Keele UNIVERSITY

Using Python and Flask to build a web-based cipher

Computer Science - Mini-placement research week
16-20 June 2025

Marco Ortolani, Senior Lecturer in Computer Science
m.ortolani@keele.ac.uk

THIS IS KEELE

Day 1

A bit about me

Keele UNIVERSITY
School of Computer Science and Mathematics

- **Marco Ortolani**
  - I got my PhD in Computer Engineering from the University of Palermo (Italy) in 2004
  - In 2017 I was a visiting researcher under a Fulbright grant at the Missouri University of Science and Technology,
  - and in March 2019 I joined Keele University
- My research interests regard
  - intelligent data analysis, machine learning, and knowledge discovery,
  - applications to big data analysis, security, and pervasive systems
- In particular, I'm interested in:
  - **interpretable** machine learning
  - bias, fairness and **ethical issues** in AI

THIS IS KEELE

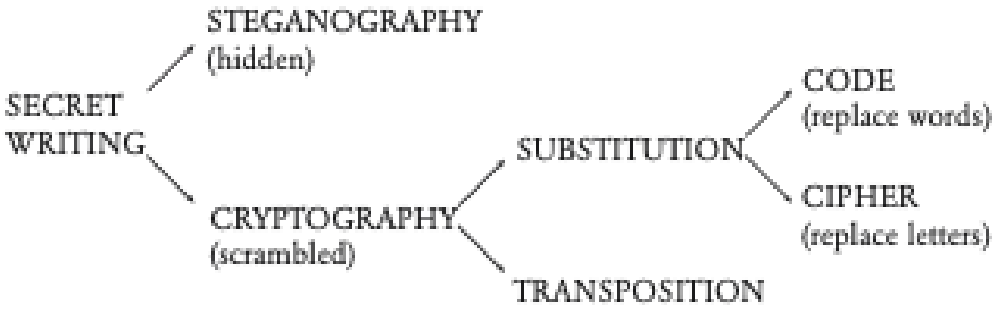
Outline – day 1

Keele UNIVERSITY
School of Computer Science and Mathematics

- Intro: Using Python and Flask to build a web-based cipher
- Caesar cipher
- Setup git account
- Show app

