Week 1 Practical: *CryptTool 2 overview*

Hassan Chizari and Madhu Khuruna

University of Gloucestershire

hchizari@glos.ac.uk

UNIVERSITY OF GLOUCESTERSHIRE

Overview

1. Caesar Cipher
2. Vigenère cipher
3. Bringing it all together
4. Post-sessional work

UNIVERSITY OF GLOUCESTERSHIRE

Alphabet index

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Table: Alphabet and their indices

UNIVERSITY OF GLOUCESTERSHIRE

Overview

- Developed and used by Julius Caesar
- Substitution cipher
- Encryption achieved through shifting each character by a *fixed* amount
- For each character (C_p) in a plaintext, each character is shifted using:

$$E(C_p) = (C_p + Shift) mod\ 26$$

Character shifting

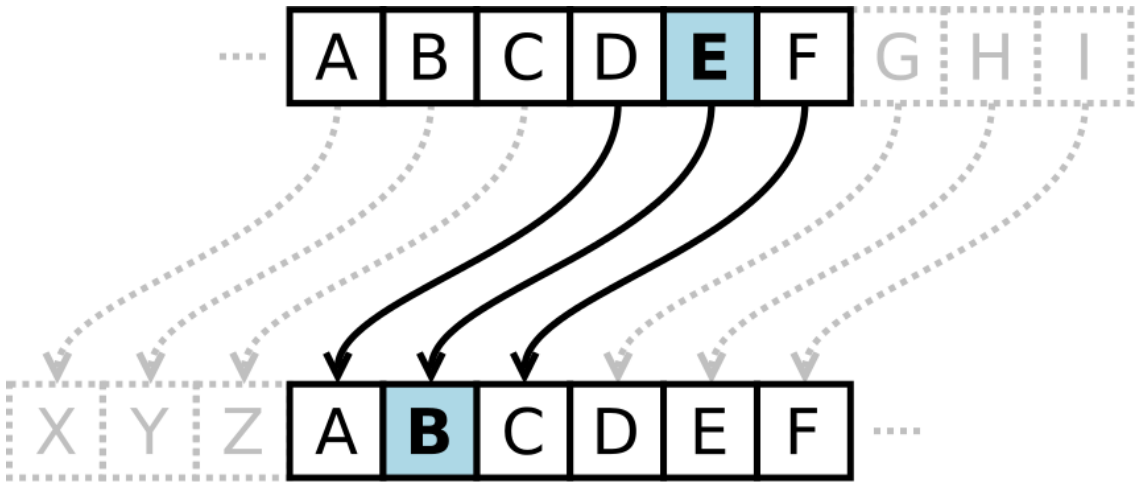

Figure: How Caesar cipher works, from [1]

How it works

- Imagine that we have the plaintext P: *roses are red*
- Suppose we are going to encrypt P using Caesar cipher with Shift $S = 3$
- The resulting ciphertext C then becomes: *urvhvduhuhg*

Working with CryptTool 2

- Provides implementations of different cryptographic algorithms
- For our practical session, download it from here
- Once installed, run it to see its functionalities

