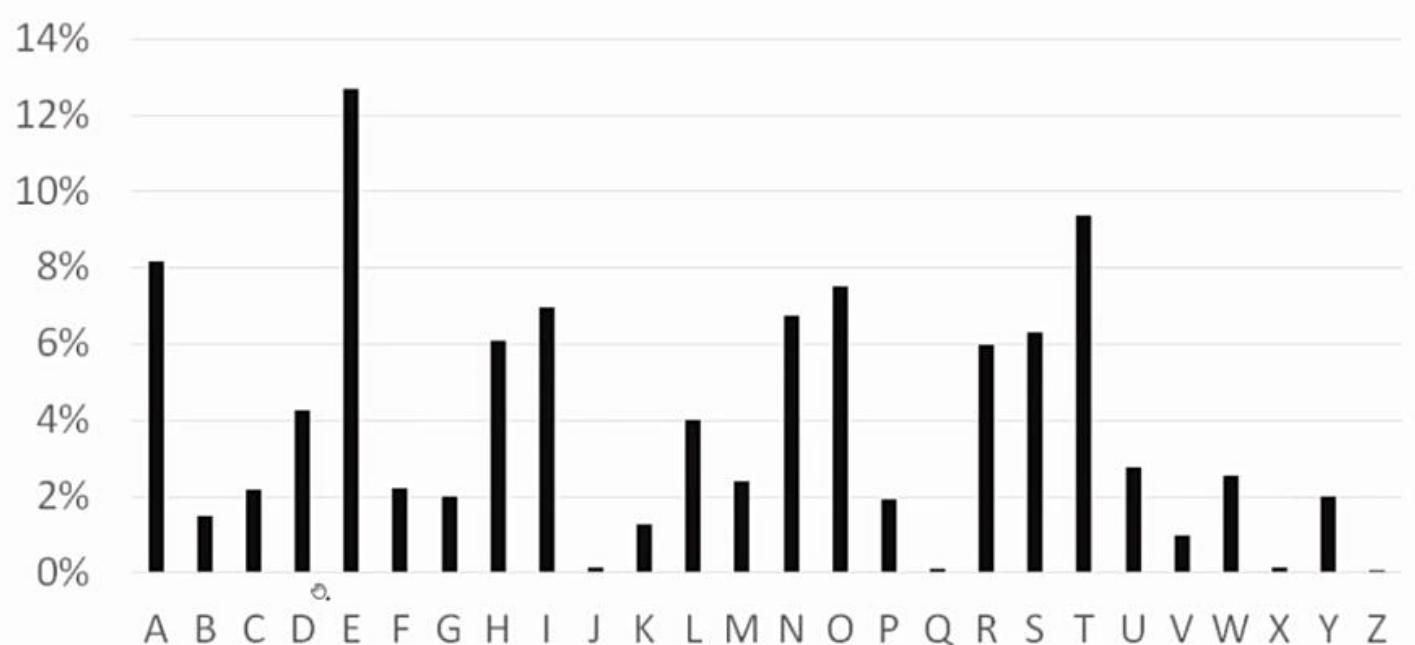
- Implementation of manual attacks, e.g. automated frequency analysis
- Heuristic attacks work on many classical ciphers, e.g. MASC, transposition, Enigma, ...



# Basic Crypto II

- Cryptography using Cryptool (video+slides)
  - Statistic (i)

Each language has its individual letter frequency distribution (here: all 26 English unigrams)

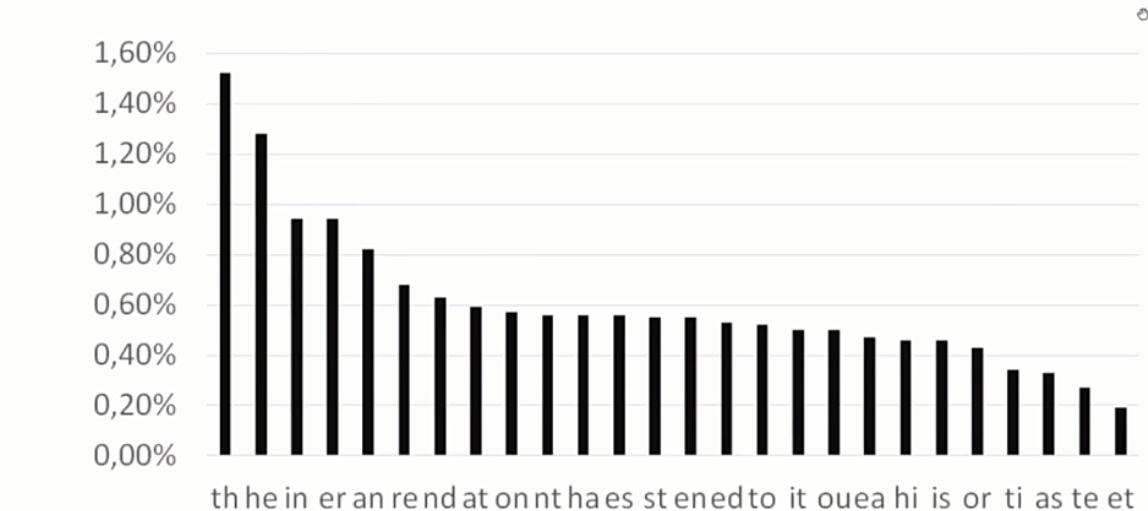




# Basic Crypto II

- Cryptography using Cryptool (video+slides)
  - Statistic (ii)

Each language has its individual letter frequency distribution (here: 39 most frequent English bigrams)

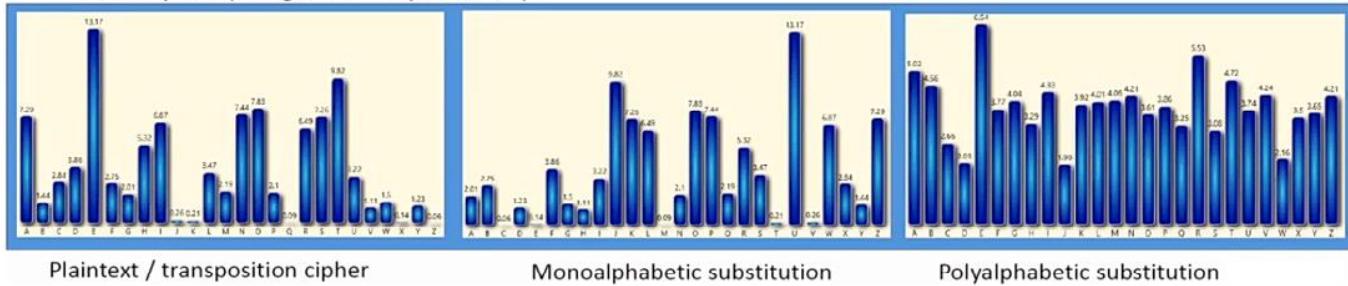




# Basic Crypto II

## ■ Cryptography using Cryptool (video+slides) – Statistic (iii)

- Ciphers try to flat the letter frequencies of the text
  - Substitution ciphers flat unigrams, bigrams, trigrams, etc.
  - Transposition ciphers **do not** flat unigrams, but flat bigrams, trigrams, etc.
- The flatter the frequencies, the more difficult is the analysis of a cipher
- Examples (unigram frequencies):





# Basic Crypto II

## ■ Cryptography using Cryptool (video+slides) – Statistic (iv)

Ciphertext (26 letters) = BUUBDL UIF FOFNZ JO UIF FWFOJOH

Count unigrams

B = 2	D = 1	F = 6	H = 1	I = 2	J = 2
L = 1	N = 1	O = 4	U = 4	W = 1	Z = 1

- Most frequent letter is “F”; assumption that “E” is encrypted to “F”

Look at bigrams, trigrams, and words

- Double letters “UU” may be “NN”, “LL”, or “TT”
- “JO” may be “IN”, “ON”, “AT”
- Word “UIF” may be “THE”; then, “UU” would be “TT”
- If “UU” is “TT”, then “BUUBDL UIF” may be “ATTACK THE”
- Following, “FOFNZ” may be “ENEMY”
- Final solution: plaintext = “ATTACK THE ENEMY IN THE EVENING”

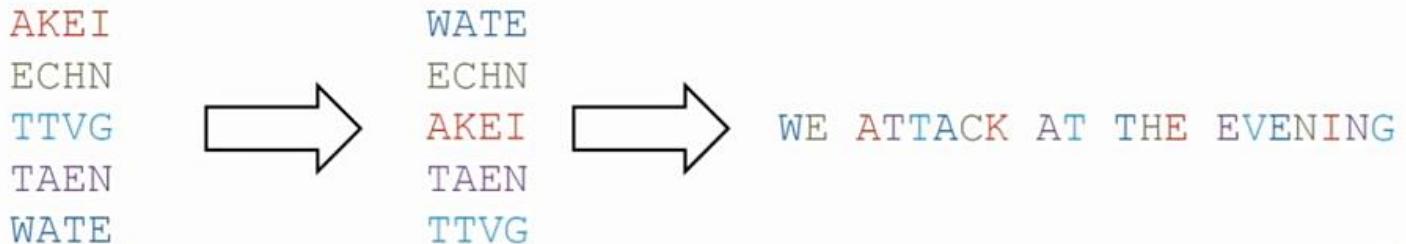


# Basic Crypto II

## ■ Cryptography using Cryptool (video+slides) – Transposition

Ciphertext (20 letters) = AKEIECHNTTVGTAENWATE

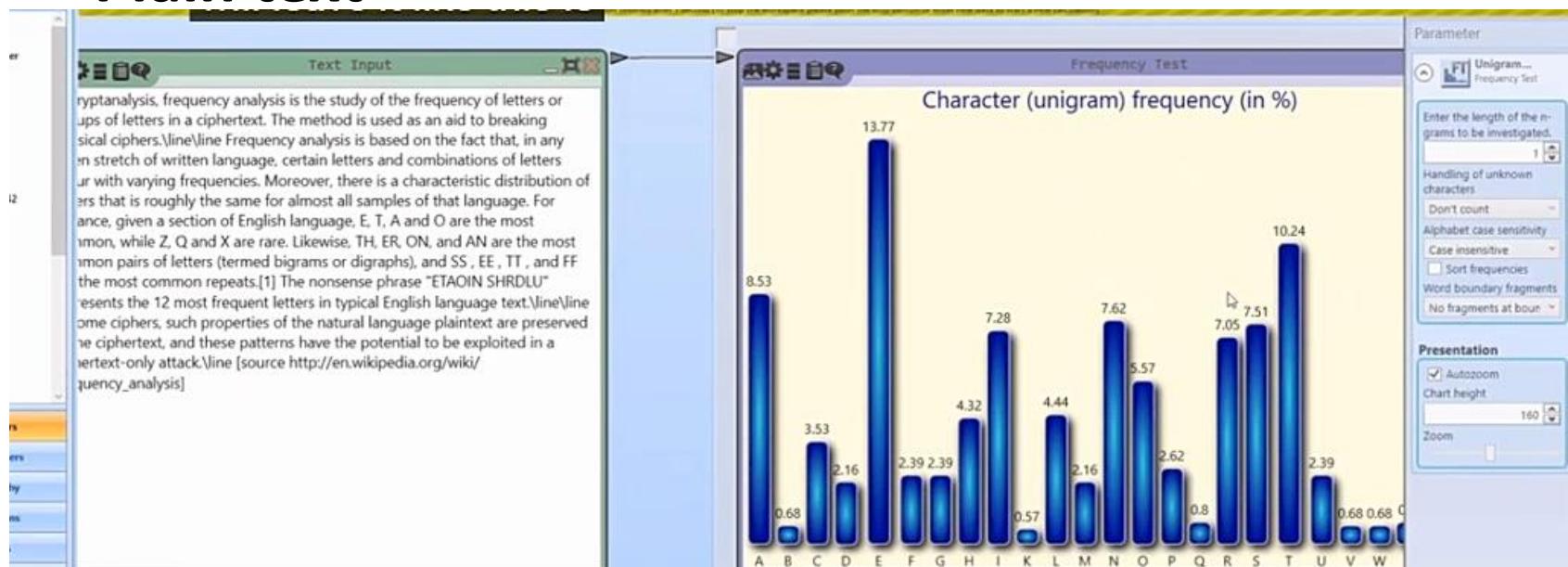
1. Determine/assume key length; we assume key length = 5  
**Hint:** we have a regular transposition with key length = 5
2. Divide text into columns with length 5; i.e. row size = 4
3. Rearrange the rows to break the ciphertext  
we see „A“, „T“ and „T“; assumption „ATT(ack)“  
Also, „W“ and „E“ may be „WE“





# Basic Crypto II

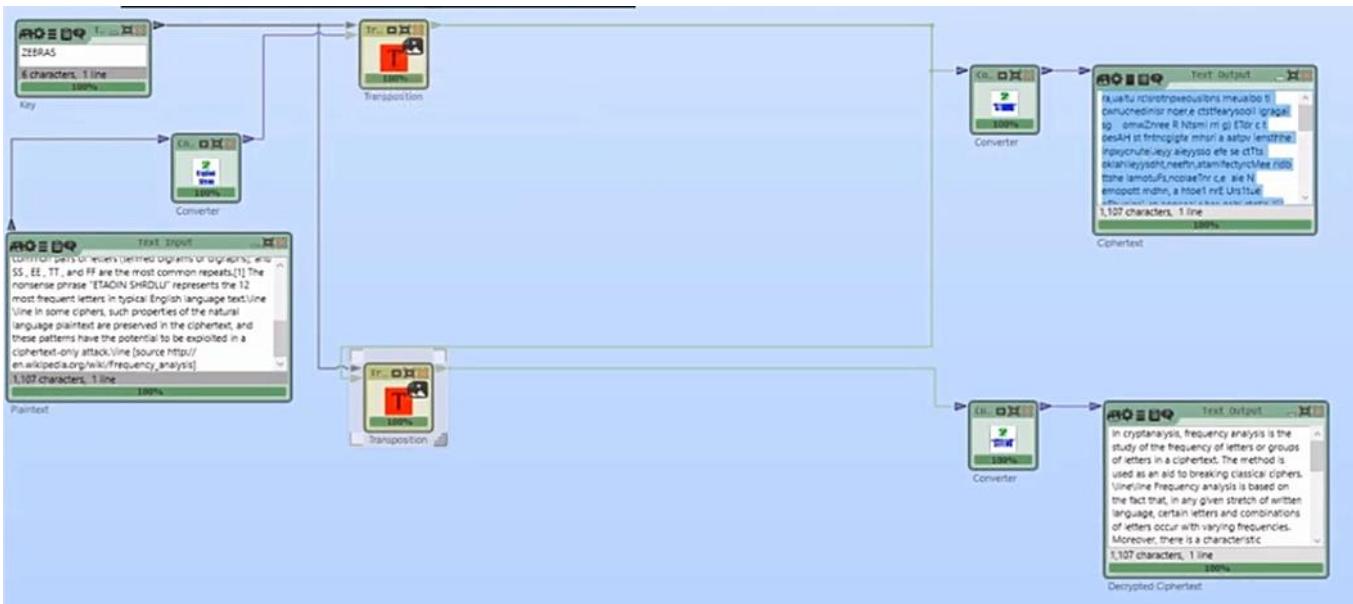
- Cryptography using Cryptool (video+slides)
  - Letter Frequency of ciphers (i)
  - Plain text





# Basic Crypto II

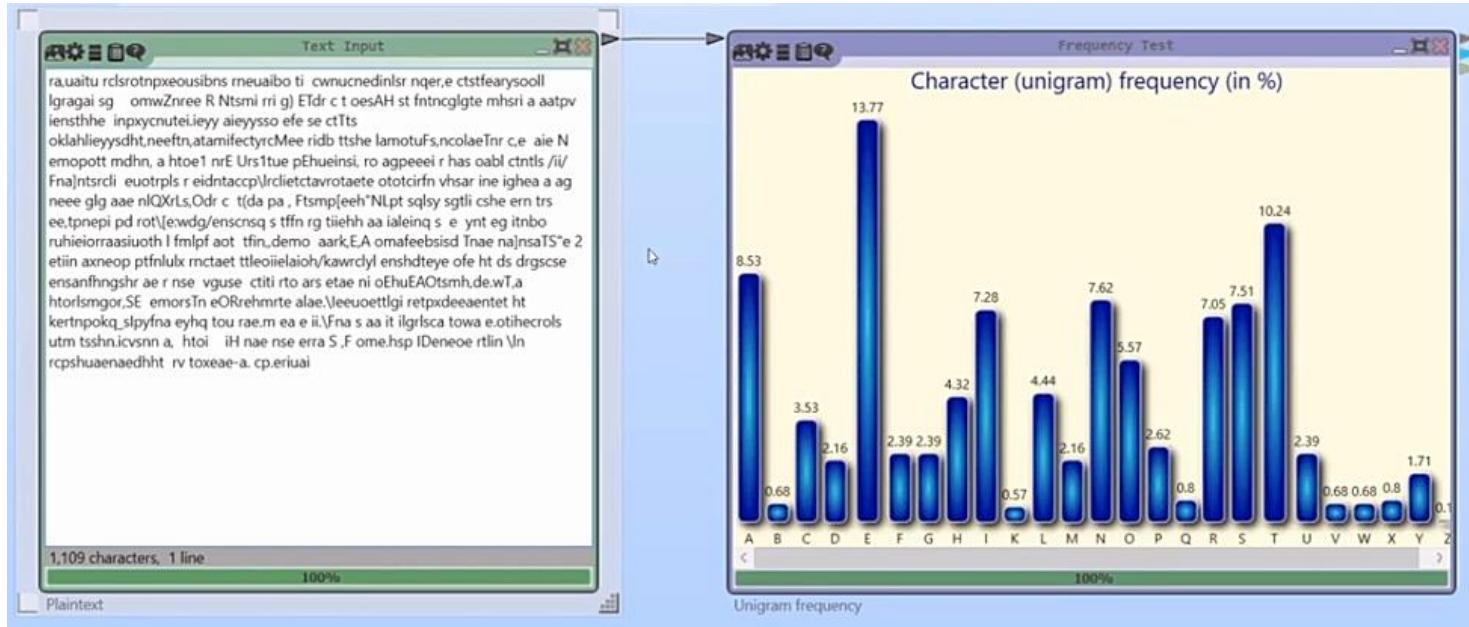
- Cryptography using Cryptool (video+slides)
  - Letter Frequency of ciphers (ii)
  - Transposition (i)