THIS IS KEELE

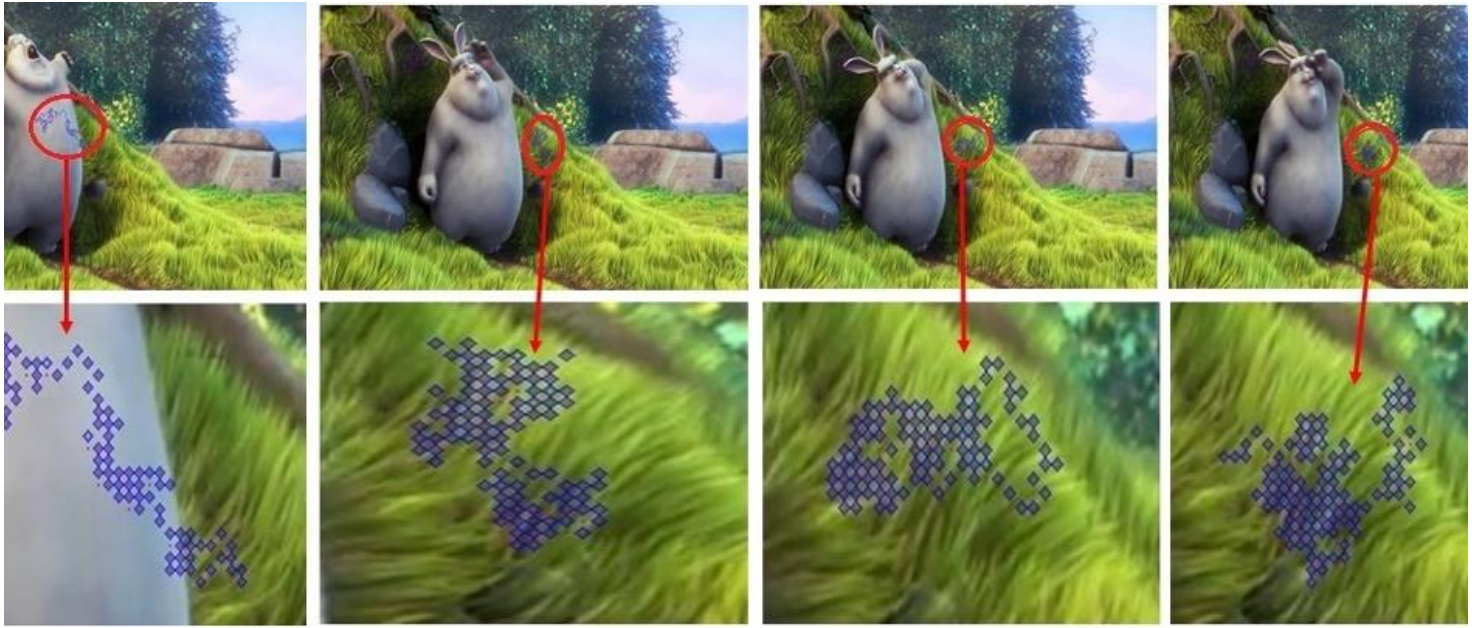
The science of secret writing



From: Singh, S., 2002. *The Code Book: How to Make It, Break It, Hack It, Or Crack it*. Delacorte Press.