How CrypTool 2 looks like

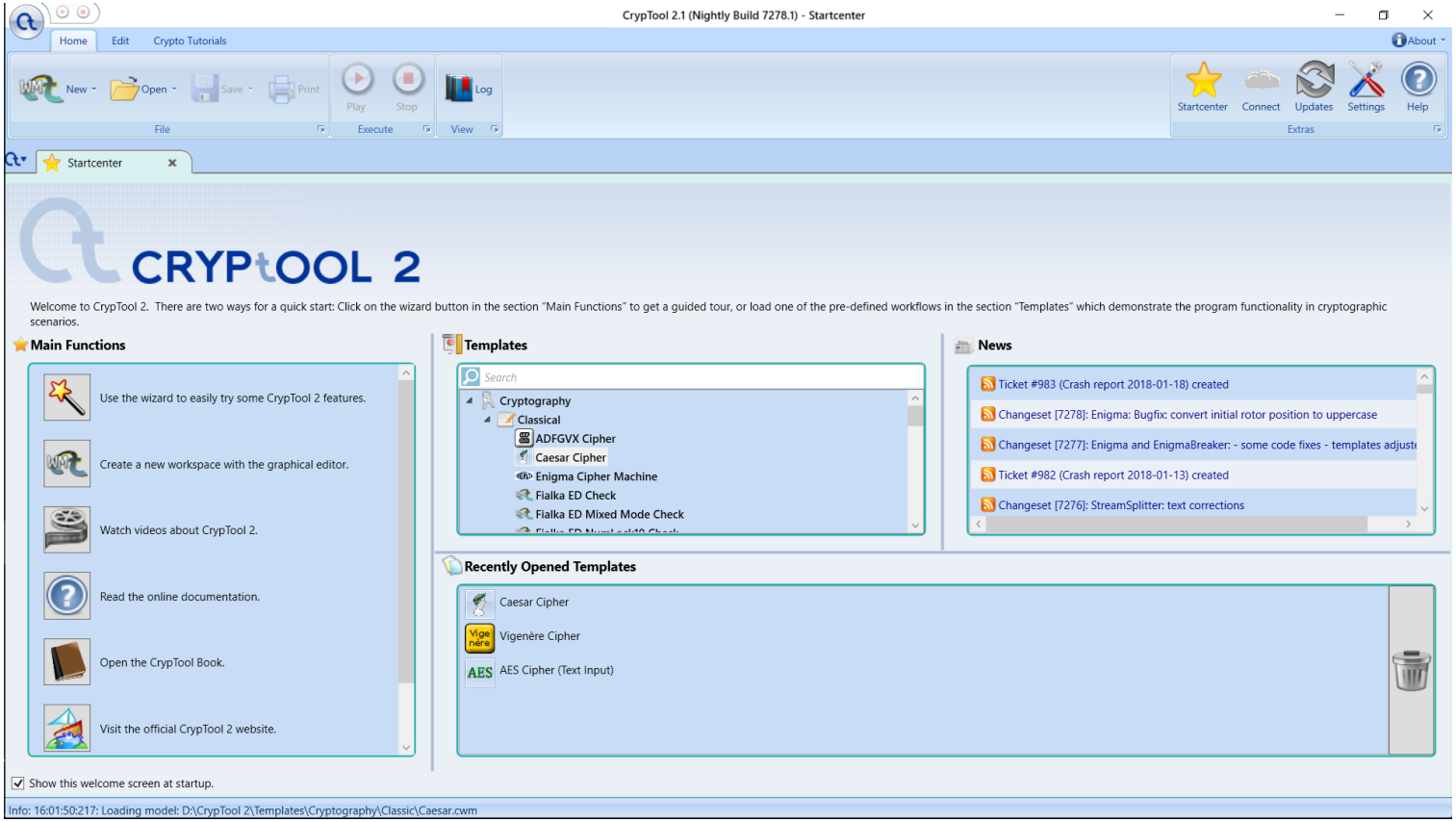

Figure: CrypTool 2 interface

UNIVERSITY OF GLOUCESTERSHIRE

Caesar cipher on CryptTool 2

- From the *CryptTool 2* startup menu, click *Cryptography*
- Then click *Classical* and then select *Caesar cipher*
- In the plaintext section of *TextInput*, type in: *roses are red*
- Then in the *Key as integer* box, set it to 3
- Finally click on the *Play* button to execute