# Basic Crypto II

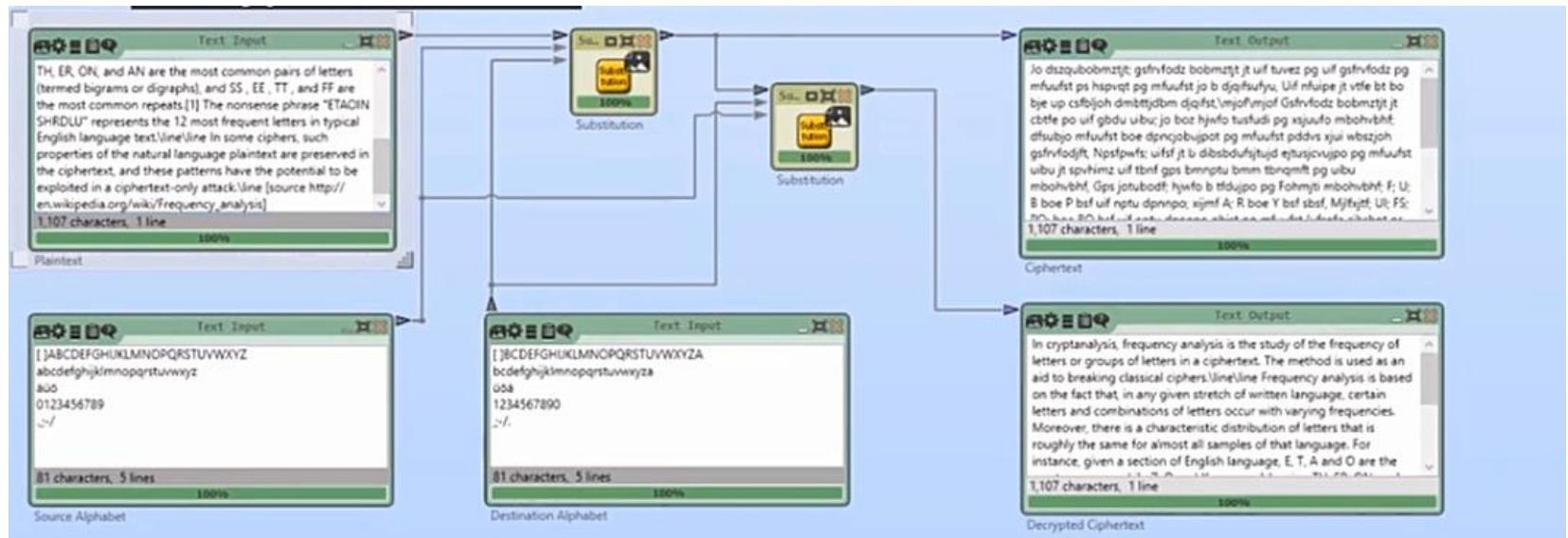
- Cryptography using Cryptool (video+slides)
  - Letter Frequency of ciphers (iii)
  - Transposition (ii)



# Basic Crypto II



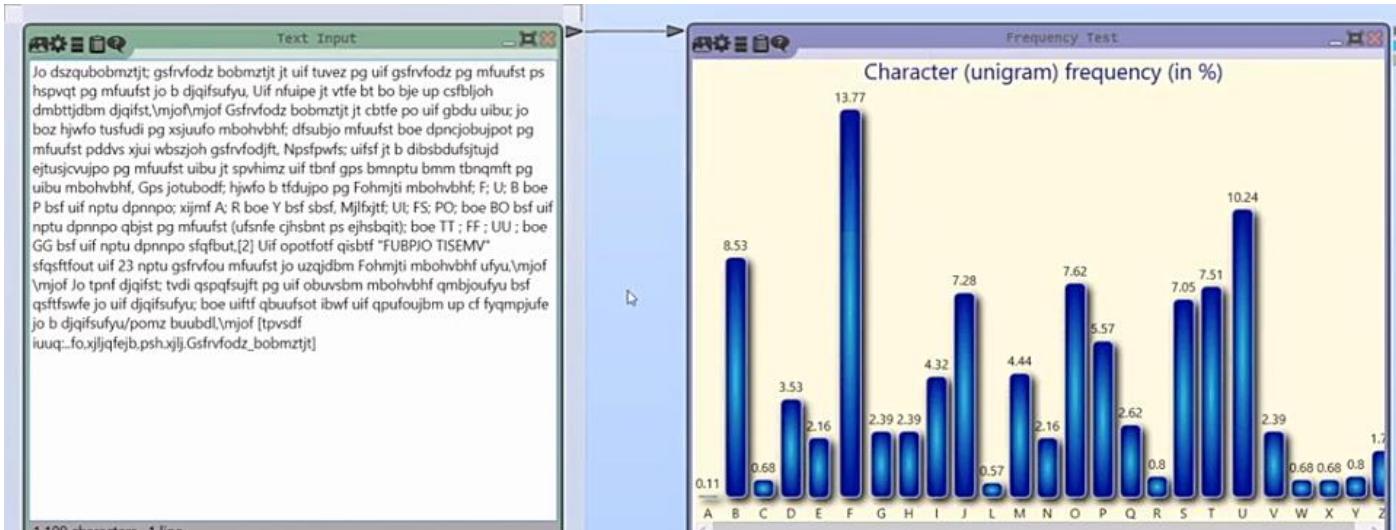
- Cryptography using Cryptool (video+slides)
  - Letter Frequency of ciphers (iv)
  - Substitution (i), no password





# Basic Crypto II

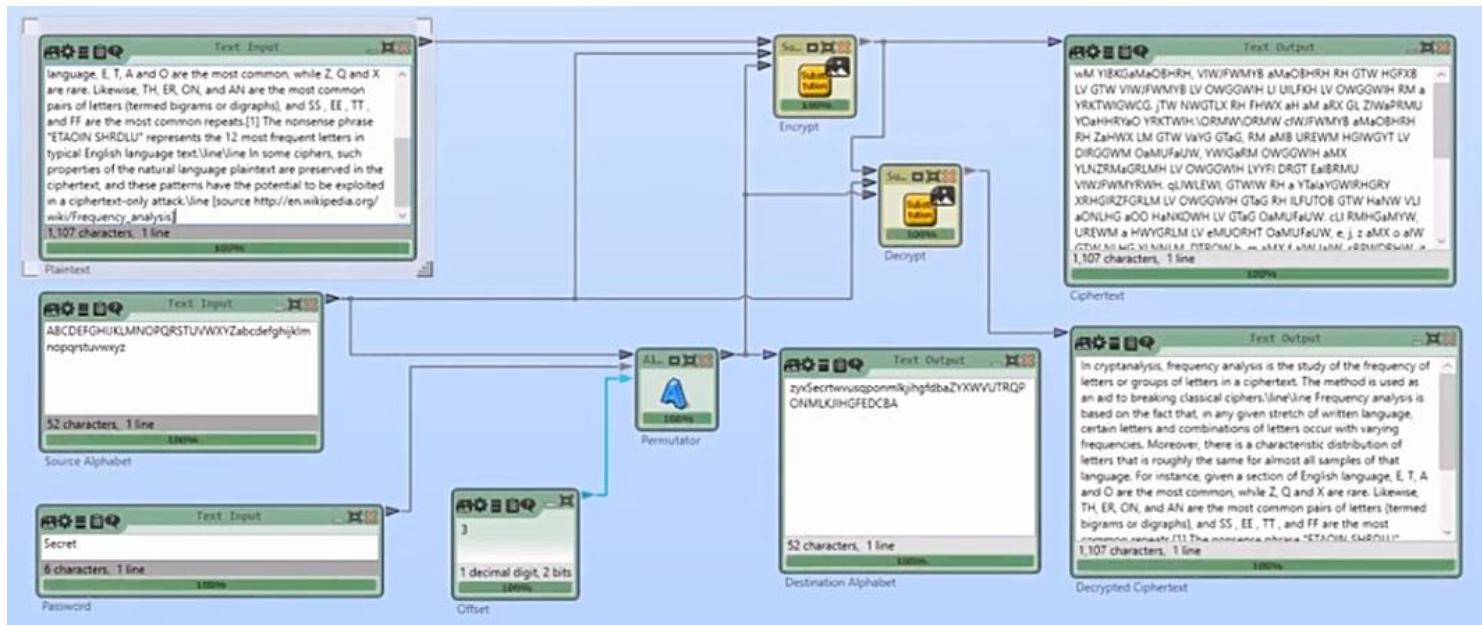
- **Cryptography using Cryptool (video+slides)**
  - Letter Frequency of ciphers (v)
  - Substitution (ii), no password





# Basic Crypto II

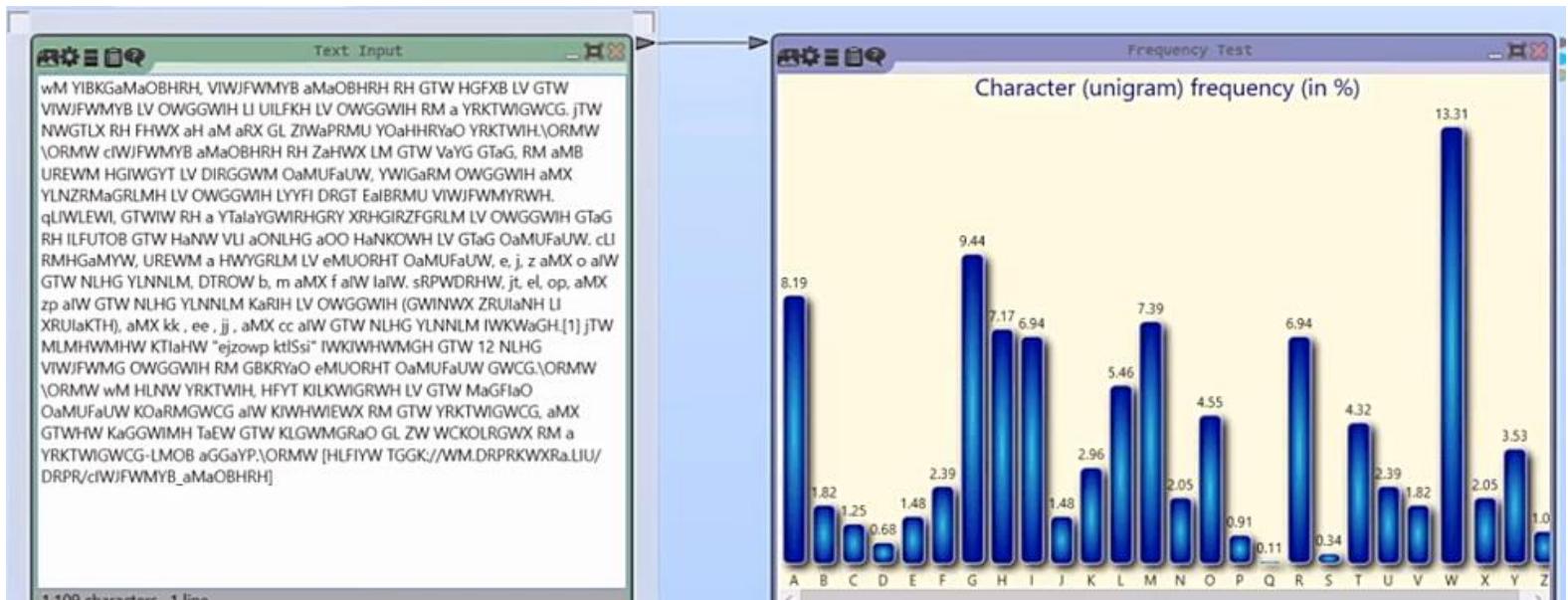
- Cryptography using Cryptool (video+slides)
  - Letter Frequency of ciphers (vi)
  - Substitution (iii), password





# Basic Crypto II

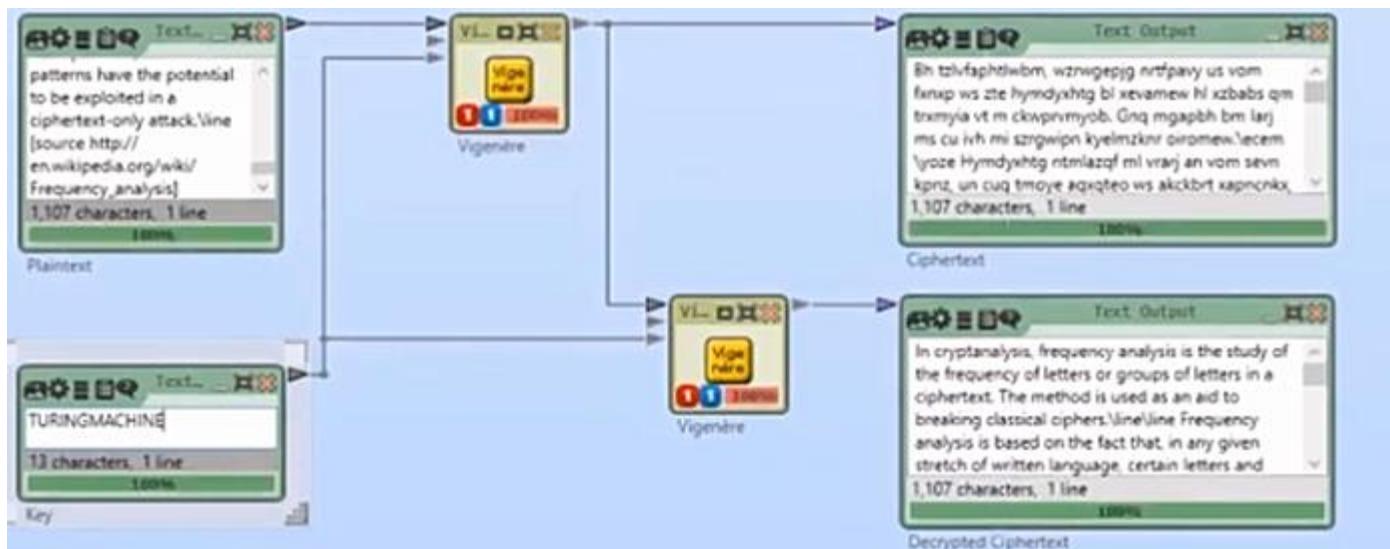
- **Cryptography using Cryptool (video+slides)**
  - Letter Frequency of ciphers (vii)
  - Substitution (iv), password





# Basic Crypto II

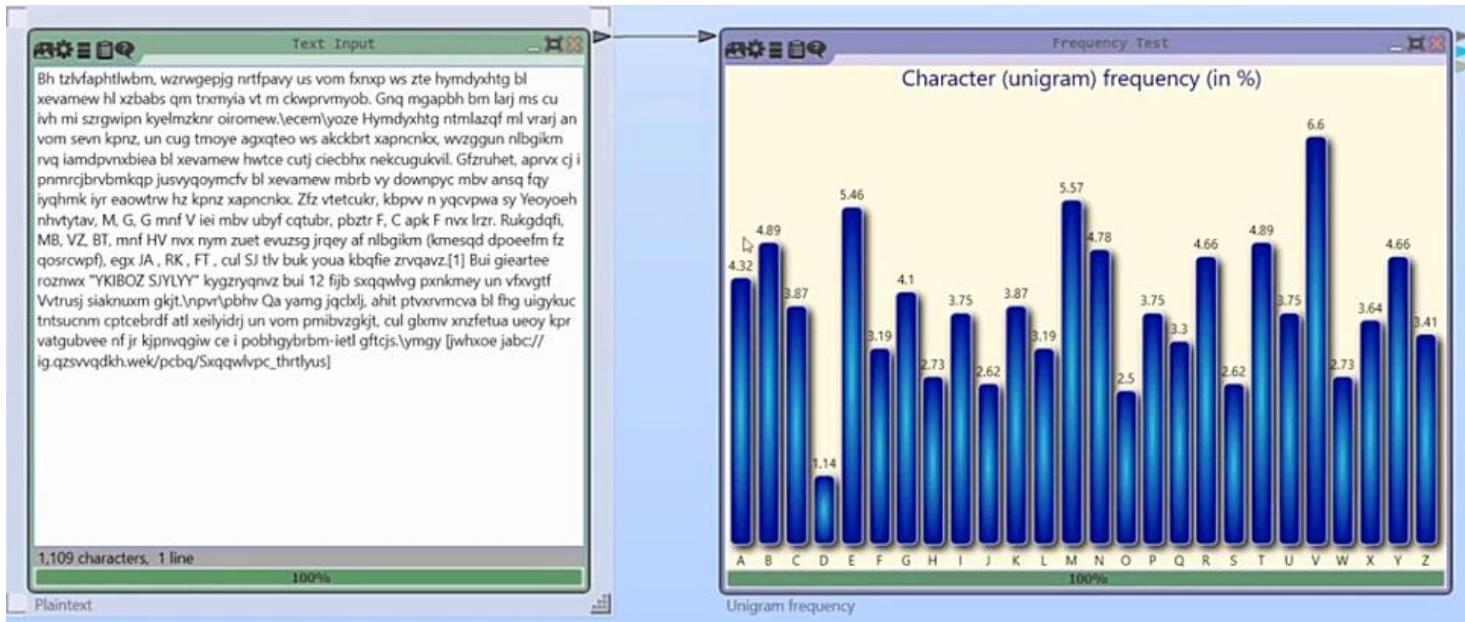
- Cryptography using Cryptool (video+slides)
  - Letter Frequency of ciphers (viii)
  - Substitution (v), polyalphabetic