Watermark videos

Keele UNIVERSITY
School of Computer Science and Mathematics

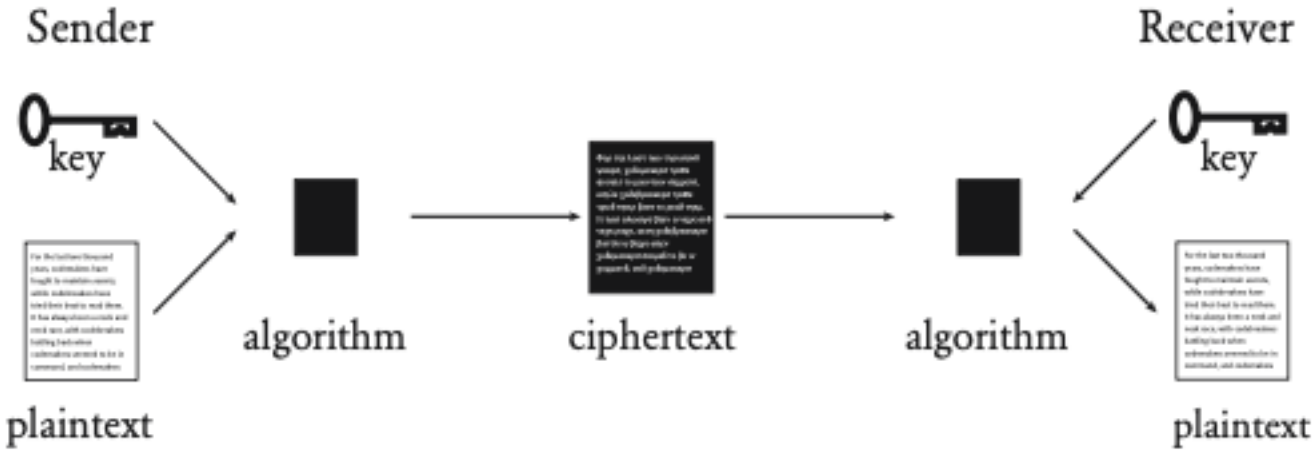


Unchangeable Video Content (Steganography)
Project by Dr Nadia Kanwal

THIS IS KEELE

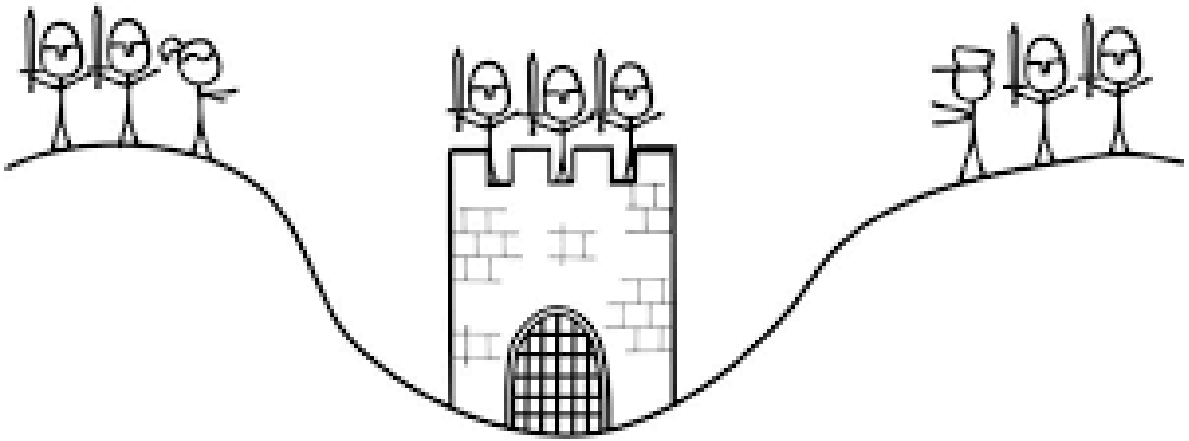
Encryption and ciphers

Keele University
School of Computer Science and Mathematics



From: Singh, S., 2002. *The Code Book: How to Make It, Break It, Hack It, Or Crack it*. Delacorte Press.

Communicating over insecure channels



The two generals problem

Work

6p99472x96-5000.app.github.dev

Codes and secrets 🔐 on GitHub Codespaces and Flask

Edit `templates/index.html` or `vigenere.py` and refresh to see your changes!