Caesar cipher on CrypTool 2

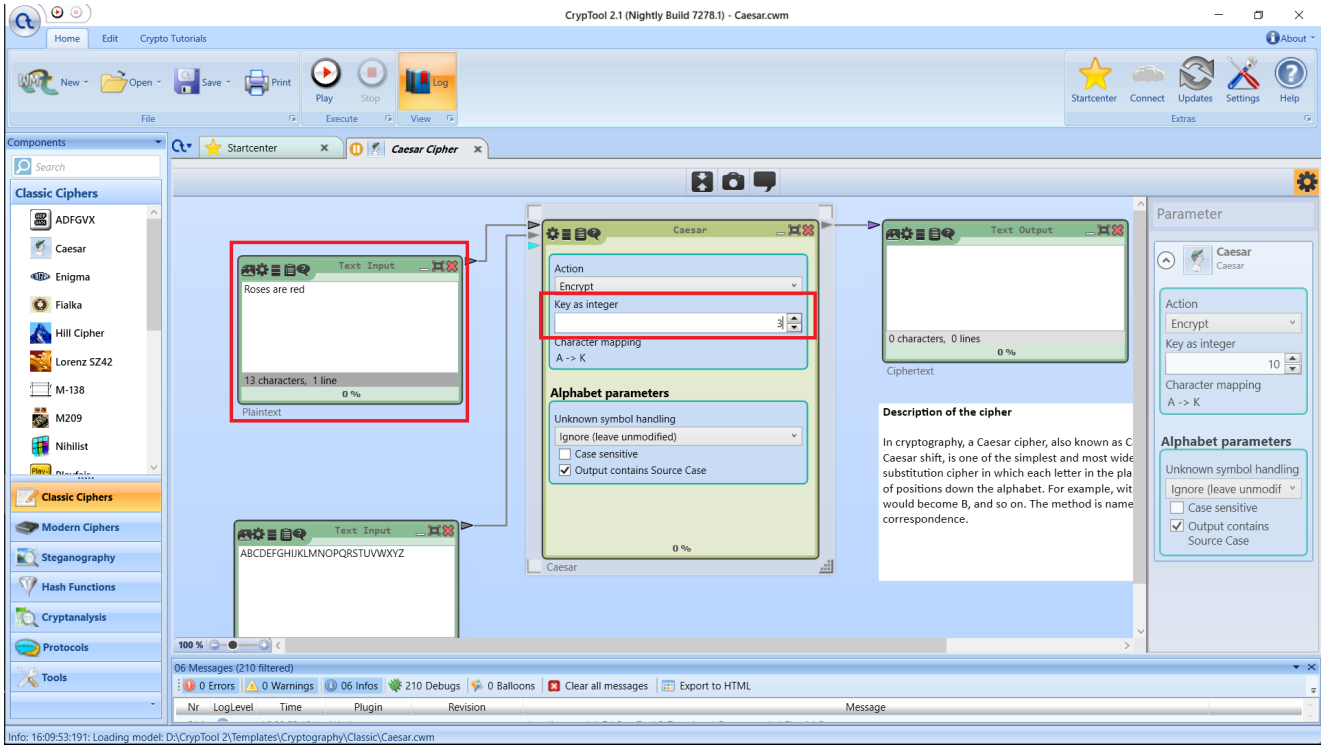

Figure: Caesar cipher on CrypTool 2

Exercise

- Imagine you have been given this plaintext P: *Eren needs to go to Wall Rose*
- Using Caesar cipher and a shift number of your choice (between $0 \sim 25$), encrypt P
- Send the encrypted ciphertext C to the student next to you and ask him/her to decrypt it

Overview

- Developed by Balise de Vigenère
- Can be thought of as a modified version of the Caesar cipher
- Features the use of *key* rather than shifting characters around
- Makes the use of frequency analysis more difficult

Overview

- Given a plaintext $P = \{p_1, p_2, ..., p_m\}$, and key $K = \{k_1, k_2, .., k_n\}$
- Ciphertext $C = \{c_1, c_2, ..., c_m\}$ is obtained using