# Basic Crypto II

- Cryptography using Cryptool (video+slides)
  - Letter Frequency of ciphers (ix)
  - Substitution (vi), polyalphabetic





# Basic Crypto II (LAB I)

- **Task I. Repeat the analysis at lab (15 MINS)**
- **Frequency analysis for:**
  - plain text
  - monoalphabetic (no password)
  - monoalphabetic (password)
  - polyalphabetic



# Breaking cipher I

- **Breaking Caesar (video+slides) (i)**
  - Shift of 13





# Breaking cipher I

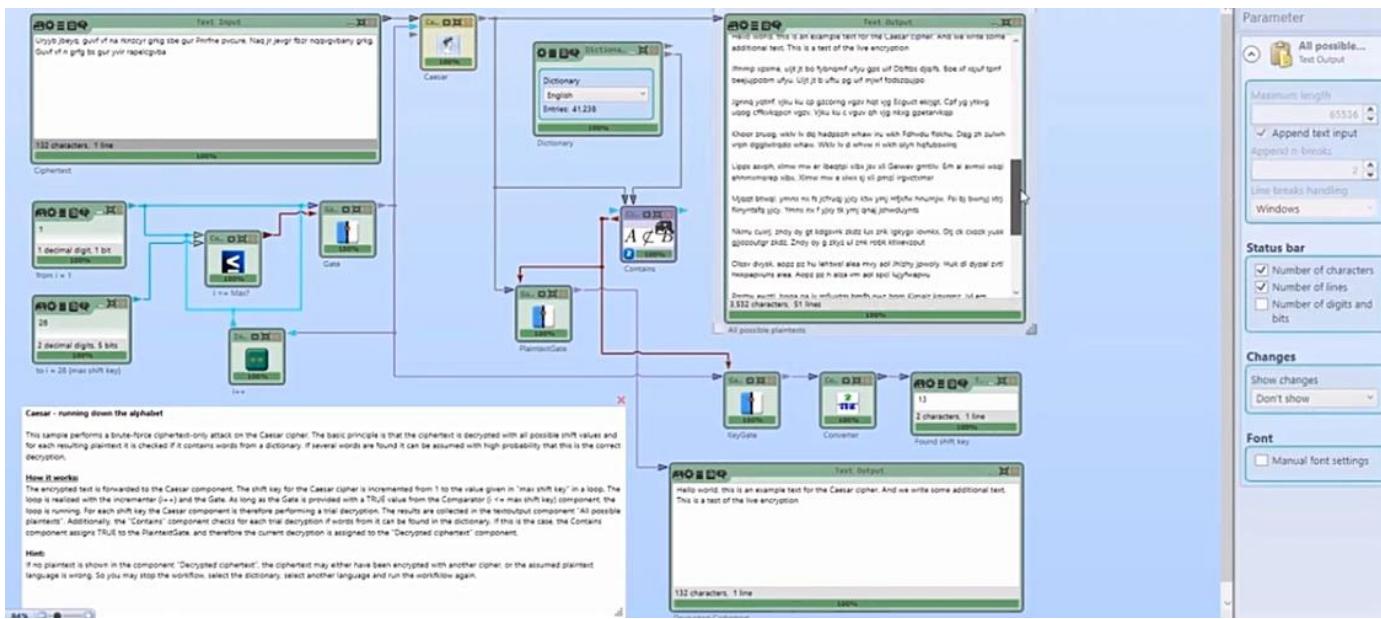
- Breaking Caesar (video+slides) (ii)
  - Brute Force analysis





# Breaking cipher I

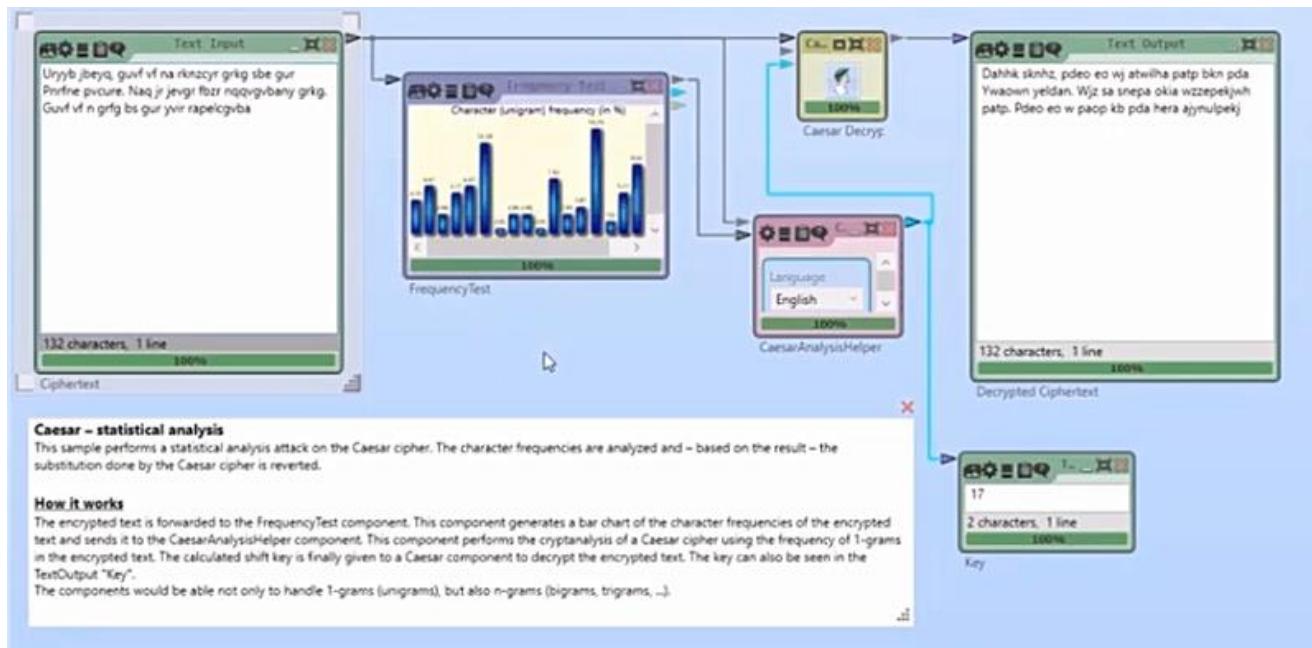
## ■ Breaking Caesar (video+slides) (iii) – Brute Force analysis





# Breaking cipher I

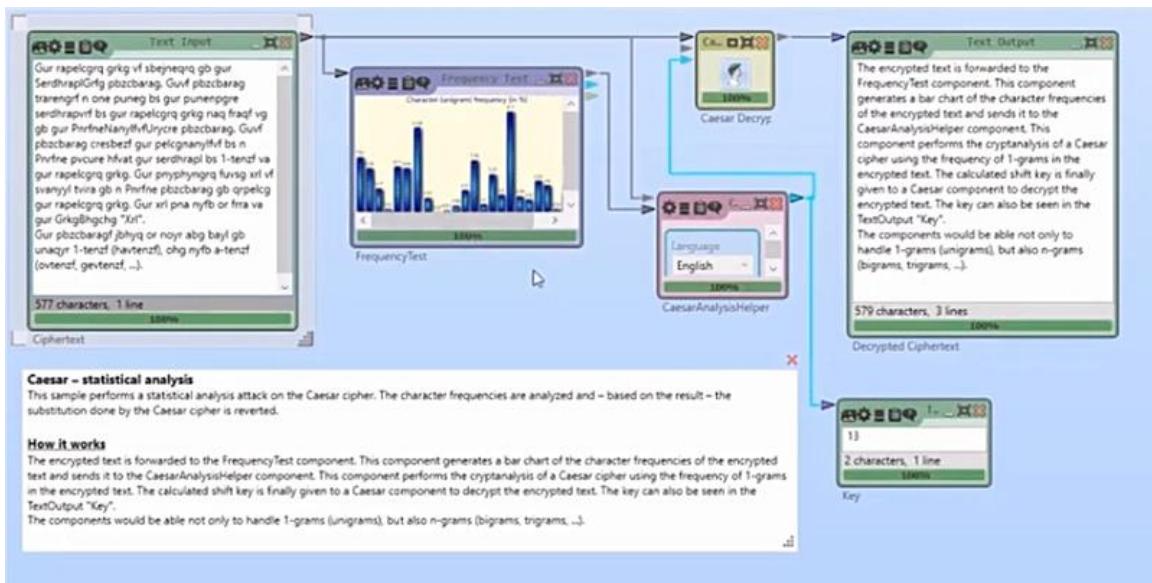
- Breaking Caesar (video+slides) (iv)
  - Analysis using Character Frequencies
  - Needed enough info, wrong result =17





# Breaking cipher I

- Breaking Caesar (video+slides) (v)
  - Analysis using Character Frequencies
  - Needed enough info, correct result=13





# Breaking cipher I

- Breaking Caesar (video+slides) (vi)
  - Shift of 13 as output





# Breaking cipher II

## ■ Breaking Monoalphabetic substitution (i)

**Definition:** In cryptography, a simple monoalphabetic substitution cipher replaces the letters of the plaintext with the letters from a single ciphertext alphabet. Each individual plaintext letter is always replaced with exactly the same ciphertext letter. The cryptographic key of the simple monoalphabetic substitution cipher is the mapping from plaintext alphabet to ciphertext alphabet.

- > Q: What is a plaintext or ciphertext alphabet?  
A: In our case, the plaintext alphabet is the Latin alphabet: ABCD...XYZ  
A: The ciphertext alphabet is a permutation of the plaintext alphabet, e.g. XZTY...PQR
- > Q: How many different keys (= ciphertext alphabets) exist?  
A: With the Latin alphabet used as plaintext alphabet, there exist  $26!$  ciphertext alphabets ( $\Rightarrow$  approx.  $2^{88}$  keys)
- > Q: How can we break the simple monoalphabetic substitution cipher which has such a huge keyspace?  
A: Using language statistics simple monoalphabetic substitution ciphers can be easily broken (even) by hand. We will use CrypTool 2 to break the cipher. CrypTool 2 uses heuristics which also use language statistics in the background.

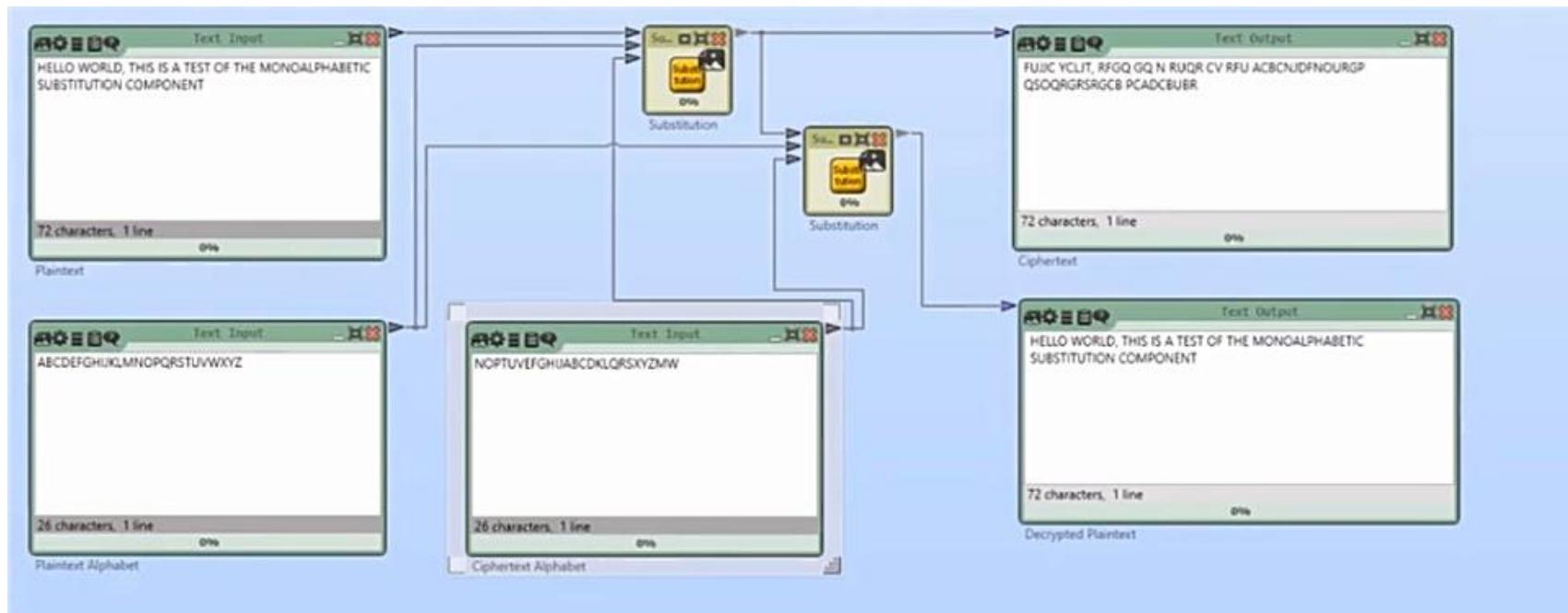
Task 1: Create a simple monoalphabetic substitution workspace in CrypTool 2  
(a) Encrypt and (b) decrypt text

Task 2: Break a ciphertext, which has been encrypted with the simple monoalphabetic substitution cipher



# Breaking cipher II

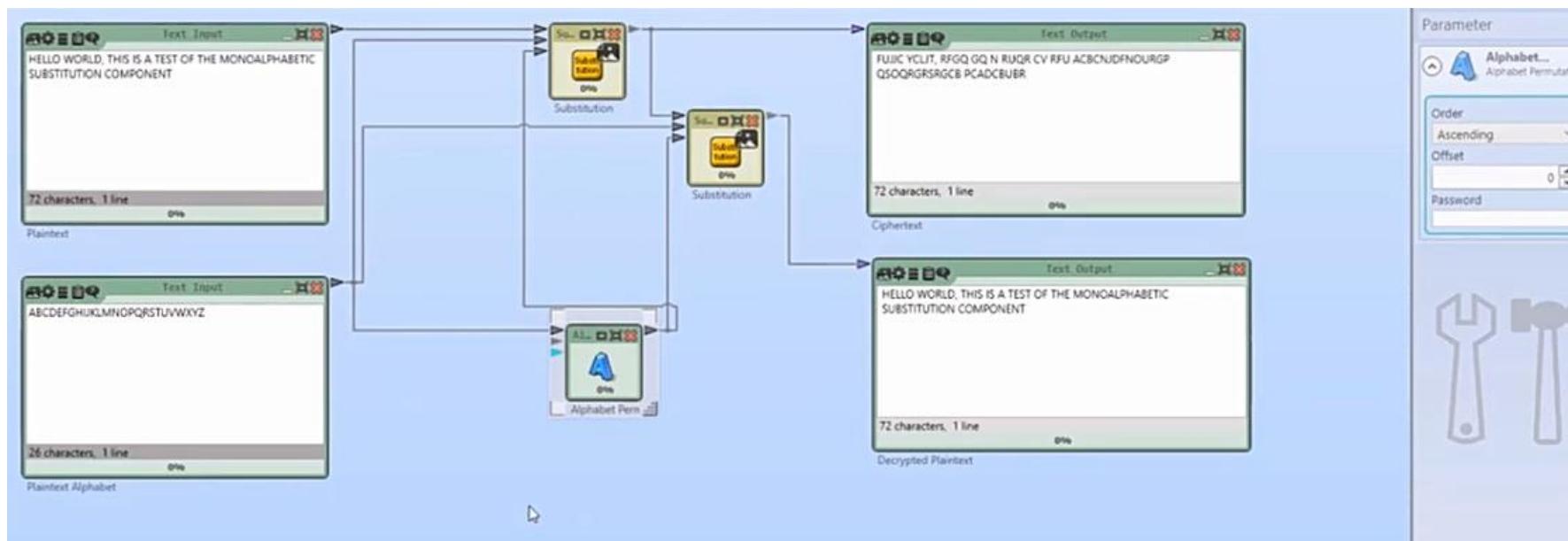
## ■ Breaking Monoalphabetic substitution (ii)