Enter your text

This is a test

Encrypt Decrypt Clear

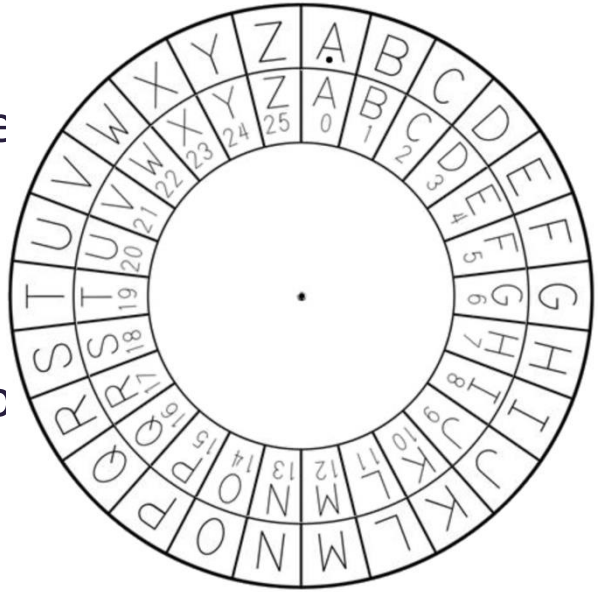
Processed text

Llkj ml s xgjx

Class activity

Keele UNIVERSITY
School of Computer Science and Mathematics

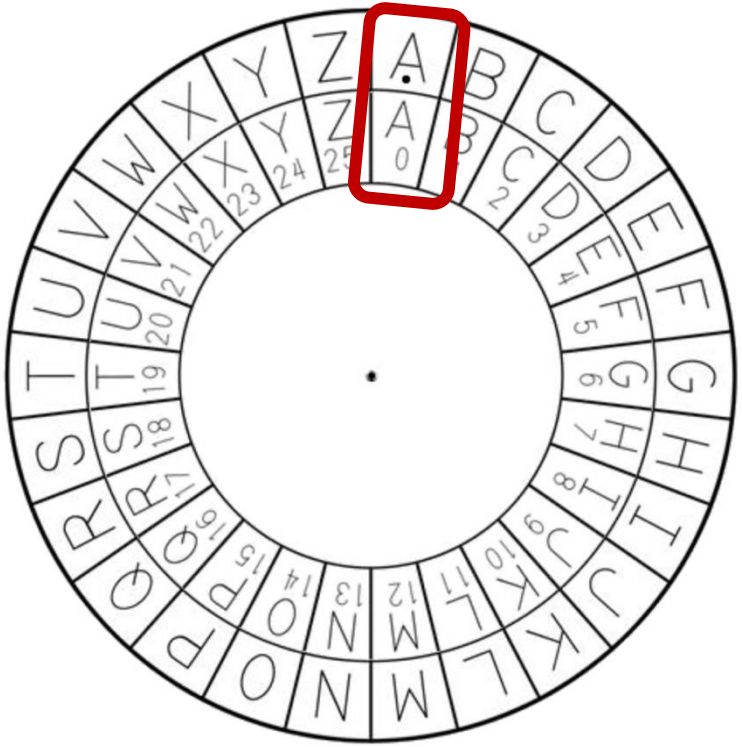
- Use your cipher wheel to try and decrypt a given ciphertext
- The wheel uses a “key” to encrypt (a numbe
  relative positions of the two wheels)
- Your tasks consists in guessing the key, so yo
  text



THIS IS KEELE

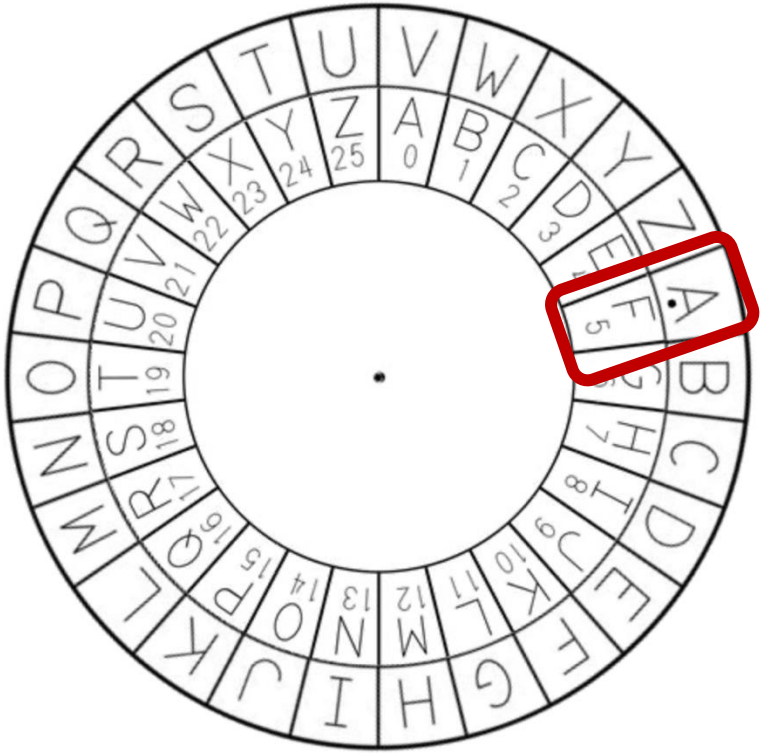
Class activity

- For instance, key=0 means no shift
  - ciphertext will be the same as cleartext



Class activity

- key=1 means shifting the external wheel so that A corresponds to
  - ciphertext will be the same as cleartext