$$c_i = (p_i + k_i) mod\ 26$$

- Decryption

$$p_i = (c_i - k_i) mod\ 26$$

- Plaintext P: *Roses are red*
- Key K: *KING*

UNIVERSITY OF GLOUCESTERSHIRE

How it works

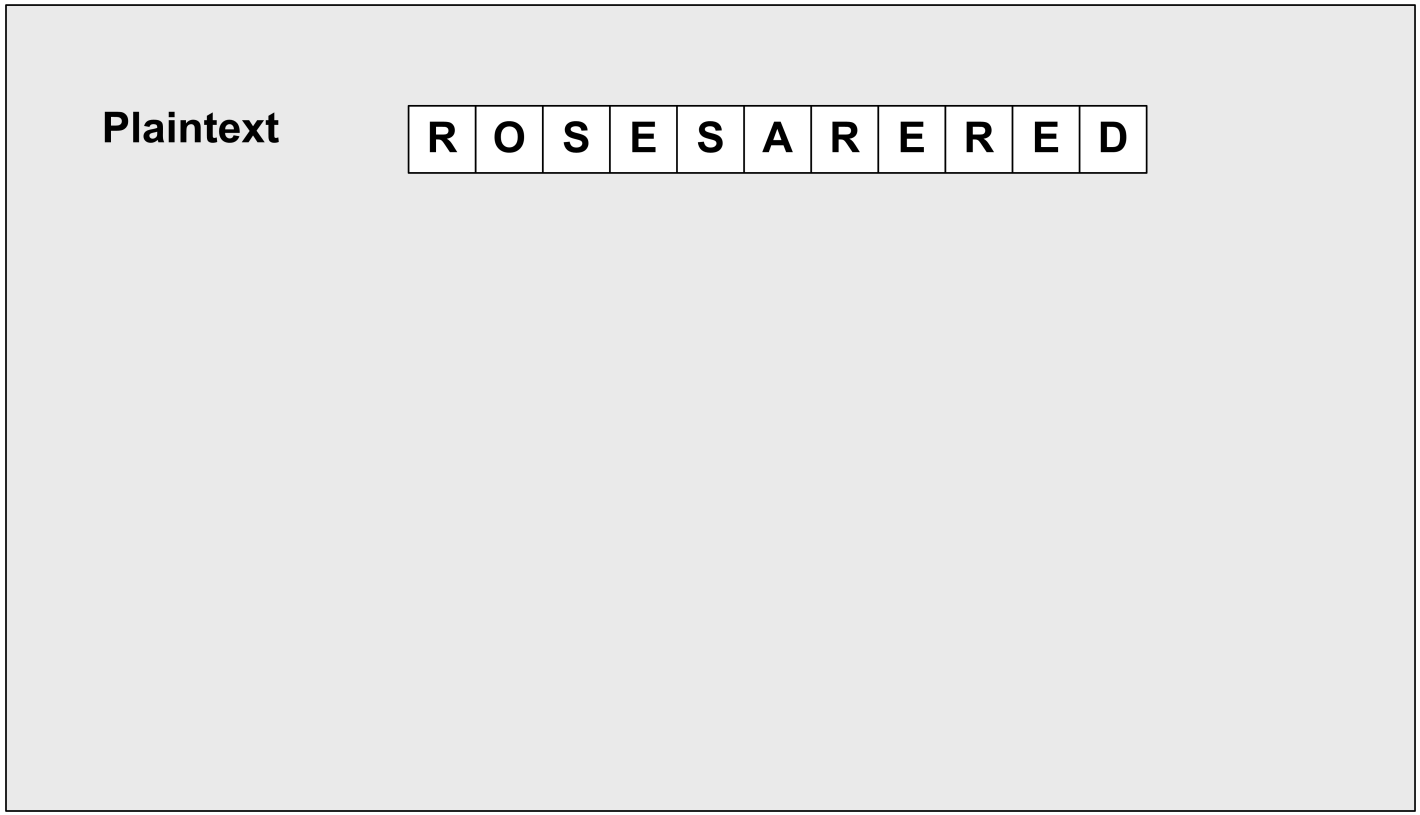