# Breaking cipher II

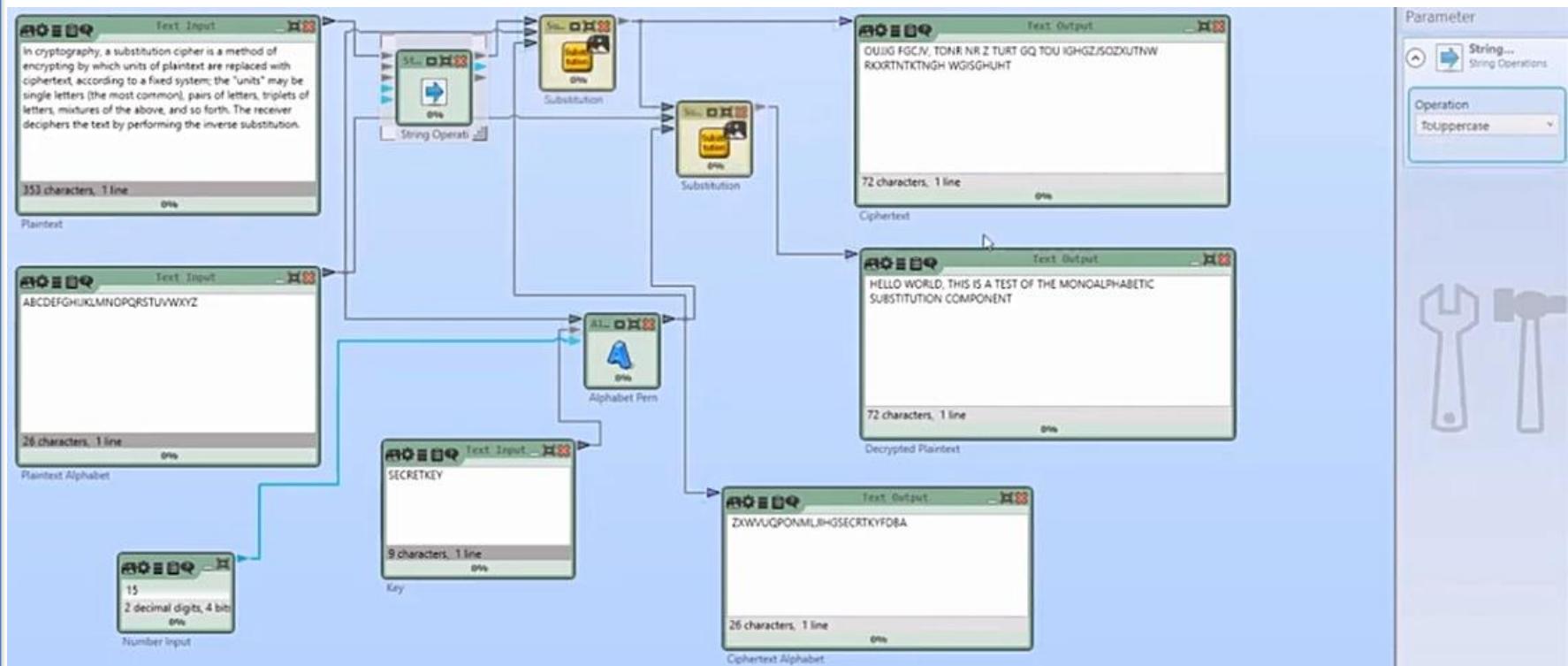
## ■ Breaking Monoalphabetic substitution (iii)





# Breaking cipher II

## ■ Breaking Monoalphabetic substitution (iv)





# Breaking cipher II

## ■ Breaking Monoalphabetic substitution (v)

The screenshot shows the Cryptology for IoT software interface with the following components and their interactions:

- Text In:** A component containing the ciphertext "IGRT WGIGHI, SZNCR GQ JUTTUCR, TCNSJUTR GQ JUTTUCR, INDTKCUR GQ TOU ZXGYU, ZHV RG QGCTO, TOU CUWUNYUC VUWNSOUCR TOU TUDT XB SUCQGCINHP TOU NI-HYUCRU RIQRNTKTNGH." (353 characters, 1 line, 100%). It has an arrow pointing to the Monoalphabetic Substitution Analyzer.
- Text Out:** A component displaying the decrypted plaintext: "IN CRYPTOGRAPHY A SUBSTITUTION CIPHER IS A METHOD OF ENCRYPTING BY WHICH UNITS OF PLAINTEXT ARE REPLACED WITH CIPHERTEXT ACCORDING TO A FIXED SYSTEM THE UNITS MAY BE SINGLE LETTERS THE MOST COMMON PAIRS OF LETTERS TRIPLETS OF LETTERS MIXTURES OF THE ABOVE AND SO FORTH THE RECEIVER DECIPHERS THE TEXT BY" (340 characters, 1 line, 100%). It has an arrow pointing from the Monoalphabetic Substitution Analyzer.
- Text In:** A component containing the plaintext alphabet "ABCDEFGHIJKLMNOPQRSTUVWXYZ" (27 characters, 1 line, 100%). It has an arrow pointing to the Monoalphabetic Substitution Analyzer.
- Text Out:** A component displaying the decrypted plaintext: "ABCDEFHJKLMNPQRSTUWXYZ" (27 characters, 1 line, 100%). It has an arrow pointing from the Monoalphabetic Substitution Analyzer.
- Text Out:** A component displaying the key: "KYRX/WONMLUZQIHGSPTEDCBVA" (27 characters, 1 line, 100%). It has an arrow pointing from the Monoalphabetic Substitution Analyzer.
- Parameter Panel:** On the right side, it includes sections for "Attack type" (set to "Monalphabetic..."), "Algorithm" (set to "Hillclimbing"), "Language" (set to "English" with "Use spaces" checked), and "Advanced settings" (set to "Ignore").

**Text In (Ciphertext):**

```
IGRT WGIGHI, SZNCR  
GQ JUTTUCR, TCNSJUTR  
GQ JUTTUCR, INDTKCUR  
GQ TOU ZXGYU, ZHV RG  
QGCTO, TOU  
CUWUNYUC  
VUWNSOUCR TOU  
TUDT XB SUCQGCINHP  
TOU NI-HYUCRU  
RIQRNTKTNGH.
```

**Text Out (Plaintext):**

```
IN CRYPTOGRAPHY A  
SUBSTITUTION CIPHER IS A  
METHOD OF ENCRYPTING BY  
WHICH UNITS OF PLAINTEXT  
ARE REPLACED WITH  
CIPHERTEXT ACCORDING TO A  
FIXED SYSTEM THE UNITS MAY  
BE SINGLE LETTERS THE MOST  
COMMON PAIRS OF LETTERS  
TRIPLETS OF LETTERS  
MIXTURES OF THE ABOVE AND  
SO FORTH THE RECEIVER  
DECIPHERS THE TEXT BY
```

**Text In (Plaintext Alphabet):**

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

**Text Out (Decrypted Plaintext):**

```
ABCDEFHJKLMNPQRSTUWXYZ
```

**Text Out (Key):**

```
KYRX/WONMLUZQIHGSPTEDCBVA
```

**Parameter Panel:**

- Attack type:** Cryptanalysis... / Monalphabetic...
- Algorithm:** Hillclimbing
- Language:** English (checked)
- Advanced settings:** Invalid Characters: Ignore



# Basic Crypto II (LAB II)

- **Task II. Reproduce the analysis at lab (20 MINS)**
- **Break Monoalphabetic substitution:**
  - Caesar
    - Brute Force:
      - Alphabet (=26). Invariant to uppercase.
      - Gate (Hits=4)
    - Try different parameters of alphabet, gates, languages.
    - Frequency analysis:
      - Try different word number. Perform an analysis for different languages releasing minimum word number to success
    - Try also assignments 1-3 (from assignment M4 slides)



# Basic Crypto II (LAB II)

- **Task II. Reproduce the analysis at lab (20 MINS)**
- **Break Monoalphabetic substitution:**
  - Monoalphabetic (no password)
  - Monoalphabetic (password)
    - Try also assignments 4-6 (from assignment M4 slides)



# Breaking cipher III

## ■ Breaking Polyalphabetic substitution (i)

- Blaise de Vigenère was a **French diplomat, cryptographer, translator, and alchemist**
- He lived from **1523-04-05** to **1596-02-19**
- 1549 he was ordered to work for **two years in the Vatican** where he got in **contact with cryptography**
- 1570 he quit his diplomatic duties and dedicated his life to **writing and cryptography**
- Vigenère wrote more than **20 books** including ***Traicté de Cometes* (1580)** and ***Traicté de Chiffres* (1586)**
- He developed the **Autokey Cipher** and a cipher developed by **Giovan Battista Bellaso** was named after him



# Breaking cipher III

## ■ Breaking Polyalphabetic substitution (ii)

- The **first polyalphabetic cipher** was described by **Johannes Trithemius** in his 1518 book "**Polygraphiae**", where he described the **Trithemius Cipher** with a fixed **tabula recta**
- The polyalphabetic cipher known today as the **Vigenère Cipher** was developed by **Giovan Battista Bellaso** and described in his 1553 book "**La cifra del. Sig. Giovan Battista Bellaso**". Bellaso added a **keyword** which was used as lookup into the tabula recta
- Finally, **Blaise de Vigenère** developed a stronger version of a polyalphabetic cipher based on the one described by Bellaso. In his **Autokey Cipher**, he does not repeat the keyword but **appends the plaintext to the keyword** and uses it as additional key material. He described that cipher in his 1586 book "**Traicté des chiffres ou secrètes manières d'escrire**"

Polyalphabetic ciphers timeline:

Trithemius Cipher (1518) → Vigenère Cipher (1553) → Autokey Cipher (1586)



# Breaking cipher III

## ■ Breaking Polyalphabetic substitution (iii)

- To encrypt a plaintext using the Vigenère Cipher, **write the keyword above the plaintext**
- Then, use **plaintext letters and key letters** in the tabula recta to look up the ciphertext letters (or use equation)

Example:

Key           => KEYKEYKEYK

Plaintext   => HELLOWORLD

Ciphertext => RIJVSUYVJN

$$\text{Equation: } C_i = (K_i + P_i) \bmod 26$$

where  $A = 0, B = 1, C = 2, \dots, Z = 25$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X



# Breaking cipher III

## ■ Breaking Polyalphabetic substitution (iv)

- To encrypt a plaintext using the Autokey Cipher, **write the keyword and plaintext above the plaintext**
- Then, use **plaintext letters and key letters** in the tabula recta to look up the ciphertext letters (or use equation)

Example:

Key           => KEYHELLOWO

Plaintext   => HELLOWORLD

Ciphertext => RIJSSHZFHR

Equation:  $C_i = (K_i + P_i) \bmod 26$   
where  $A = 0, B = 1, C = 2, \dots, Z = 25$

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y



# Breaking cipher III

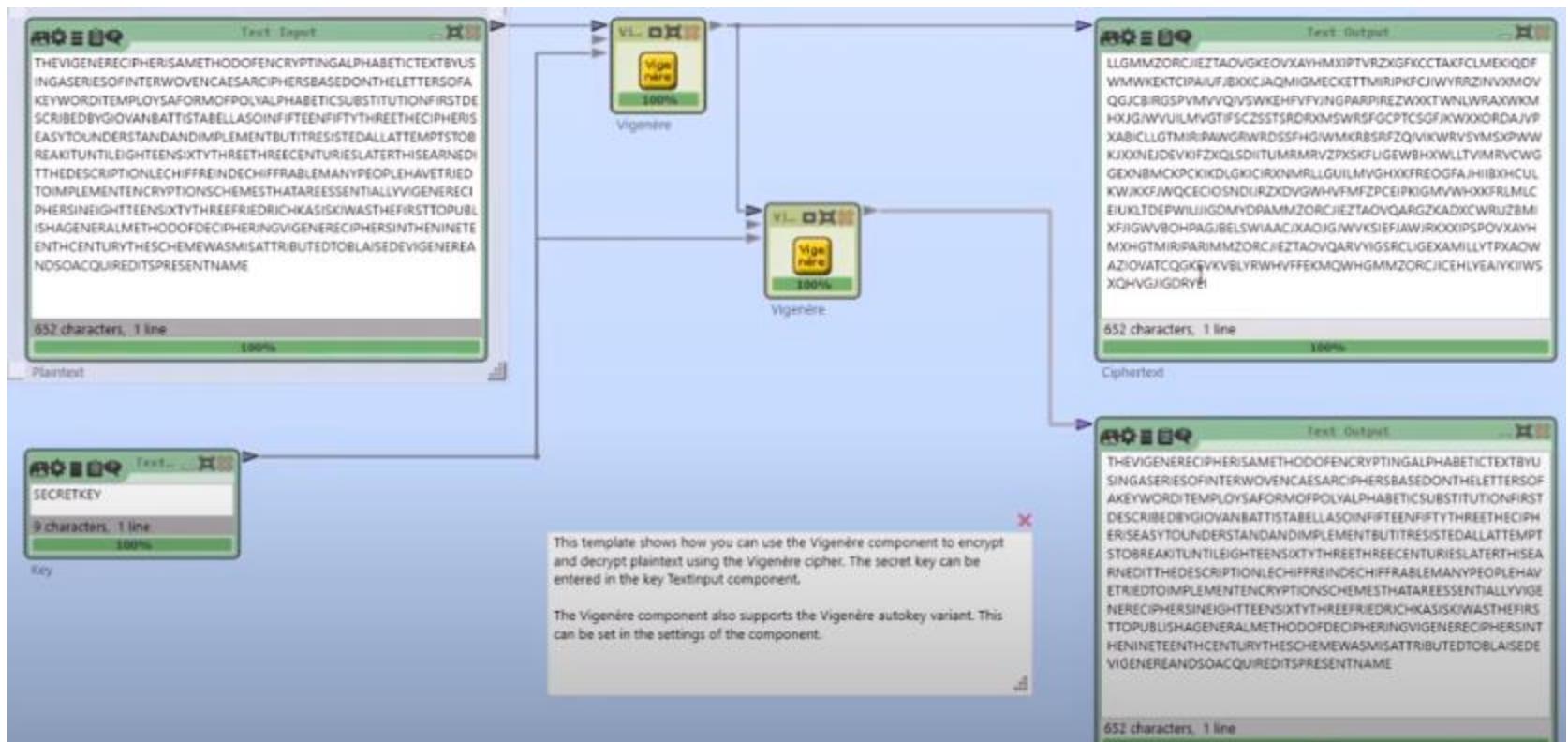
## ■ Breaking Polyalphabetic substitution (v)

- The Vigenère Cipher can be implemented with **different ciphertext alphabets**
  1. Latin Alphabet (today): ABCDEFGHIJKLMNOPQRSTUVWXYZ (26 letters)
  2. Latin Alphabet (“historic”): ABCDEFGHIJKLMNOPQRSTUVWXYZ (24 letters)
  3. Kryptos Alphabet: KRYPTOSABCDEFGHIJKLMNQUVWXZ (26 letters)
- We updated the Vigenère Analyzer in CrypTool 2 to support alphabets with less than 26 letters to support the **analysis of original historical ciphers**
- The analyzer **“updates” the used cost function (e.g. tetragrams)**, by removing unused letters from the cost value calculation during the execution of the hill climbing algorithm



# Breaking cipher III

## ■ Breaking Polyalphabetic substitution (vi)





# Breaking cipher III

## ■ Breaking Polyalphabetic substitution (vii)

The screenshot shows a software interface for breaking a Vigenère cipher. The interface consists of three main windows connected by arrows:

- Text Input:** Contains the ciphertext "LLGMNMZORCIEZTAOVGKEDOVXAVHMXIPTVRZ1GFKCTAKFC LMEKQDPFWMKWKEKTCIRAUJFIBXICAJQMIGMEEKETTMIRPK FCIIWYRZINVNXMVOVQGCBIRGPVMV/VQIV3WKEHFVIFYING PARIPIREZWXXTWNLUWRJWVXMHXIG/WVUJLMVGTIFSCZSST SRDRIXMSWRSFGCPTCSGFIKXWJOORDA/PXABCLLGTMRIP AHWGRNWPDSFHGIWNAKBSRFZQV/RKRRSYMSXPWPHCQX NEJDEVKFXQILSDITUMRMRVZPXSFKFLGEWBHKWLLTVIMR VCWGGEXOBEMB KPCCKDLOKCIROHNRLLGUJLNUVHDKFRE OGFAJHIBDXHCKWKWIKRF/WQCECOSNDURZKDVGWHVTFMF ZPCEIRKGMVWHXXFRMLMCEIUKLTDEPWUJGOMYDRAMM ZORCIEZTAOV/GAREZKADIXCVWRUZBMIXFKGWVBOHPAGJBE LSWIAACJAOIG/WVKS EJFJAWURKOKXPSPOV/KAHMXXHGTMJ RUPARIMMZORCIEZTAOV/DARVYVGSRC2LGEKAMILLYTRXAO WAZIOVATCQGKEVKVBLYRWHVFFEKMQWHGMZMZORCIEC HLYEAIKYKWSXQHVGRGDRYEI". It is noted as having 650 characters, 1 line.
- Vigenère Analyzer:** This window contains a table titled "Analysis" with columns: #, Value, Key, Key Length, and Text. The table currently shows one entry: "# 1 Value: Bcrypt Key: Bcrypt Key Length: 1 Text: Bcrypt". Below the table, it says "0%".
- Text Output:** Displays "0 characters, 0 lines" and "0%".