Class activity

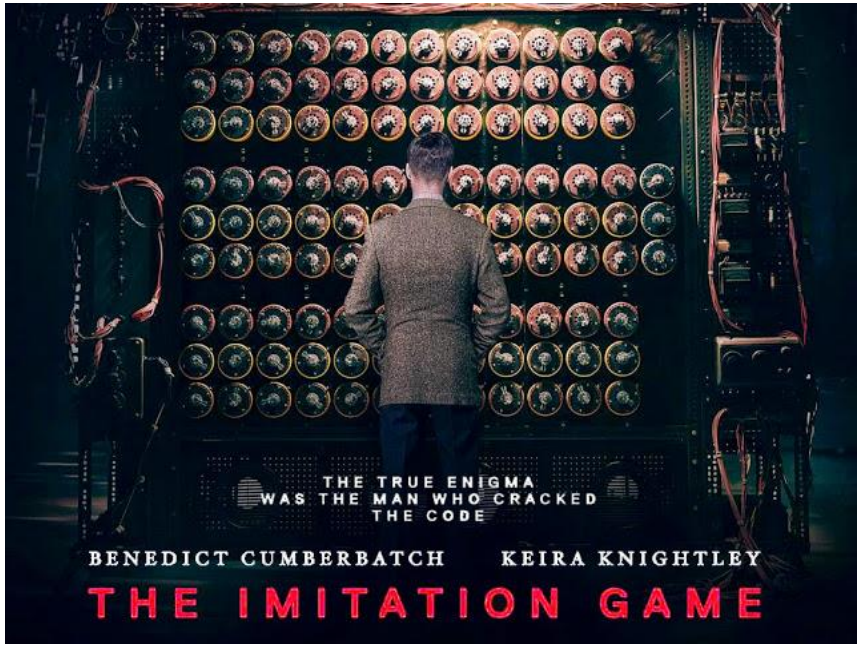
Keele UNIVERSITY
School of Computer Science and Mathematics

- Ciphertext

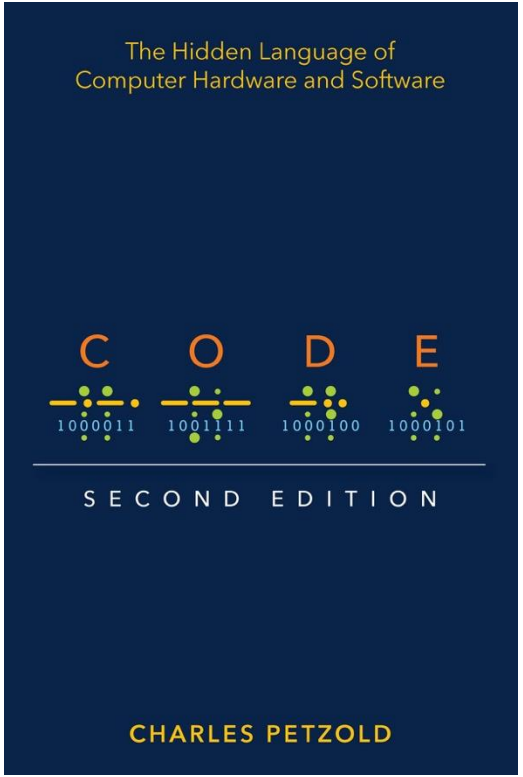
SZERMT UFM DRGS XLWVH ZG PVVOV

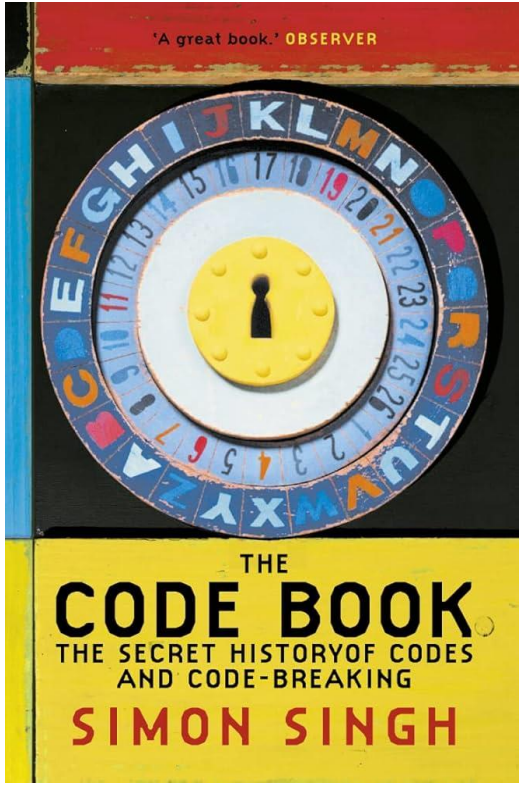
Some extra material

Keele UNIVERSITY
School of Computer Science and Mathematics



Some extra material





Activity

Keele UNIVERSITY
School of Computer Science and Mathematics

- Go to: https://github.com and create an account (if you don't have one already)
  - You can also sign up for the Student Developer Pack

