

Cryptography challenge: facilitator notes

The Alan Turing Institute

Last updated: October 27, 2023

General comments

Timings, etc.

Whom to ask if you need help.

1 Introduction

For any students who are struggling to crack the initial cipher, the best place to start is the first and last lines, which are respectively “Hello Bob” and “Alice”. Hints to this include the capitalisation of the names, as well as the repeated letters in Bob’s name. With these letters filled in, the rest of the message becomes

Hello Bob,

Ho* a*e *o*?

Le*'* *ee* o* *o**a*!

Alice

(The answer is Monday.)

Symmetric ciphers

2 Caesar cipher

The Caesar cipher page did not seem to pose any problems in the 2023 sessions. The answer for the question at the bottom is `HIDDENMESSAGE`.

For very advanced students, you may wish to ask them why there are only 26 possibilities (or 25 useful ones) for a Caesar cipher. The answer is that there are only 26 letters in the English alphabet, so shifting by 27 is the same as shifting by 1—this is a very early example of the modular arithmetic which will be covered in the second half.

3 Monoalphabetic ciphers

For why texts may deviate from the standard frequency distribution: a simple one is the use of different spellings, e.g. American vs British English. More examples can be found at https://en.wikipedia.org/wiki/Letter_frequency.

One thing worth pointing out is that frequencies are only really stable if the text is long enough.

The decoding challenge is probably the part of the first half that students will spend the most time on, if only because there is a lot of trial-and-error involved. It is generally obvious that the most common letter in English is E, but the next most common letters tend to depend on the text from which it is drawn, so are less immediately useful.

From the frequency analysis, students should be able to guess that ciphertext I corresponds to plaintext E. Furthermore, in the ciphertext, the trigram PVI appears regularly. Together this implies that P corresponds to T and V corresponds to H. Sensible next steps would be to try to match up the remaining common letters, namely Y and A: these correspond to A and O in plaintext respectively.

The full answers are:

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

4 Vigenère cipher

Reading the Vigenère square the other way around works because the square is symmetric: at a more fundamental level this is because the encoding is effectively carried out by adding two numbers, and addition is a commutative operation.

We found that providing a concrete example of calculating the IoC for a short piece of text was helpful for aiding students' understanding.

To prove that the IoC for long, random text is 1: let the length of the text be N . Then, we have that $n_A = n_B = \dots = N/26$, and so:

$$\text{IoC} = 26 \cdot \frac{N/26(N/26 - 1) \cdot 26}{N(N - 1)} = \frac{N - 26}{N - 1},$$

and as $N \rightarrow \infty$, this tends to 1. (Strictly, we only need that $N \gg 26$ or that $N/26 \gg 1$, which the question states.)

For the decoding challenge, the key is (quite literally) KEY. The text is the opening of Turing's 1936 paper *On Computable Numbers, with an Application to the Entscheidungsproblem* (DOI: [10.1112/plms/s2-42.1.230](https://doi.org/10.1112/plms/s2-42.1.230)).

5 Enigma

Asymmetric ciphers

6 Modular arithmetic I

7 RSA scheme I

8 Modular arithmetic II

9 RSA scheme II

10 Cryptography Game Resources