**Parameter Panel:**

- Mode:** Classic Vigenère
- Lower bound of keylength:** 1
- Upper bound of keylength:** 20
- Restarts:** 50
- Language:** English
- Keystyle:** Natural Language

**Text Input Panel:**

This panel contains two sections:

- A detailed description of the template: "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. Plaintext and key candidates are shown in the best list." It also notes that the template can be used for Vigenère autokey ciphers.
- A note: "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"."



# Breaking cipher III

## ■ Breaking Polyalphabetic substitution (viii)

The diagram illustrates the process of breaking a polyalphabetic substitution cipher using a Vigenère Analyzer component.

**Step 1:** The input ciphertext is shown in the first window: "LJÖMMZORCJETAOVOKO3DVYAHMKAFTVREZKGKOCCTAKC...".

**Step 2:** The Vigenère Analyzer component is used to find the key. It shows the following parameters:

- Start Time: 2/18/2021 4:15:30 PM
- End Time: 2/19/2021 4:15:54 PM
- Elapsed Time: 00:00:24
- Keys/second: 65,846
- Current analyzed keylength: 20

The results table lists 13 key candidates:

#	Value	Key	Key Length	Text
1	8.8880413428177	SECRETSECRETSECRET	18	THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME
2	8.8880433428177	SECRETSECRET	9	THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME
3	14.2489420164242	SECRETSECRET	12	THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME
4	14.2489420164242	SECRETSECRET	12	THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME
5	14.48894013883	XXXXXXSECRETSECRET	15	THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME
6	14.48894013883	SECRETSECRETSECRET	15	THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME
7	14.541513308884	SECRET	4	THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME
8	14.914804868012	SEC	3	THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME
9	15.81052409405	ZTSDBRSQHSDWAV749-GET	20	THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME
10	15.913448229113	EM5GQ0088888888888889	20	THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME
11	15.948139915489	ZTSDBRSQHSDWAV749-GET	20	THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME
12	15.948139915489	ACKTAR004330879-GET	20	THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME
13	15.97444748212	ETE23690PARMEH777-GET	20	THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME

**Step 3:** The decrypted plaintext is shown in the third window: "THEVIGENÉRCIPHERISAMETHODOFENCRYPTINGALPHABETICTEXTBYUSINGA SERIESOFINTERWOVENCAESARCIPHERSBASEDONTHELETTERSOFAKEWORDTOMIXUPASFORMOF POLYALPHABETICSUBSTITUTIONFIRSTDESCRIBEDBYJOAQUINBATTISTABELLAONAFIFTEENFIFTYTHREECENTURYCIPHERSASVTOUNDERSTANDINGIMPLEMENTBUTITREMOVEDALLTHE MPTSTOBREAKUNTILEIGHTENSIXTYTHREECENTURIESLATERTHISLEARNEDITIDESCRIPCIONDECHIRFRENDECHIFFRABLEMANYPERSONSHAVETESTCOMPLEMENTENCYPTIONSCH-EHENESTHATARESSENTIALLYVIGENÉRCIPHERSIN EIGHTEENTHCENTURYTHREEFREEDUCHASISOWASTHEFIRSTTOPUBLISHAGENERALMETHODOFDECIPHERINGVIGENÉRCIPHERSINTHEEIGHTEENTHCENTURYTHESCHEMENADMISSENBUTDIDNOTBLAISEDEVIGENÉRCIPHERANDSOACQUIREDSPRESENTPNAME".

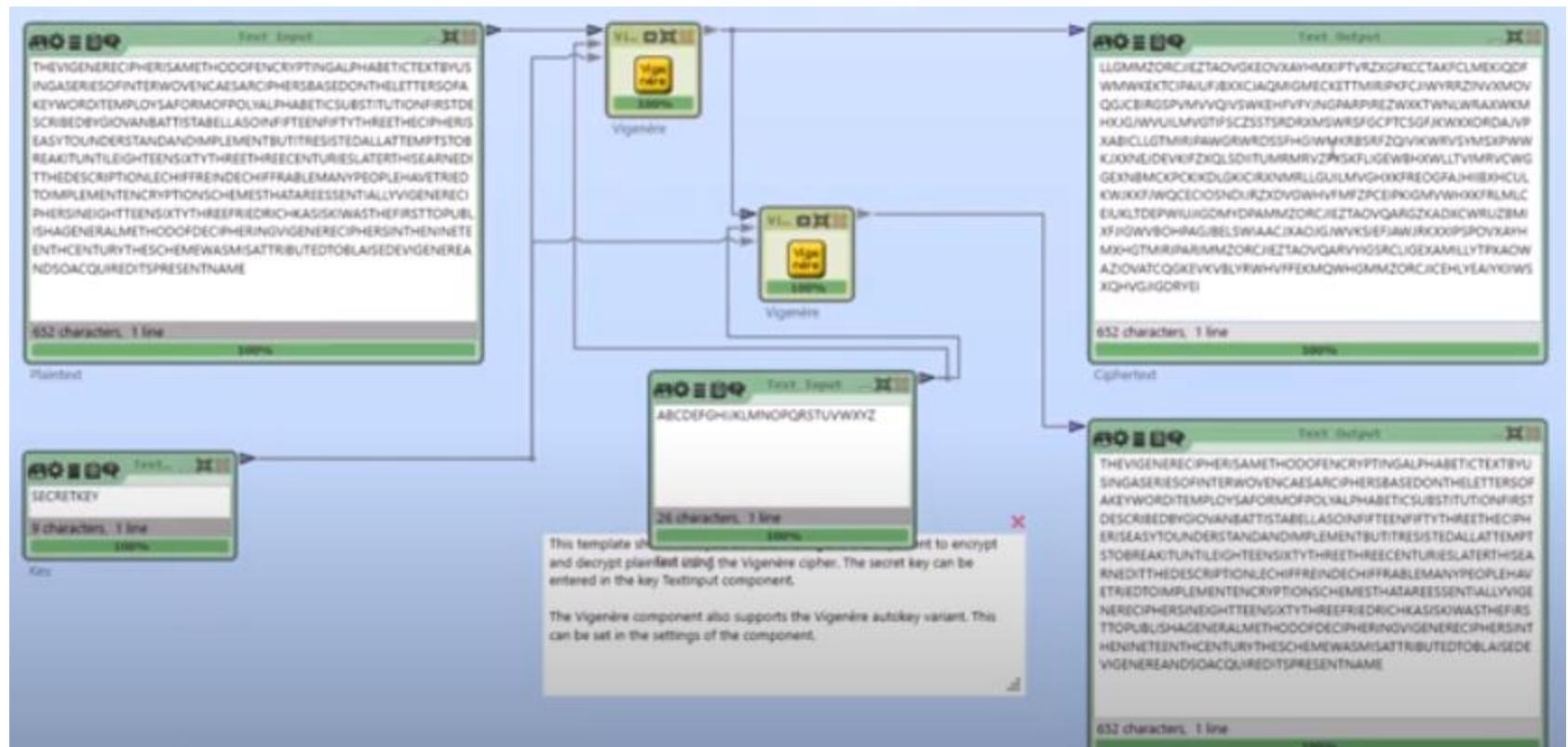
**Information from the Vigenère Analyzer component:**

- 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. Planted 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".



# Breaking cipher III

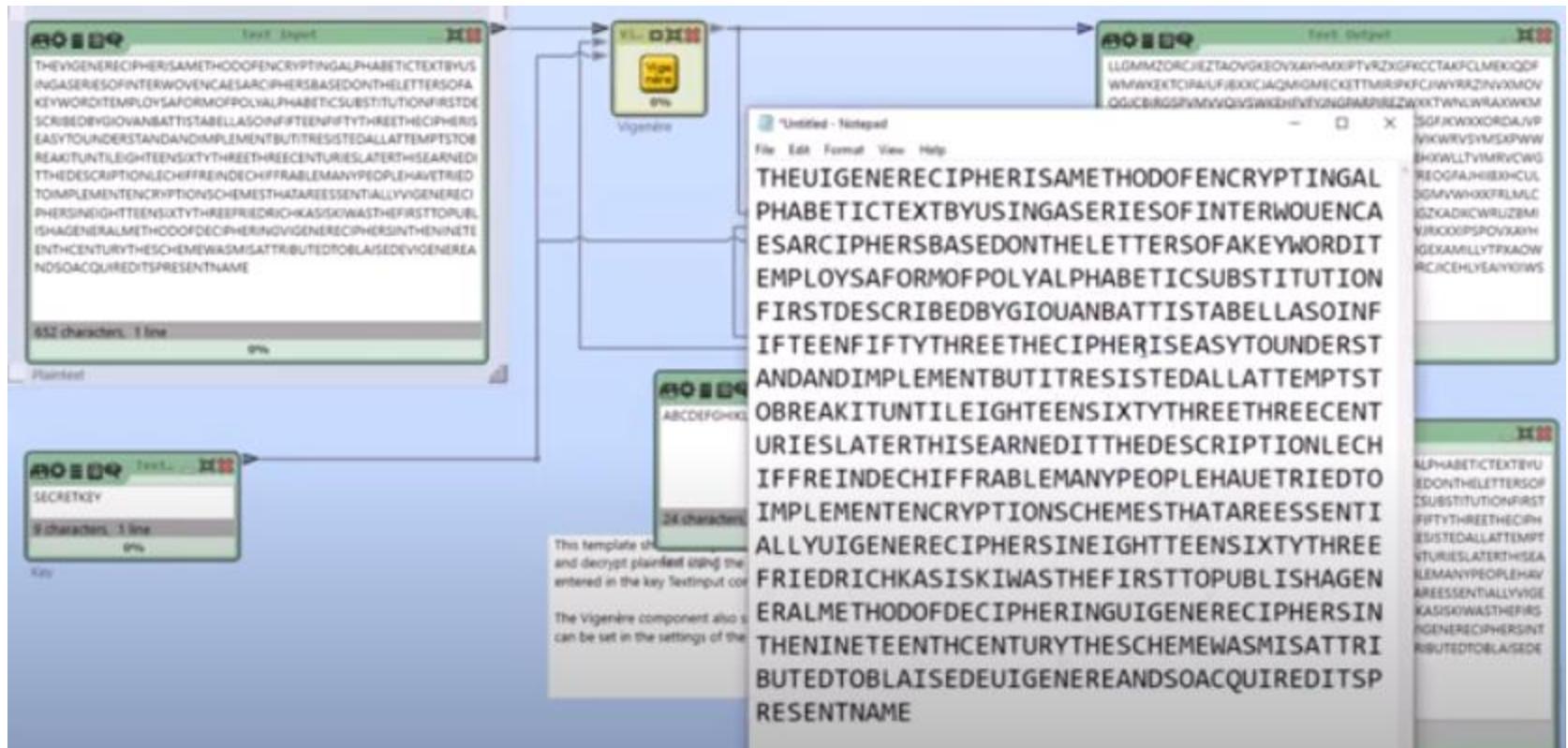
## ■ Breaking Polyalphabetic substitution (ix)





# Breaking cipher III

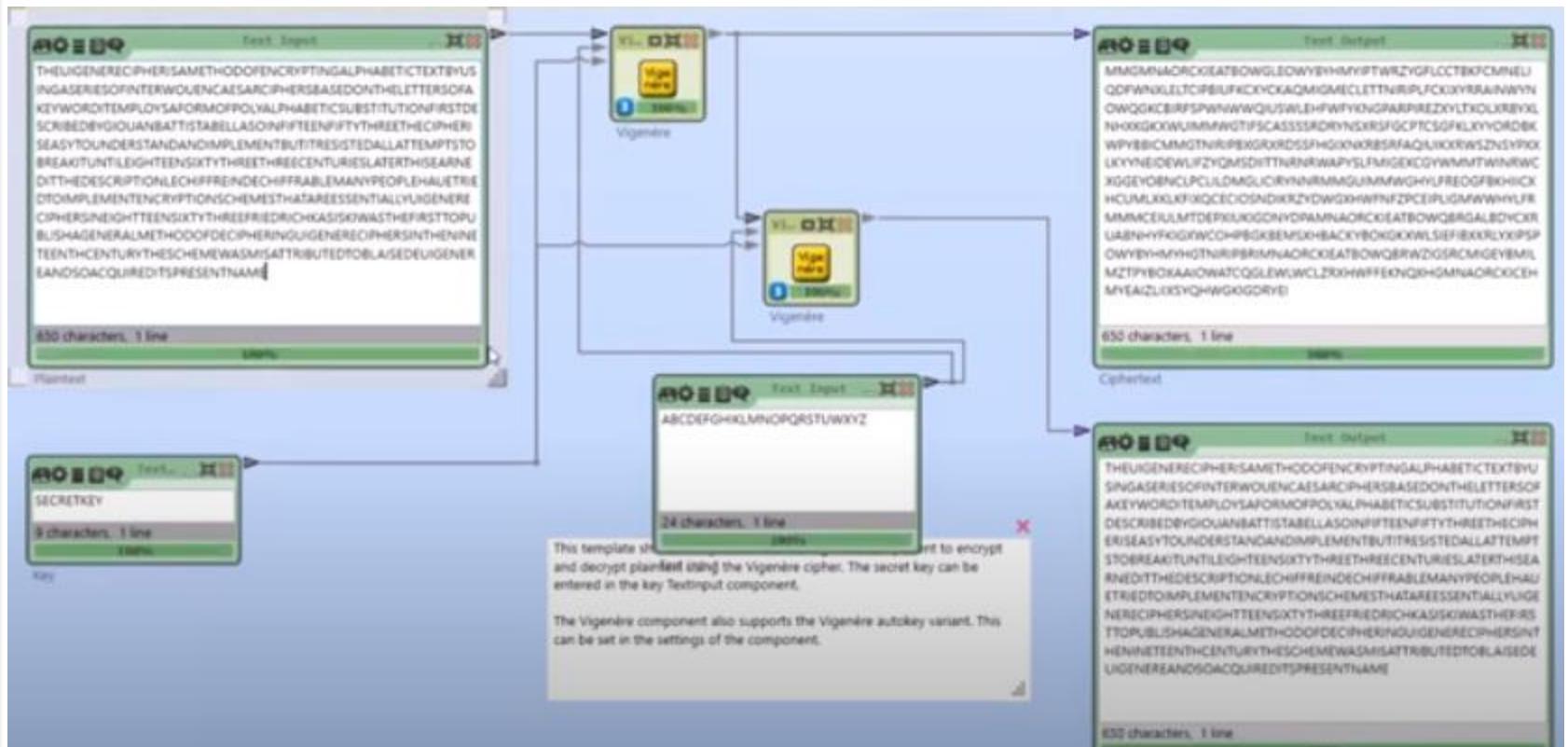
## ■ Breaking Polyalphabetic substitution (x)





# Breaking cipher III

## ■ Breaking Polyalphabetic substitution (xi)





# Breaking cipher III

## ■ Breaking Polyalphabetic substitution (xii)

Screenshot of a software interface for breaking ciphers, specifically a Vigenère cipher. The interface consists of three main windows:

- Text Input:** Shows the encrypted text: "MNCQMNAAORCKEATBOWGLEWVBYHNMNPTFWRZHGRCCTB KFCMMNEJQDFWNUKLETCPCPUFRCKYOKAOMKGMCELETTNR IFLFCQDXYBBARWVWYHNOHQSKCERFSUPWAWQUSWLEHFW FHNNGRABPZRZYKTRDLXREYLXLNHOKGDWKAUUMMINGTIFSC ASSSSHEDRYNSKSPCPCTSGFELYHODRNWPSBECMMGOT NARPERGKXNDISPHGOSRPAQURKORWSNZSYFOLX YNEDDEWLUFZHQMSEITTHNENWAPYSLFNUIGECDYWMNMT WNRWMOIGSEYOBNCUPLCULMSLICRYUNQHMMWQHMMWQHMMWQH HYLFDQGFKHHICHCUMUXLXPKXOECIOGSNDKZYDNG XHWBNPZCPEPLGMWWHYLFRMMMCUMLTDFRSHQGD NYGRAMNAORCKEATBOWGBRGKEDWYXRLAJBNHYNQDX WCCHPBKDKEMSKHBACKYBODSKOKRSLSFUWBBLXLYKSPD WIBYHMYHTGNRBRBRMNAORKEATBOWGBRWZGRCM IGEYBMLRMZTPVBCAAHOMWATCQGEJWUWCLZSRHWFEDN QHGMNAORCCEHMYEAZLQSYQH8GKORYE".
- Vigenère Analyzer:** A component showing analysis results. It includes fields for Start Time, End Time, Elapsed Time, Keys/second, and Current analyzed keylength. A table lists 13 key candidates with their values, key length, and text. The first candidate is highlighted.