    https://education.github.com/pack
- Read Chapter 1 from The code book
- Decrypt

SZERMT UFM DRGS XLWVH ZG PVVOV

THIS IS KEELE

Day 2

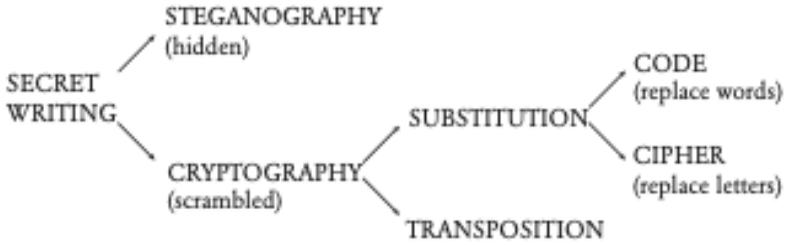
Outline – day 2

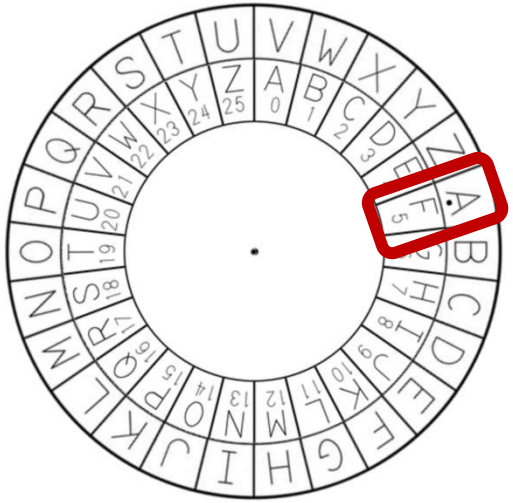
Keele UNIVERSITY
School of Computer Science and Mathematics

- Recap on ciphers
- Vigenère cipher
- Breaking the Babington Plot

Substitution ciphers

- Caesar's cipher is a substitution cipher





Substitution ciphers

Keele UNIVERSITY
School of Computer Science and Mathematics

- Caesar's cipher is a substitution cipher

Plain alphabet	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
Cipher alphabet	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

Plaintext	i came, i saw, i conquered
Ciphertext	L FDPH, L VDZ, L FRQTXHUHG

THIS IS KEELE

Substitution ciphers

Keele UNIVERSITY
School of Computer Science and Mathematics

- Ciphertext

```
SZERMT UFM DRGS XLWVH ZG PVVOV
```

- Plaintext (using “our” wheel)

```
***** *** **** ***E* ** *EE*E
```

- V -> E

THIS IS KEELE

Substitution ciphers

Keele UNIVERSITY
School of Computer Science and Mathematics

- Ciphertext

  SZERMT UFM DRGS XLWVH ZG PVVOV

- Plaintext (using “our” wheel)

  HAVING FUN WITH CODES AT KEELE

- V -> E (then we got the key!)

THIS IS KEELE

Substitution ciphers

Keele UNIVERSITY
School of Computer Science and Mathematics

- Caesar's cipher is a substitution cipher

Plain alphabet	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
Cipher alphabet	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

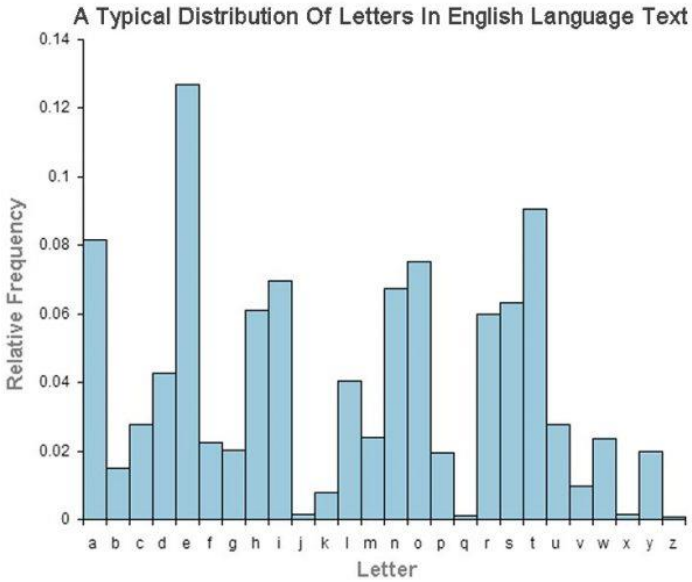
Plaintext	i came, i saw, i conquered
Ciphertext	L FDPH, L VDZ, L FRQTXHUHG

