

Introduction to Cryptography

This exploration sheet contains some more codebreaking puzzles. During the session, we will learn about a few more encryption techniques, and also how to break them.

Our aim is to learn and enjoy the art of codebreaking. This joy will be lost if we resort to technology prematurely. Solve the challenges without resorting to computers or the internet.

Challenge 1: Each of the following sets contains messages encrypted using Shift cipher (from the previous session). Decode the messages and find the plaintext.

Note: some errors have been introduced to make this more challenging.

Team 1:

a) RFLDLIKSVKYV TYREXVPFLNREKJVVZEKYVNFGCV

b)

OFEFKXFNYVIVKYVGRKYDRPCVRUXFZEJKVRUNYVIVKYVIVZJEFGRKYRE
UCVRLVRKIRZC

c)

IPKYDZTJPDGYFEZVJRIVGIFWFLEUTVTRLJVFWKYVZINFEUVIWLCCPRDRQ
ZEXSVRLRP

d) SVRFLIJVCWVMVIPFEVVCJVZJRCIVRUPKRBVE

e) UFFEVKYZEXVMVIPURPKYRKJTIVJPFL

f) KYVFECPKYZEXNVYRMIKFWVRIZJWVRIZKJVCW

Team 2:

a) ORLBHEFRYSRIRELBARRYFRVFGNXRA

b) WBYYLWBVAGURWHTTYREWUTTYRQGURWNZSVYYRQWNEF

c) JRYYQBARVFORGGREGUNAJRYYFNVQ

d) LBHZHFGORGURPUNATRLNHIVFUGBFRRVAGURJBHEYQ

e) GURBAYLGUNATJRUNIRGBSRNEVFSRNEVGFRYS

f) QBBARGUVATRIRELQNLGUNGFPNERFLBH

Team 3:

a) KNHxDABNUONENAHKXMHNUBNRBJUANJMHJCJINW

b) ZKZJUJVFIEXFUIVRIBVJKDFDVEKJKYRKNDLJKWFTLJKFJVRYCZXYK

c) KFRTREURPNYVEKYFLSVKIRPVUKYPZEKYVQFXQNFEX

d) KYVFECHKYZEXNVYRMVKFWVRTZJWVRIZKJVCW

e) HXDVDBCKNCQNLQJWPNHXDFRBQCXBNNRWCQNFAXUM

f)

BYANJMVXENNENAHQFNANUNCWXXWNNENALXVNCXHXDFRCQXDCUNHE
RWPQJYYRNR

Team 4:

a) LOIYBCOVPOFOBIYXOOVCOSCKVBOKNIDKUOX

b)

CZBOKNVYFOOFOBIGROBOIYEQYVODXYYXOOFOBMYWODYIYEGSDRYDFVO
KFSXQRKZZSNB

c) DROAESMULBYGXPHYHTEWZCYFOBDROVKJINYQ

d)

NYXYDQYGROBODROZKDRWKIVOKNQYSXCDOKNGROBODROBOSCXYZKDR
KXNVOKFOKDBKSV

e) DROYXVIDRSXGGORKFQDYPOKBSCPOKBSDCOVP

f) IYEWECDLQJROMRKDQOIYEGSCRDXCDOXDROGOBVN

- How did you crack the code?
- Would you consider shift cipher to be strong? Why or why not?

Challenge 2: Norse Code

Elder futhark is Europe's oldest runic alphabet, used in Scandinavia to write Old Norse between the second and eighth centuries AD. Below are the names of 11 Old Norse gods written in elder futhark runes. The Anglicised names are given for nine of them. Match the correct names to their runes, and translate into English the names of the two remaining gods.

Runic Symbols	English Script
1. 𐀪𐀦𐀹𐀾	a) Baldur
2. 𐀵𐀶𐀹	b) Dallinger
3. 𐀵𐀶𐀮𐀦𐀦	c) Day
4. 𐀮𐀦𐀶𐀹	d) Earth
5. 𐀦𐀶𐀮𐀦	e) Freya
6. 𐀶𐀹𐀮𐀦𐀦𐀶𐀦	f) Freyr
7. 𐀶𐀶𐀹𐀾	g) Ithun
8. 𐀮𐀮𐀦𐀦𐀶𐀹	h) Night
9. 𐀶𐀹𐀮𐀦𐀹	i) Sun
10. 𐀶𐀮𐀦𐀦	j) ?
11. 𐀶𐀶𐀦	k) ?

Challenge 3: Match the state names in the different scripts.

English	Kannada	Bengali	Random Font
Rajasthan	ಸಿಕ್ಕಿಂ	সিকিম	★**▲**
Odisha	ತೆಲಂಗಾಣ	নাগাল্যান্ড	☆*□*●*
Sikkim	ಗೋವಾ	উত্তরাখণ্ড	**●*■*■*
Kerala	ರಾಜಸ್ಥಾನ	গোভা	*▼▼*□*■*
Nagaland	ಕೇರಳ	ওড়িশা	****▲▼**■
Goa	ಉತ್ತರಾಖಂಡ	তেলেঙ্গানা	☆**●*■*
Uttarakhand	ఒడిశా	রাজস্থান	◇□*
Telengana	నాగార్జునం	কেরালা	*****○

- How did you match the names?
- What are the features of each script?
- What were your assumptions regarding each language?

Challenge 4: Transposition Cipher

In this type of encryption, the letters of the plaintext remain the same. However, their positions are rearranged.

E.g. 'mynameisashwinguha' is written in two columns.

M	N	M	I	A	H	I	G	H
Y	A	E	S	S	W	N	U	A

Then the two rows are appended to get the ciphertext 'MNMIAHIGHYAESSWNUA'.

Decode the following messages which have been encrypted using transposition.

1.

FNUNIDTAOSNDVEHLRNDSEEEERROETRPMQEBRHSLAVAOSEEYTXSDTUIMI
MOYANSACP.

2.

TADMABAKDLLMUOPMANERIELISBPATIODNNCYSRELTISULGTTTPCKAIHCT
TOAEURUNNEEIOWONLAOOD.

- How can did you break the code?
- Would you consider this technique strong?

Challenge 5: Design your own method to encrypt text.

Encode the following text in your method.

‘It is often said that mathematics is the language of science. But the language analogy is incomplete. It is also an incredibly powerful system of reasoning.’

We will compare the different methods of encryption during the session.