#	Value	Key	Key Length	Text
1	13.05442311800	TEIAGWPFSTCRHKEY	18	TIEVGENERICHESSAMTHOCOPENCKPUJAHCHAB
2	13.322239423944	TEFGKREH	9	ETICUDATBUTINGZSERIESOFINJERWHDIMCAESARDCH
3	13.694971330666	EFTTGCAREYTAZRD	18	ERSATDOONTHELTTESSAGADEFYQHDQJULDKYSAJOFRL
4	13.47734781634	KEETEAMROJ	13	OCPNLYMKHABEJUXCSUETTUJVURNGIRTUDOSCIAEDER
5	13.72123622180	KEETEAMRETQ	13	GIOUZNBATITT28BLKZC0MAGJSTBENIGUYTHRETECICH
6	13.741762347980	TRTKEVEREPRFRET	18	ERITAEXTOUMDERSTANCZNDLAKEMENUJLUTREUTITTE
7	13.74885314394	EFTTGCAREH	13	DANKAUUJOLPUSTORZDZITJUNLUKEHJHTEENSWUYTIRFDT
8	13.6489523242781	EFTTGCARET	13	HEEICONTURUELSAUDRTSARMEDDTBEDDSQSILOJAKRE
9	13.8123798822717	TEETEZ	6	CHIGFRDNDEREJUGRABKSMANXKDEOPKJAUJTSDEUQPL
10	13.8123798822717	TEET	3	ELIENJUDMACHOUJOMSCILESHUMTAURESTDMTIALYVSE
11	13.0810074744831	EFTTGCAREHREHREH	18	NERECIOHESSINEOHTJEENS/WTKUHREIGREDRICK2SITR
12	13.2599423363831	EFTTGT	6	WATTHEGERTUUNCOUENTAGENERKLMTHOCDEOICHE
13	13.2599423363831	EFTTGCAREHREHREH	18	RINGVENEREICOHESIVUJOMVNETER/THCENTVRYTHE

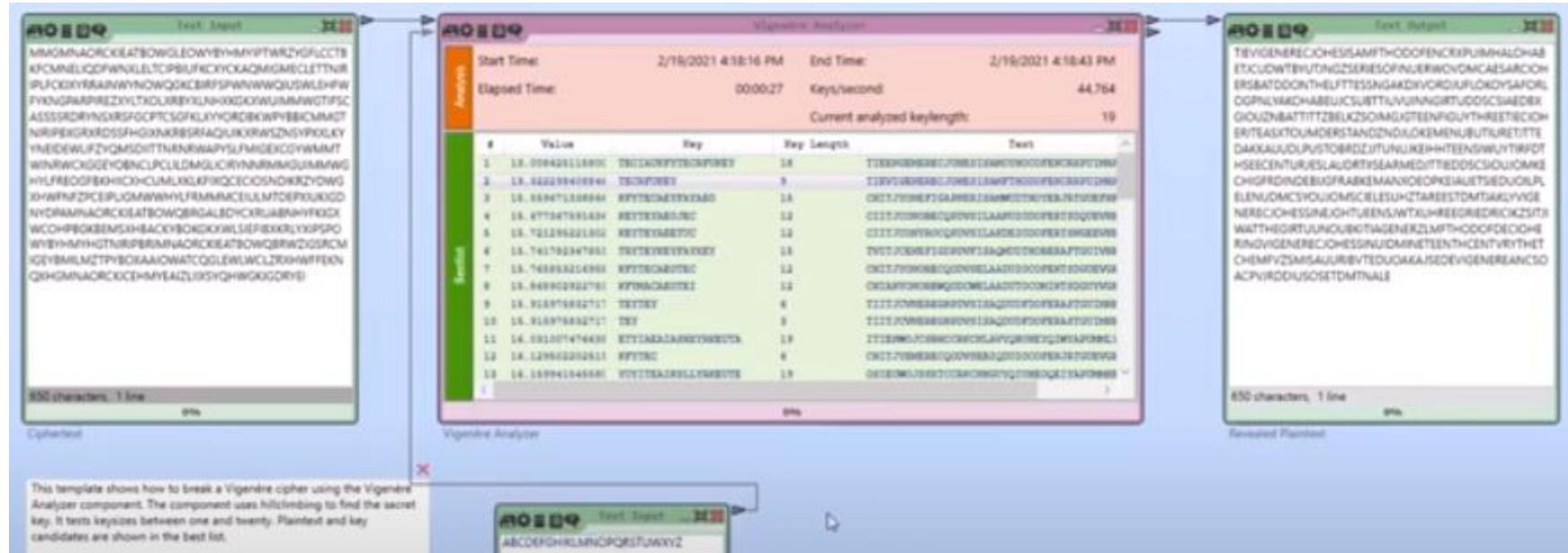
- Text Output:** Shows the decrypted text: "TIEVGENERICHESSAMTHOCOPENCKPUJAHCHAB ETICUDATBUTINGZSERIESOFINJERWHDIMCAESARDCH ERSATDOONTHELTTESSAGADEFYQHDQJULDKYSAJOFRL OCPNLYMKHABEJUXCSUETTUJVURNGIRTUDOSCIAEDER GIOUZNBATITT28BLKZC0MAGJSTBENIGUYTHRETECICH ERITAEXTOUMDERSTANCZNDLAKEMENUJLUTREUTITTE DANKAUUJOLPUSTORZDZITJUNLUKEHJHTEENSWUYTIRFDT HEEICONTURUELSAUDRTSARMEDDTBEDDSQSILOJAKRE CHIGFRDNDEREJUGRABKSMANXKDEOPKJAUJTSDEUQPL ELIENJUDMACHOUJOMSCILESHUMTAURESTDMTIALYVSE NERECIOHESSINEOHTJEENS/WTKUHREIGREDRICK2SITR WATTHEGERTUUNCOUENTAGENERKLMTHOCDEOICHE RINGVENEREICOHESIVUJOMVNETER/THCENTVRYTHE CHEMPV2SMSALURBYTEUCAKAJSEDEJGENEREANSCO ACPVIRDDAUOSSETDMTNALE".

The bottom left of the interface has a note: "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. Plaintext and key candidates are shown in the best list."



# Breaking cipher III

## ■ Breaking Polyalphabetic substitution (xiii)





# Breaking cipher III

## ■ Breaking Polyalphabetic substitution (xiv)





# Basic Crypto II (LAB III)

- **Task III. Repeat the analysis at lab (15 MINS)**
- **Break Polyalphabetic substitution:**
  - Vigenere using “Hill Climbing” heuristic
    - (lower, upper, restart)
    - Usual alphabet and changing alphabet
    - Try also assignments 7-9 (from assignment M4 slides)



# Breaking cipher IV

## ■ Breaking Transposition. Scytale (i)

Definition: In cryptography, a scytale cipher is a tool (mostly a wooden stick) which can be used to encrypt and to decrypt a text using a simple transposition cipher. A strip of paper is wrapped around the stick. Then, the plaintext is written on the paper. After removing the paper, the text appears transposed on the strip. To decrypt the ciphertext, a scytale with the same diameter has to be used. The paper strip is wrapped onto the receiver's scytale. After that, the plaintext is readable again.

-> Q: What is the keyspace size of the scytale?  
A: The number of different possible stick diameters.

-> Q: What is a "different stick diameter"?  
A: Two diameters are different if they have different numbers of columns on the stick.

-> Q: How many different diameters exist?  
A: There are at most "text length" different diameters, where the biggest diameter allows to wrap the strip exactly one time around the stick. In this case, the generated ciphertext equals the plaintext.

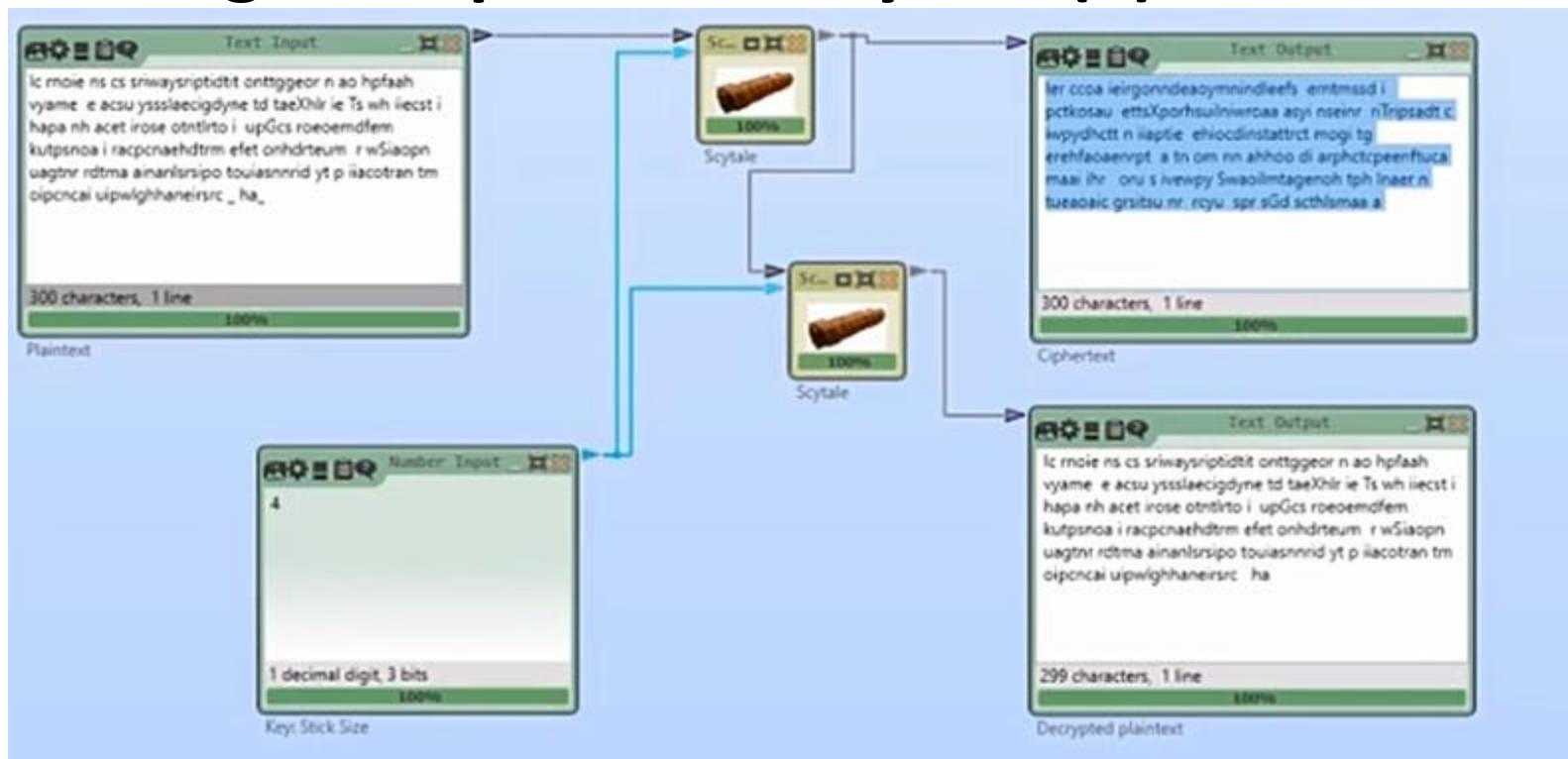
Task 1: Create a scytale workspace in CrypTool 2  
(a) Encrypt and (b) decrypt text

Task 2: Break a ciphertext, which has been encrypted with the scytale



# Breaking cipher IV

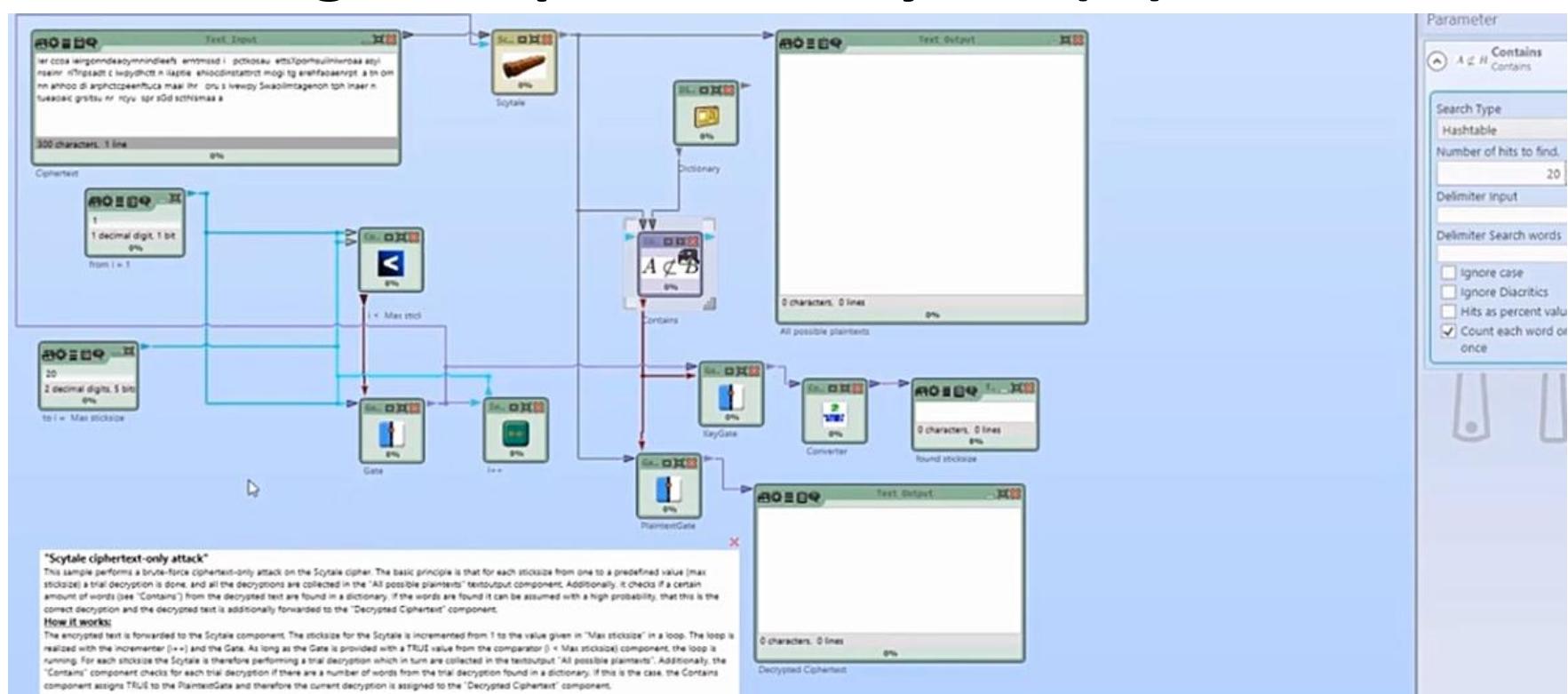
## ■ Breaking Transposition. Scytale (ii)





# Breaking cipher IV

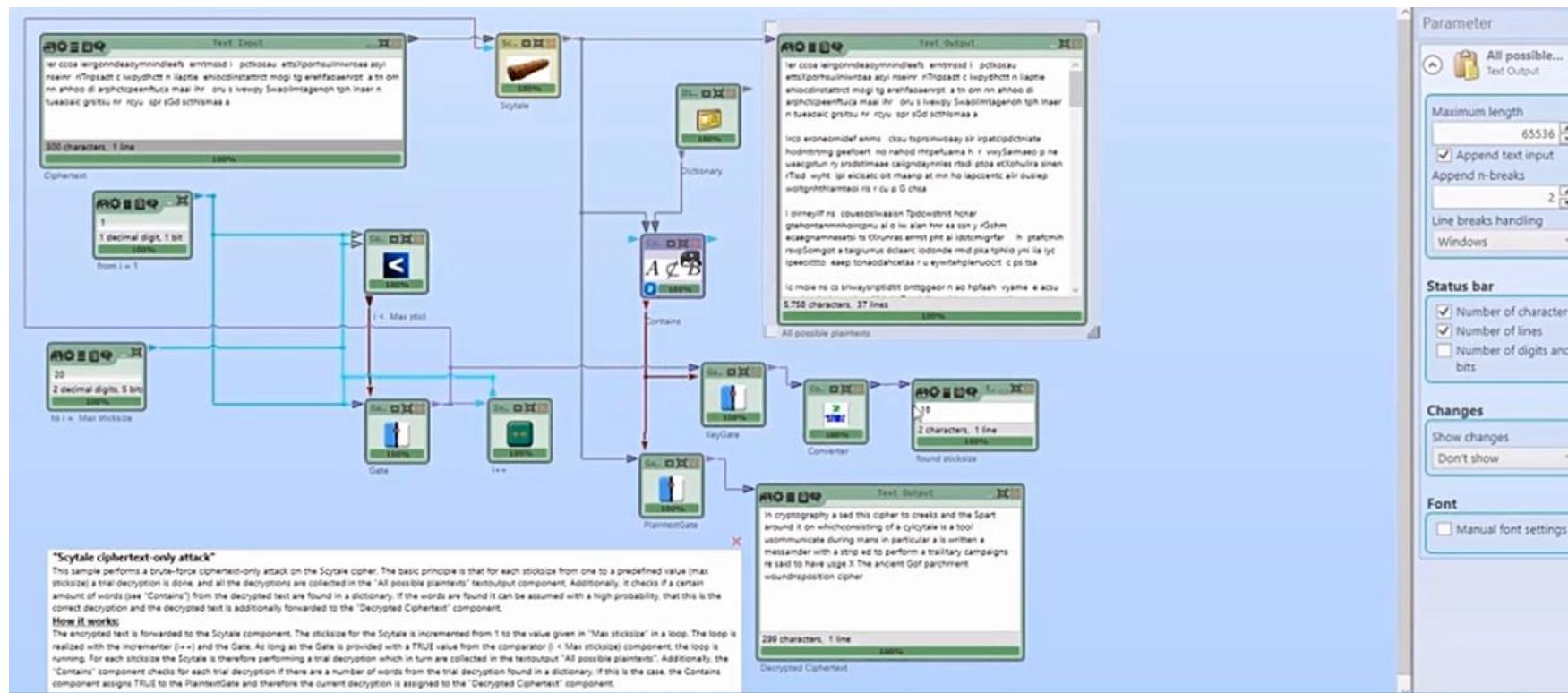
## ■ Breaking Transposition. Scytale (iii)





# Breaking cipher IV

## ■ Breaking Transposition. Scytale (iv)





# Breaking cipher V

## ■ Breaking Columnar Transposition (i)

### Break a Columnar Transposition Cipher

Definition: In cryptography, a transposition cipher is a cipher in which the order of the letters is modified, rather than replacing the letters with other symbols as in substitution ciphers. The most popular transposition cipher was the columnar transposition cipher, due to its simplicity. The columnar transposition cipher arranges the ciphertext in a grid of rows and columns. Then, a keyword is written over the grid (over each column exactly one letter). Then, the columns are ordered by the positions of the keyword's letters in the alphabet. Finally, the ciphertext is read out column-wise. To decrypt the text, the method is performed in the reverse order.