THIS IS KEELE

Substitution ciphers

Keele UNIVERSITY
School of Computer Science and Mathematics

- Simple substitution ciphers are intrinsically **vulnerable** to statistical **cryptanalysis**



THIS IS KEELE

Substitution ciphers

Keele UNIVERSITY
School of Computer Science and Mathematics

- Ciphertext

```
SZERMT UFM DRGS XLWVH ZG PVVOV
```

- Plaintext (using “our” wheel)

```
***** *** **** ***E* ** *EE*E
```

- V -> E

THIS IS KEELE

Ciphers and plots

Keele UNIVERSITY
School of Computer Science and Mathematics

Mary Queen of Scots

More complex ciphers

Keele University
School of Computer Science and Mathematics

- Using more ciphers at the same time

Plain alphabet	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
Cipher alphabet 1	F Z B V K I X A Y M E P L S D H J O R G N Q C U T W
Cipher alphabet 2	G O X B F W T H Q I L A P Z J D E S V Y C R K U H N

- Plaintext wheel
- Ciphertext CHKFP

Vigenère cipher

Keele UNIVERSITY
School of Computer Science and Mathematics

- We can use a keyword to encode different shif for the sequence of letters in the plaintext

Plaintext	D	O	G	S
Keyword	P	E	T	S
Ciphertext	S	S	Z	K

THIS IS KEELE

Vigenère cipher

Keele UNIVERSITY
School of Computer Science and Mathematics

Plaintext	D	O	G	S
Keyword	P	E	T	S
Ciphertext	S	S	Z	K

- D → S
- We use “P” as the shift (P is the 16th letter of the alphabet

Vigenère cipher

Keele UNIVERSITY

School *of* Computer Science *and* Mathematics

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

THIS IS KEELE

Breaking Vigenère

Keele University
School of Computer Science and Mathematics

FHZQ US KFQ PCYZ TYYF WZJX WFPW. TYC CUVCZ MLQF FRJX IERA TYC FRRN. FHV QOOKQ IICJ OODC IHVL IE XGHE KFQ WFPP.

TYGE IJ MGR KGYE. XMP WZJX HVJB.

TYC EIXL TAJ ZQEE EUVVL ROI EAOU.

Breaking Vigenère

Keele UNIVERSITY
School of Computer Science and Mathematics

Group 1: F U Q T F W T C M F I A F Q K I T I K Y H H J

Group 2: H S P Y W F Y U L R R V O Q I O V E F W E M Z

Group 3: Z K C Y Z P C V Q J Q O O C L G P P G R G W J

Group 4: Q F Y F J W Z C F X D D X H F P T I M E M X B

THIS IS KEELE

Breaking Vigenère

Keele University
School of Computer Science and Mathematics

Group	Most Frequent Letter(s)	Frequency
1	F	4
2	R, V, F, Y, O, E	2 (tie)
3	C, P, G	3 (tie)
4	F	4

Try it out

Keele UNIVERSITY
School of Computer Science and Mathematics

- See tasks
- Use code: https://github.com/marcoortolani/vigenere.git

THIS IS KEELE

Day 3

Work

6p99472x96-5000.app.github.dev

Codes and secrets 🔐 on GitHub Codespaces and Flask

Edit `templates/index.html` or `vigenere.py` and refresh to see your changes!