Figure: How Vigenère cipher works

How it works

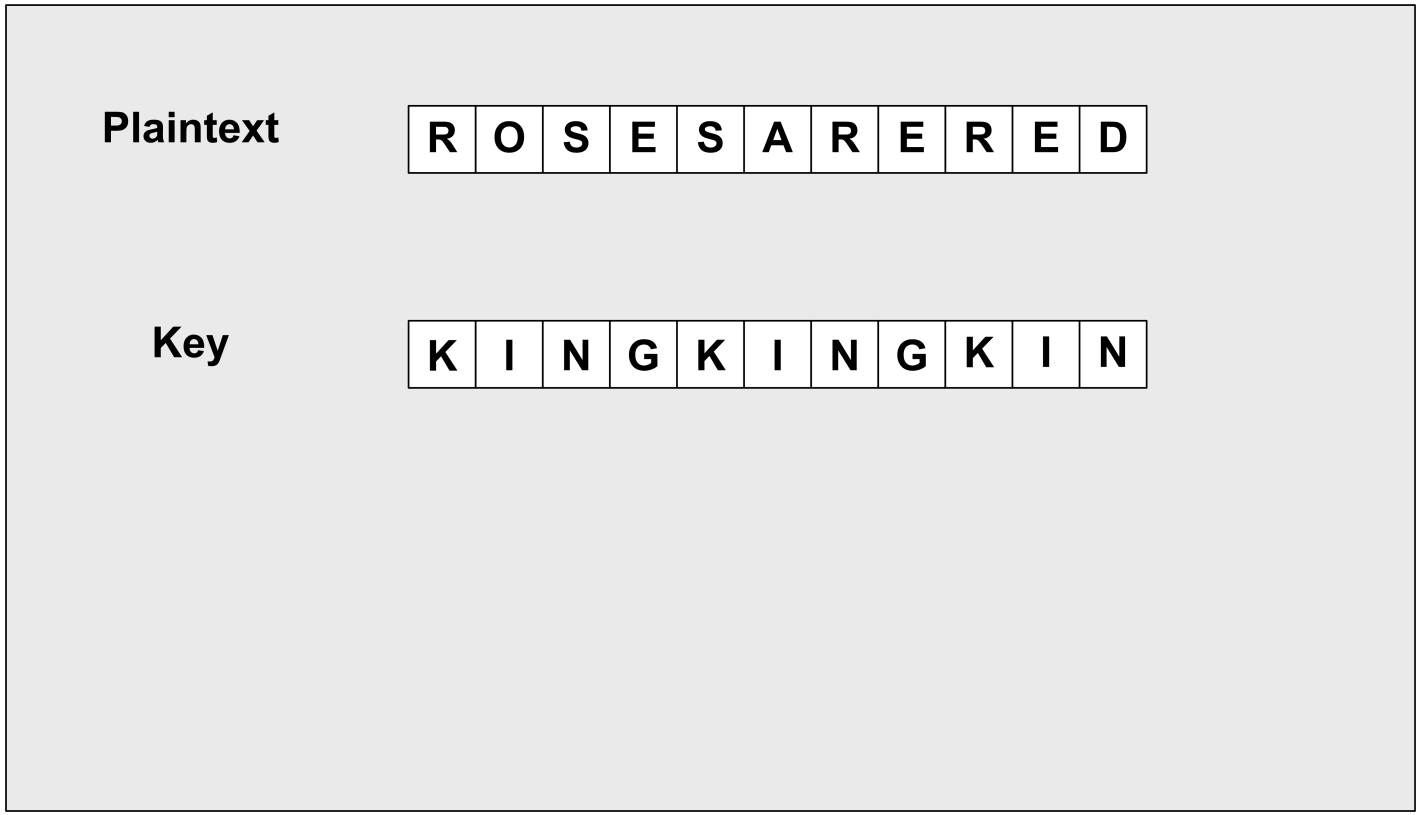

Figure: How Vigenère cipher works

How it works

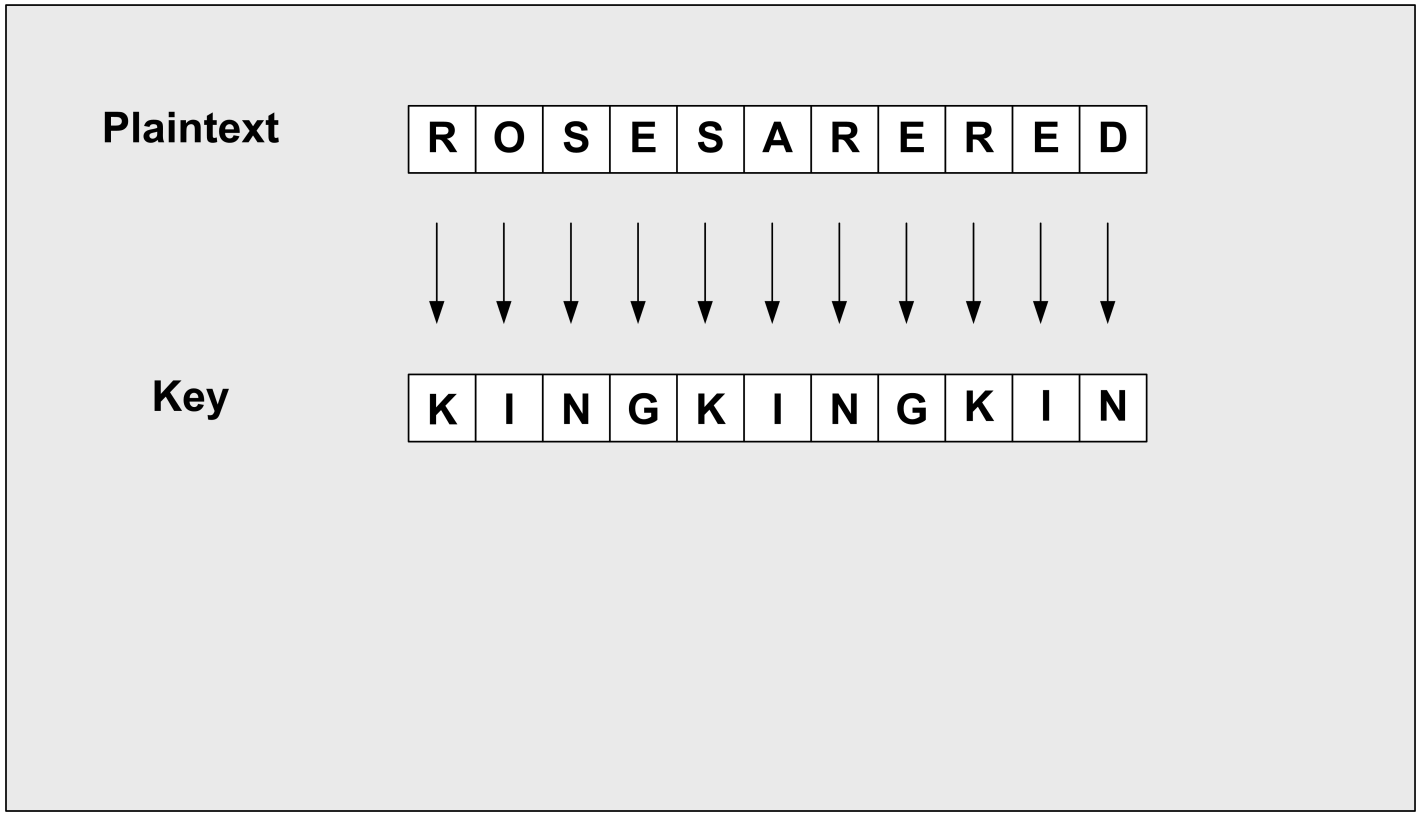

Figure: How Vigenère cipher works