-> Q: How many different keys exist?

A: If we assume that the keyword has length  $n$ , then  $n!$  keys exist.

We have to sum these factorials for each possible keyword length, from the longest possible keyword length  $n$  to 1.

Example 1: the maximum assumed keyword length is 6.

Then, we have  $6! + 5! + 4! + 3! + 2! + 1! = 873$

Example 2: If we have a keyword of length  $18!$ , we already have about  $2^{53}$  keys (only for  $18!$ ).

And we still have to add the number of all shorter possible key lengths.

Task 1: Create a transposition cipher workspace in CrypTool 2

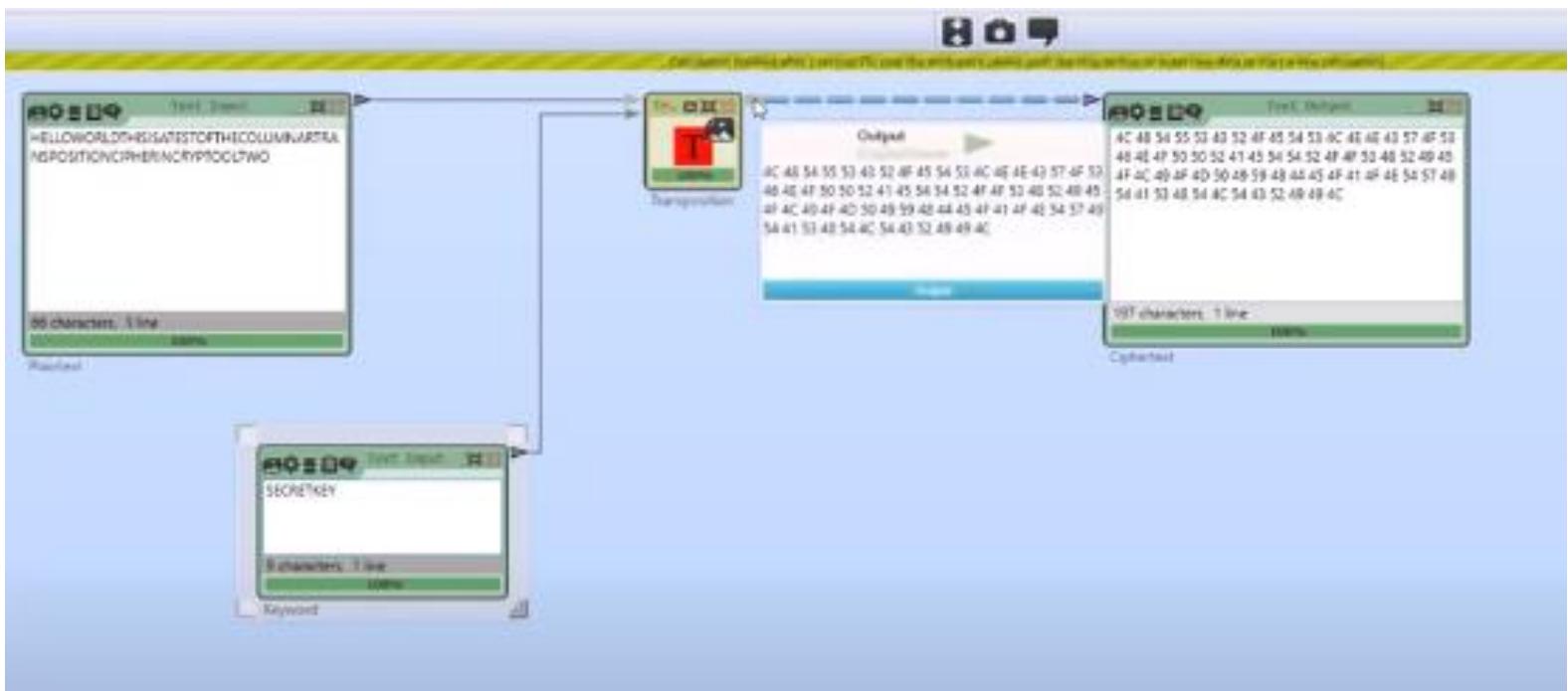
(a) Encrypt and (b) decrypt text

Task 2: Break a ciphertext, which has been encrypted with the columnar transposition cipher



# Breaking cipher V

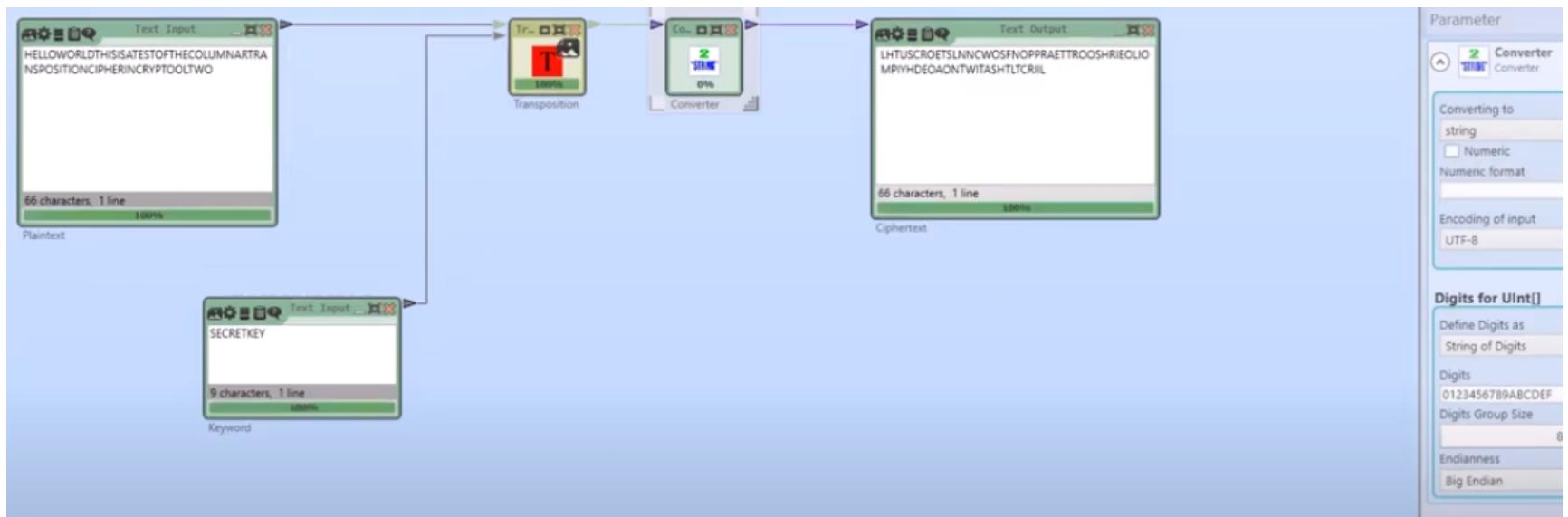
## ■ Breaking Columnar Transposition (ii)





# Breaking cipher V

## ■ Breaking Columnar Transposition (iii)





# Breaking cipher V

## ■ Breaking Columnar Transposition (iv)

HELLOWORLDTHISISATES	7 2 1 6 3 8 5 4 9
TOFTHECOLUMNARTRANS	SECRETKEY
POSITIONCIPHERINCRYPT	HELLOWORL
OOLTWO	

ES	7 2 1 6 3 8 5 4 9
TOFTHECOLUMNARTRANS	SECRETKEY
POSITIONCIPHERINCRYPT	HELLOWORL
OOLTWO	DTHISISAT

OLUMNARTRANS	7 2 1 6 3 8 5 4 9
POSITIONCIPHERINCRYPT	SECRETKEY
OOLTWO	HELLOWORL
	DTHISISAT
	ESTOFTHEC

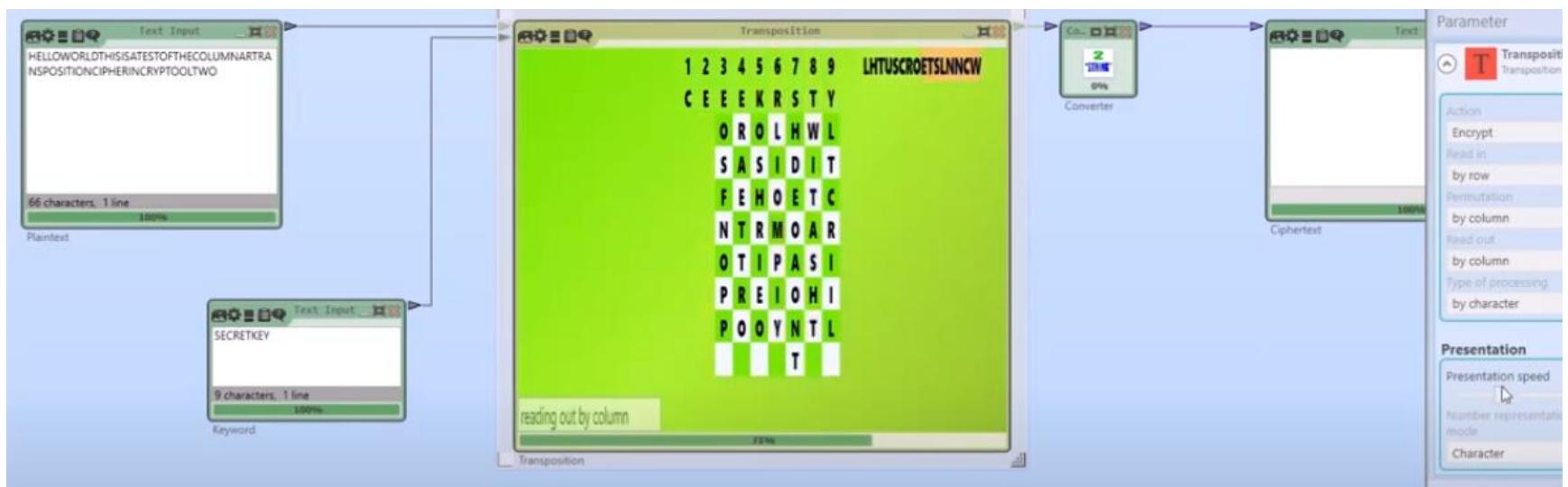
NCRYPT	7 2 1 6 3 8 5 4 9
OOLTWO	SECRETKEY
	HELLOWORL
	DTHISISAT
	ESTOFTHEC
	OLUMNARTR
	ANSPOSITI
	ONCIPHERI
	NCRYPTOOL
	TWO

	7 2 1 6 3 8 5 4 9
	SECRETKEY
	HELLOWORL
	DTHISISAT
	ESTOFTHEC
	OLUMNARTR
	ANSPOSITI
	ONCIPHERI
	NCRYPTOOL
	TWO



# Breaking cipher V

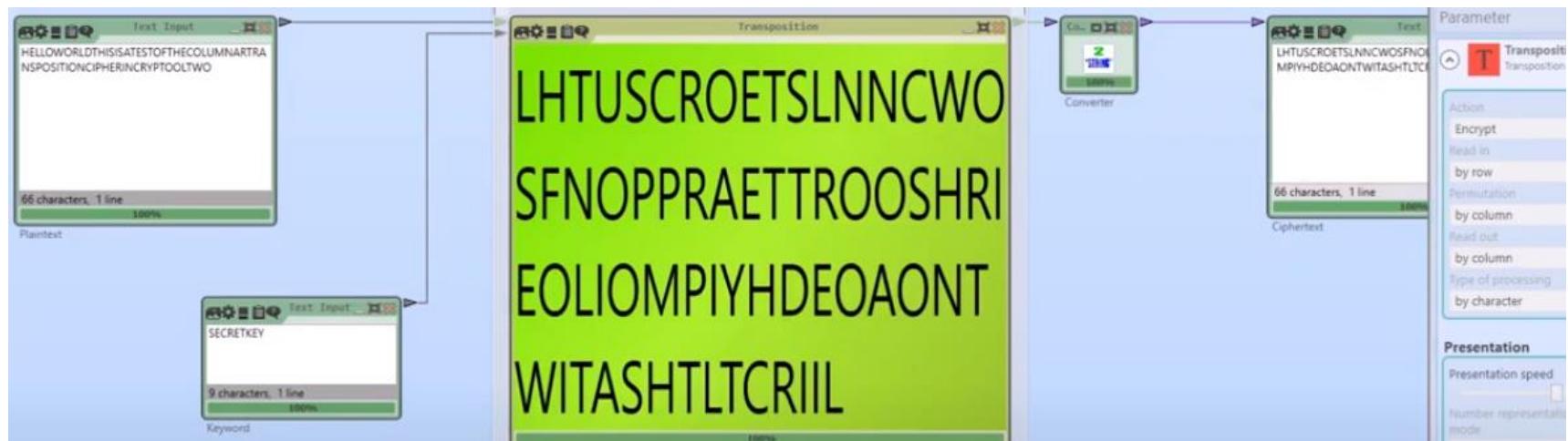
## ■ Breaking Columnar Transposition (v)





# Breaking cipher V

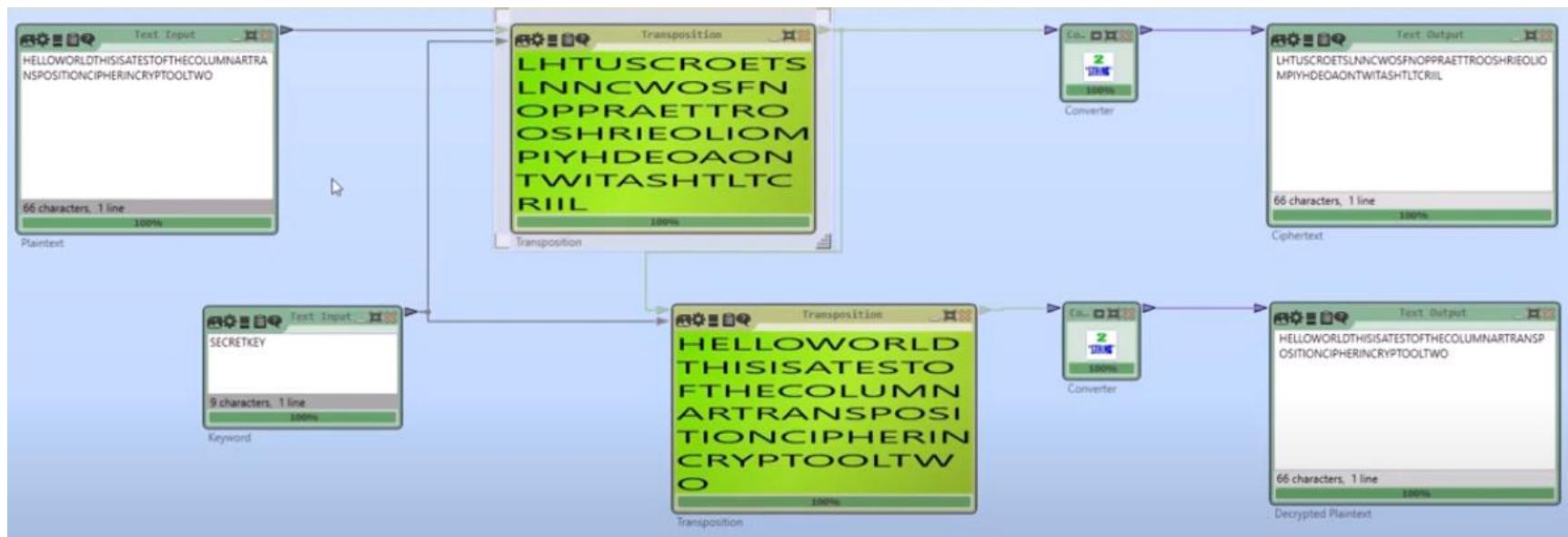
## ■ Breaking Columnar Transposition (vi)





# Breaking cipher V

## ■ Breaking Columnar Transposition (vii)





# Breaking cipher V

## ■ Breaking Columnar Transposition (viii)

The screenshot shows a software interface for breaking a columnar transposition cipher. The process flow is as follows:

- Text Input:** Contains the ciphertext: CPPIECYPTTIALEPCPORSTRNENIT EIGIEAACTDRSEDETNASCMBESI NHNTUASCAYAESPOAADNNARM CECACAOONSNTYSSHYHSLOEXC SOEDGEHETMFTSOSDTRHLIONC TCNUDORIOIHILHMRGHADGA OICEAETEHCTERABSERNPVTRTT TRDCTBWPWAARCSENLSCITTHX HTSHXEMAEIHEGYNCCRHOPTRW OESERYRSTIRETTTRONIRNENTOL TIOAINAFORRNNAENHNNICOCO RECOGSHMMAIHRILALSQUNISHRT 389 characters, 1 line 0%
- Transposition Analyzer:** Shows analysis parameters: Start, End, Elapsed, Remaining, Keys / sec. It also displays the "Value Key Mode Text" and a log area labeled "TranspositionAnalyzer". The status bar indicates 0% completion.
- Converter:** A small window showing a green icon with a 'Z' and the word "String" below it, along with a progress bar at 0%.
- Text Output:** Displays the Revealed Plaintext: 0 characters, 0 lines 0%
- Parameter:** A sidebar with the following settings:
  - TA:** Transposition Transposition Analyzer
  - Transposition:** Hill Climbing
  - Cost Function:** Transposition Analyzer
  - Analysis method:** Hill Climbing
  - Repetitions:** 10
  - Iterations:** 50000
  - Keysize:** 25

**Information Panel:**

This template shows the analysis of a ciphertext that was encrypted with a columnar transposition and a key of length 25. The analysis uses a hill climbing algorithm. This approach is not deterministic, hence, if the result (WHYHEWASSOANGRY...) is not found at the first run, simply try to run again.