Enter your text

This is a test

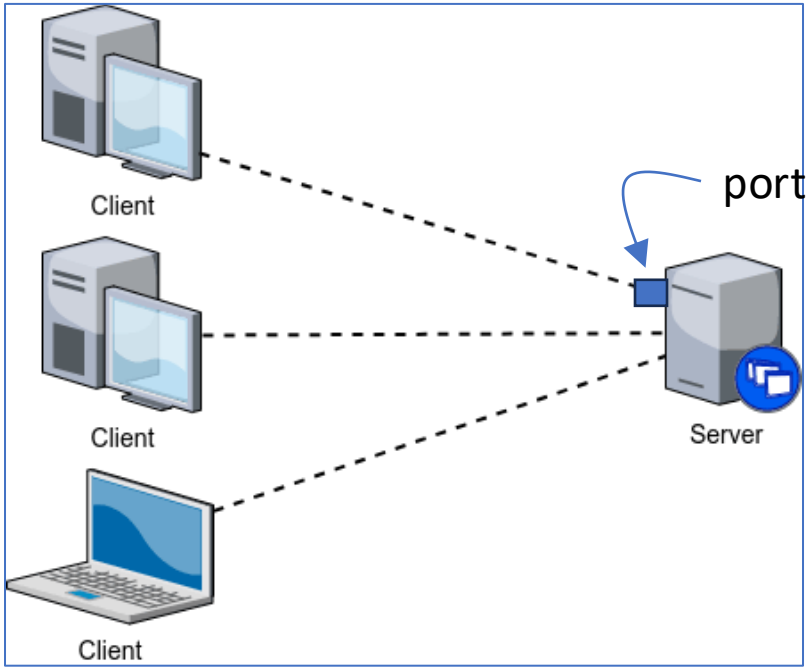
Encrypt Decrypt Clear

Processed text

Llkj ml s xgjx

The cipher server

Keele UNIVERSITY
School of Computer Science and Mathematics



Coding the Caesar cipher

Keele UNIVERSITY
School of Computer Science and Mathematics

- Loop through each character in the input text.
- If the character is a **letter**:
  - Check if it's uppercase or lowercase.
  - **Shift** it forward in the alphabet by the given number.
  - Make sure it **wraps around** (Z goes back to A).
- If it's not a letter (e.g. space, punctuation)
  - keep it the same

THIS IS KEELE

Coding the Caesar cipher

Keele UNIVERSITY
School of Computer Science and Mathematics

- **Key Python Features Used**
  - `char.isalpha()` → checks if the character is a **letter**
  - `ord(char)` → gets the **number code** of the character
  - `chr(number)` → gets the **letter** from the number code
  - `% 26` → wraps around the alphabet (only 26 letters)

THIS IS KEELE

Activity

- Look into the `caesar_exercise.py`
- The method for encryption is implemented, but the method for decryption is not working
- Try to fix it!

Activity

- Look into the `vigenere_exercise.py`
- The method for encryption is implemented, but the method for decryption is not working
- Try to fix it!

Decrypting enemy code

Keele UNIVERSITY
School of Computer Science and Mathematics

Enigma and “the bombe”

try the emulator: https://www.101computing.net/enigma-machine-emulator/

THIS IS KEELE

Day 4

Suggestions for research directions

Keele UNIVERSITY
School of Computer Science and Mathematics

- The Enigma machine
- The Zimmermann Telegram
- Steganography: Hiding messages in images, music, or social media posts
- Encryption: More Than Secrets — Powering Digital Signatures, Integrity & Trust
- Other ciphers:
  - One-time pad, book cipher, pigpen cipher

THIS IS KEELE

Suggestions for research directions

Keele UNIVERSITY
School of Computer Science and Mathematics

- Frequency analysis beyond basic letter frequency to digrams (TH, ER, IN) and trigrams (THE, AND, ING)
- The Kasiski Examination for Vigenère
- Attacking the ciphers
  - Meet-in-the-Middle Attacks
  - Chosen Plaintext/Ciphertext Attacks

Keele UNIVERSITY

Thank you

Keele University
Newcastle-under-Lyme
Staffordshire
ST5 5BG
+44 (0)1782 732000

THIS IS KEELE