How it works

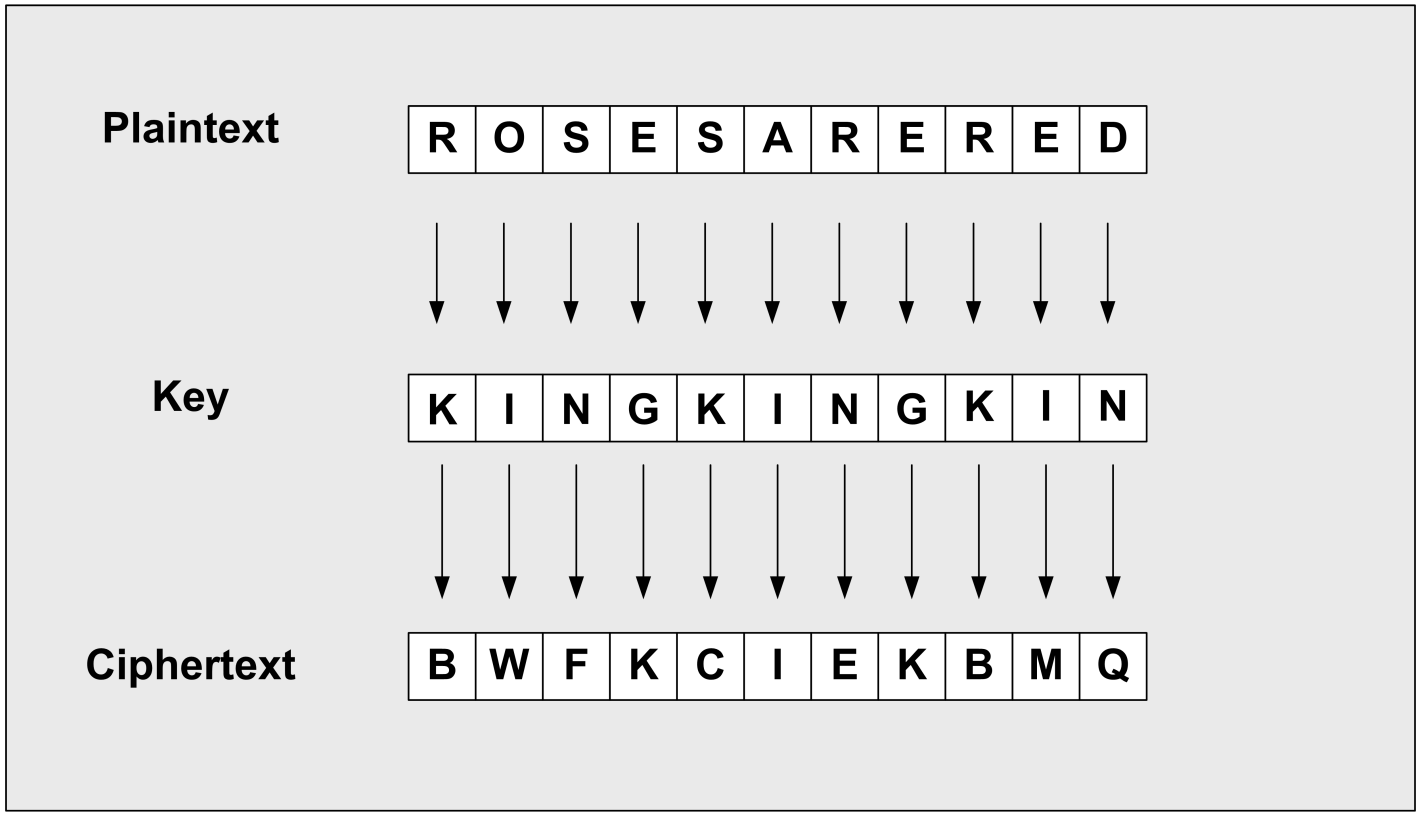

Figure: How Vigenère cipher works

Vigenère cipher on CryptTool 2

- From the *CryptTool 2* startup menu, click *Cryptography*
- Then click *Classical* and then select *Vigenère cipher cipher*
- In the plaintext section of *TextInput*, type in: *roses are red*
- Then in the *Key* box, type in: *KING*
- Finally click on the *Play* button to execute