The ciphertext was retrieved from the CC1-3 challenge of MysteryTwister I, where you can find many more ciphertexts that were encrypted with a columnar transposition. You can try to decode them with this template.

Link: <http://www.mysterytwisterc3.org/de/alte-mysterytwister-spiele/cc1-3>



# Breaking cipher V

## ■ Breaking Columnar Transposition (ix)

The figure consists of three side-by-side screenshots of a software interface for breaking columnar transposition ciphers. Each screenshot shows a 'Parameter' section at the top and a list of actions or settings below.

- Screenshot 1:** Shows the 'Parameter' section with 'TA Transposition' selected. Below it, under 'Action', are options: 'Encrypt', 'Read in', 'by row', 'Permutation', 'by column', 'Read out', 'by column', and 'Type of processing', with 'by character' highlighted.
- Screenshot 2:** Shows the 'Parameter' section with 'TA Transposition' selected. Below it, under 'Transposition', are options: 'Cost Function', 'Transposition Analyzer', and 'Transposition'. Under 'Analysis method', 'Hill Climbing' is selected. Below that are 'Repetitions' (set to 10), 'Iterations' (set to 50000), and 'Keysize' (set to 9).
- Screenshot 3:** Shows the 'Parameter' section with 'TA Transposition' selected. Below it, under 'Transposition Analyzer', are options: 'Transposition' and 'Cost Function'. Under 'Function type', 'N-grams: log 2' is selected. Below that are 'N-gram size' (set to 3), 'Bytes to use' (set to 389), 'Bytes offset' (set to 0), and 'Language' (set to English).



# Breaking cipher V

## ■ Breaking Columnar Transposition (x)

The screenshot shows the MysteryTwister3 software interface with the 'Transposition' tab selected. The main window is titled 'Transposition Analyzer' and displays a table of analysis results. The table has columns for Rank, Value, Key, Mode, and Text. The first few rows of the table are:

#	Value	Key	Mode	Text
1	1083.9352	[7,2,1,6,3,8,5,9]	R-C-C	INCRYPTOGRAPHYATTRANSPOSITIONCIPHERISAMETHODOFENCRYPTIONBYWHICHTHEPOS
2	1079.8348	[1,6,3,8,5,4,9,7,2]	R-C-C	CRYPTOGRAPHYATTRANSPOSITIONCIPHERISAMETHODOFENCRYPTIONBYWHICHTHEPOS
3	888.35394	[4,9,7,2,1,6,3,8,5]	R-C-C	DEINCRIPTOGRAPHYATTRANSPOSITIONCIPHERISAMETHODOFENCRYPTIONBYWHICHTHEPOS
4	844.89621	[7,2,3,1,6,5,4,9]	R-C-C	INCRYPTOGRAPHYATTRANSPOSITIONCIPHERISAMETHODOFENCRYPTIONBYWHICHTHEPOS
5	832.42401	[1,6,3,8,4,9,7,2,3]	R-C-C	CRYPTOGRAPHYATTRANSPOSITIONCIPHERISAMETHODOFENCRYPTIONBYWHICHTHEPOS
6	825.08235	[1,6,3,8,5,4,9,7,2,3]	R-C-C	CRYPTOGRAPHYATTRANSPOSITIONCIPHERISAMETHODOFENCRYPTIONBYWHICHTHEPOS
7	821.93459	[4,9,7,2,1,6,3,8,5]	R-C-C	DEINCRIPTOGRAPHYATTRANSPOSITIONCIPHERISAMETHODOFENCRYPTIONBYWHICHTHEPOS
8	812.92657	[7,2,4,1,6,3,8,5,9]	R-C-C	INCRYPTOGRAPHYATTRANSPOSITIONCIPHERISAMETHODOFENCRYPTIONBYWHICHTHEPOS
9	810.46185	[1,6,3,8,5,4,9,7,2]	R-C-C	CRYPTOGRAPHYATTRANSPOSITIONCIPHERISAMETHODOFENCRYPTIONBYWHICHTHEPOS
10	793.80938	[1,6,4,3,8,5,9,7,2]	R-C-C	CRYPTOGRAPHYATTRANSPOSITIONCIPHERISAMETHODOFENCRYPTIONBYWHICHTHEPOS

The 'Text Input' panel on the left contains the ciphertext: CPPIECYPHHTALEPCHORSTRTENIT EIGIEAACTDRSEDETNSACMNBEI NHNTUASCAYAESPOADNNARM CEECAOONSNTYSSHYHSLOEC SOIEFDGEHETMFTSOSDTRHLIONC TCNUDORIIIOHYLHMGRGHADGA OICEAETEHCTRAFSERNPVTRIT TRDTCTBWPWARCSENLSCTTTHX HTSHXXEMAHEOYNCCRHOPTRW OESERVYRSTETTIRRONIRNENTOL TIOQAINAFQIRNNAEHNHNICOCO RECOSSHMMALMRILASLDUNSHRT. 389 characters, 1 line. 100%.

The 'Text Output' panel on the right shows the decrypted text: INCRIPTOGRAPHYATTRANSPOSITIONCIPHE RISAMETHODOFENCRYPTIONBYWHICHTHE POSITIONSHELDBYUNITSOFLAINTEXTW HICHARECOMMONLYCHARACTERSORG UPSOFCHARACTERSARESHIFTEDACCORDI NGTOAREGULARSYSTEMSOATHATTHECIPHE RTEXTCONSTITUTESAPERMUTATIONOFTHE PLAINTEXTTHATTHEORDEROFTHEUNITSIS CHANGEDTHEPLAINTEXTISREORDEREDM ATHEMATICALLYABJECTIVEFUNCTIONIS EDONTHECHARACTERSPPOSITIONSTOENCRYPTANDANINVERSEFUNCTIONTODECRYPT.

Below the output text, a note says: This template shows the analysis of columnar transposition and a key recovery algorithm. This approach is not guaranteed to work (WHYHEWASSOANGRY...) is not found at the first run, simply try to run again.

At the bottom, it says: The ciphertext was retrieved from the CC1-3 challenge of MysteryTwister I, where you can find many more ciphertexts that were encrypted with a columnar transposition. You can try to decode them with this template.

Link: <http://www.mysterytwister3.org/de/alte-mysterytwister-spiele/cc1-3>



# Basic Crypto II (LAB IV)

- **Task IV. Repeat the analysis at lab (20 MINS)**
  - Transposition (Scytale)
    - Brute Force:  
Try different parameters shown in the slide
    - Try also assignments 25-27 (from assignment M4 slides)
  - Transposition (Columnar)
    - Heuristic:  
Try different parameters shown in the slide
    - Try also assignments 28-30 (from assignment M4 slides)



# Breaking cipher VI

## ■ Breaking Mixed cipher (i)

- **ADFGX** and **ADFGVX** are named after the used letters: A,D,F,G,V, and X
- Invented during WWI by German officer **Fritz Nebel** in **1918**
  - **ADFGX was used for the first time on March 1. 1918 on the Western Front**
  - **ADFGVX was used for the first time on June 1. 1918 on the Western and Eastern Front**
- Ciphers were broken by the French officer **Georges Painvin** in **June 1918**



# Breaking cipher VI

## ■ Breaking Mixed cipher (ii)

- What is an **ADFG(V)X cipher?**
  - Fractionating Cipher
    - 1. Substitution
    - 2. Transposition
- Small example:

	A	D	F	G	V	X
A	P	R	M	Y	U	N
D	3	L	Z	G	E	S
F	8	C	7	1	Q	O
G	V	2	9	I	T	B
V	4	0	6	K	X	H
X	5	A	J	N	D	F

Polybius Square

“**HELLO**” → **Substitution** → “**VXDVDDDDFX**”

“**VXDVDDDDFX**” → **Transpo.** → “**VXDV** → “**VDFXDXDDVD**”  
**DDDD**  
**FX**”



# Breaking cipher VI

## ■ Breaking Mixed cipher (iii)

- What is the keyspace size of the **ADFG(V)X** cipher?

- 1. **Substitution** keyspace size:

$$\mathbf{ADFGX} = 25! \quad \mathbf{ADFGVX} = 36!$$

- 2. **Transposition** keyspace size ( $n = \text{max key length}$ ):

$$= \sum_{i=1}^n n!$$

- Example: transposition key length up to 15 (**ADFGVX**):

$$= 36! \cdot \left( \sum_{i=1}^{15} n! \right) \approx 2^{178.44}$$



# Breaking cipher VI

## ■ Breaking Mixed cipher (iv)

- What is the keyspace size of the **ADFG(V)X** cipher?

- 1. **Substitution** keyspace size:

$$\mathbf{ADFGX} = 25! \quad \mathbf{ADFGVX} = 36!$$

- 2. **Transposition** keyspace size ( $n = \text{max key length}$ ):

$$= \sum_{i=1}^n n!$$

- Example: transposition key length up to 15 (**ADFGVX**):

$$= 36! \cdot (\sum_{i=1}^{15} n!) \approx 2^{178.44}$$



# Breaking cipher VI

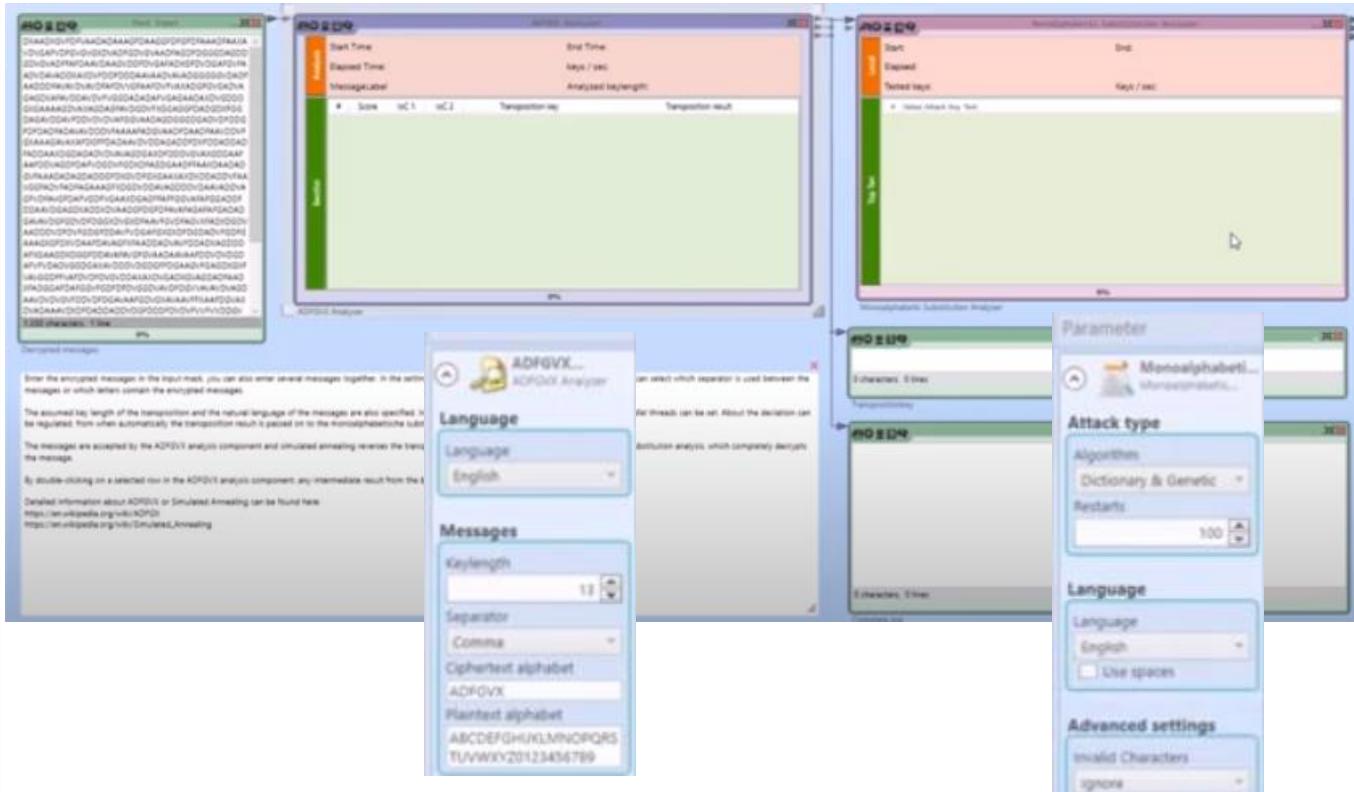
## ■ Breaking Mixed cipher (v)



# Breaking cipher VI



## ■ Breaking Mixed cipher (vi)





# Breaking cipher VI

## ■ Breaking Mixed cipher (vii)

Analysis	Start Time:		1/14/2020 3:40:10 PM		End Time:		1/14/2020 3:40:32 PM	
	Elapsed Time:		00:00:22		keys / sec:		10309 (235014)	
Best list	MessageLabel		1		Analyzed keylength:		13	
	#	Score	IoC 1	IoC 2	Transposition key	Transposition result		
	1	200899	6.5	0.9	LIADJHFKBMCGE	EGIUYSDFMUHSNYDNKHJLMVXIESNKUWHALEKQJIESNK		
	2	134214	5.21	0.57	LIADJHFMBMCGE	EGIUESDFMUJGNYDNKHJLMVGQSNKUWHALEKN1IESN		
	3	129685	5.71	0.53	LIADJHFMBKCGE	EGIS0SDFMUTGNYDNHKJLMVXCKSNKUTKAHLEKKPIESNIV		
	4	125062	5.93	0.5	LIADJHFMCBGE	EGISUYDFMUSHNYDNHKJLMVXEISNKUTEGHLEKQJIESNIE		
	5	113683	5.89	0.44	LIADJMCHFBGE	EGGUUYDFMSUHNYDNHKJLMVEXISNKTWGHLJEKQIESOI		
	6	111494	5.84	0.42	LIAMCDJHFKBGE	EGSIUYDFSMUHNYBJNKJLMEVXISNHEUWGLJEKQIEUANI		
	7	99648	5.49	0.37	DELIAMJHFKBGC	ZEGIUYSDFSUHMNYBNKJLMDXIWSNHUWGEHLKKQJCEUI		
	8	96528	5.35	0.36	LEDMAIJHFKBGC	BYKIUYVAXUAUHMZNANKJLJAPXIWMTHUWGBKLKKQJCCW		
	9	95314	5.31	0.35	FELMDUHAKBGC	TA2IIYUDSAXHMHZMNEJLDPSIWSNTUKGEHKKLQQJICENW		
	10	94710	5.51	0.34	GFLIJHAKBMDEC	NEIIYZSVAXHSAOYNEHNJLPSIDXXNUKHSATKLQKJKENWU		



# Breaking cipher VI

## ■ Breaking Mixed cipher (viii)

Monalphabetic Substitution Analysis				
Local	Start:	1/14/2020 3:40:26 PM	End:	1/14/2020 3:40:32 PM
Elapsed:	00:00:06			
Tested keys:	Keys / sec:			
#	Value	Attack	Key	
1	-4.39408	G	subtionacdefghijklmpqrwxyz	INCRYPTOGRAPHYTHEADFGVXCIPHERWASAFIELD CIPHER USED BY THE GERMAN
2	-13.69601	D	abcdefghijklmnpqrstuvwxyz	EGIUYSDFMUHSNYDNKHJLMVXIESNKUWAHLEKQJIESNKUBAKJCYDNKMUR



# Basic Crypto II (LAB V)

## ■ Task V. Repeat the analysis at lab (10 MINS)

### – Mixed

Try different parameters shown in the slide

- Try also assignments 31-36 (from assignment M4 slides)



# Cryptology for IoT

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

M4.6 Briefing of the session  
M4.7 Tasks to do in the lab

Prof.: Guillermo Botella