Vigenère cipher on CrypTool 2

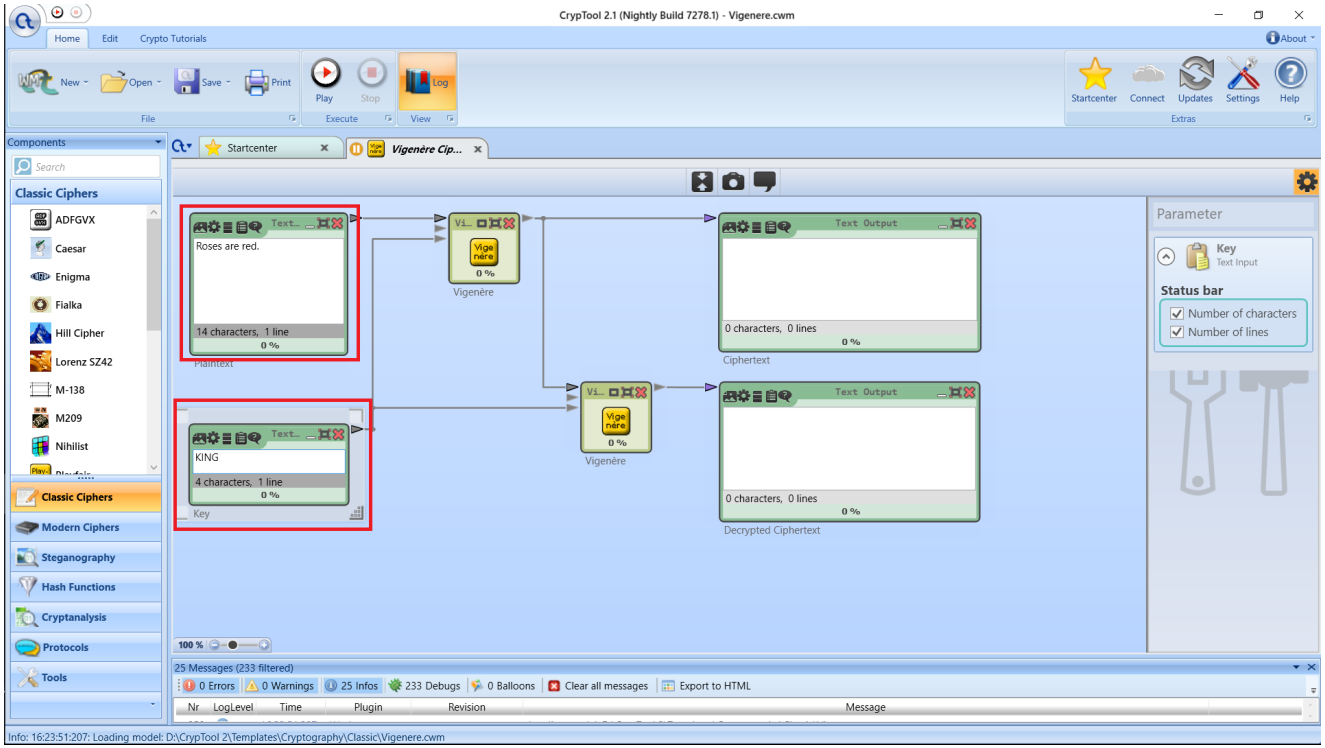

Figure: Vigenère cipher on CrypTool 2

Bringing it all together

- Today we looked at *CryptTool 2*
- We looked at both *Caesar* and *Vigenère* ciphers
- Next week: *Number theory and other classical ciphers*

Post-sessional work

- Based on your understanding of the two ciphers which we looked at, write a critial report discussing how they can be cracked
- You need to use both your understanding of the practicals as well as the post-sessional reading materials as *starting points*
- Upload your completed work to *Moodle* before next *Monday*

References

[1] learncryptography. *Caesar Cipher*. https://learncryptography.com/classical-encryption/caesar-cipher. Accessed: 23-10-2017. 2017.

Q & A