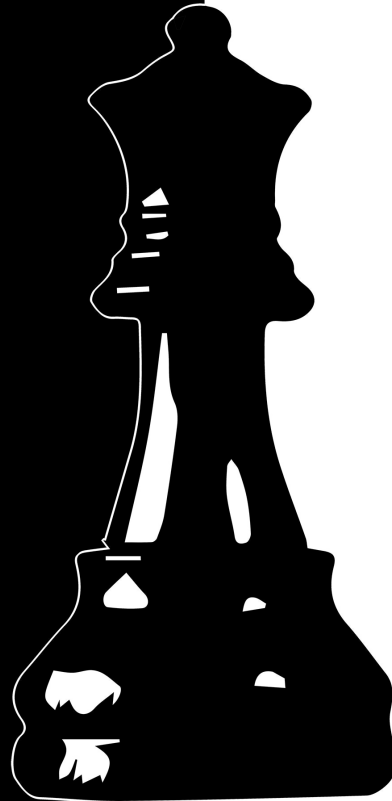


UNIVERSITY OF
Southampton

TROJAN

NATIONAL CIPHER CHALLENGE 2014

Starts 2nd October
Register online
from 18th September



LESSON PLANS

Cryptography Lesson Plan 1

Class: Cracking the Caesear shift ciphers.

Resources:

Leaflet “On substitution ciphers”.

Two handouts each with a plaintext and a cipher table

Teachers’ solutions for the handouts.

One OHP slide with cipher text to crack, and partial decrypt and solution.

Starter: (10 minutes approximately) Uses handouts for Groups A and B

Encryption exercise – split the class into groups A and B. Give each group the enclosed text to encipher using the given code. Encourage accuracy AND secrecy! Answers enclosed with handouts.

Main activity: (40 minutes approx) Uses OHP

- *Introduce the idea of a substitution cipher in general and the Caesar shift in particular.*
- *Suggest trial and error as a deciphering technique.*
- *Work through a very simple Caesar shift (by 3).*
- *Split the class again, swap over the ciphertexts from the starter exercise and get them to tackle them.*

Plenary (approx 10 minutes)

Discuss how to make the code harder to crack using a rule that is harder to determine, but remark on the need for an easy to remember rule (stressed agents must remember it and can’t write it down!) Mention “keyword” substitution.

University of Southampton National Cipher Challenge Lesson Plans

Handout for lesson 1.

GROUP A

Code: Caesar shift by 2

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
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

Plaintext

There were plenty of schools in the world, but they were all run either by the various churches or the Guilds. Miss Butts objected to churches on logical grounds and deplored the fact that the only Guilds that considered girls worth educating were the Thieves and the Seamstresses. It was a big and dangerous world out there and a girl could do worse than face it with a sound knowledge of geometry and astronomy under her bodice.

From "Soul Music" by Terry Pratchett.

University of Southampton National Cipher Challenge Lesson Plans

Handout for lesson 1.

GROUP B

Code: Caesar shift by 4

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
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

Plaintext

The four houses are called Gryffindor, Hufflepuff, Ravenclaw and Slytherin. Each house has its own noble history and each has produced outstanding witches and wizards. While you are at Hogwarts, your triumphs will earn your house points, while any rule-breaking will lose house points. At the end of the year the house with the most points is awarded the House Cup, a great honour. I hope each of you will be a credit to whichever house becomes yours.

From "Harry Potter and the Philosopher's Stone" by J.K. Rowling.

Teachers' solutions to encryption challenge

Ciphertext A

VJGTG YGTG RNGPVA QH UEJQQNU KP VJG YQTNF, DWV VJGA YGTG
CNN TWP GKVJGT DA VJG XCTKQWU EJWTEJGU QT VJG IWKNFU. OKUU
DWVVU QDLGEVGF VQ EJWTEJGU QP NQIKECN ITQWPFU CPF
FGRNQTGF VJG HCEV VJCV VJG QPNA IWKNFU VJCV EQPUKFGTGF
IKTNU YQTVJ GFWECVKPI YGTG VJG VJKGXGU CPF VJG
UGCOUVTGUUGU. KV YCU C DKI CPF FCPIGTQWU YQTNF QWV VJGTG
CPF C IKTN EQWNF FQ YQTUG VJCP HCEG KV YKVJ C UQWPF
MPQYNGFIG QH IGQOGVTA CPF CUVTQPQOA WPFGT JGT DQFKEG.

Ciphertext B

XLI JSYV LSYWIW EVI GEPIIH KVCJJMRHSV, LYJJPITYJJ, VEZIRGPEA
ERH WPCXLIVMR. IEGL LSYWI LEW MXW SAR RSFPI LMWXSVC ERH
IEGL LEW TVSHYGIH SYXWXERHMRK AMXGLIW ERH AMDEVHW.
ALMPI CSY EVI EX LSKAEVXW, CSYV XVMYQTLW AMPP IEVR CSYV
LSYWI TSMRXW, ALMPI ERC VYPI-FVIEOMRK AMPP PSWI LSYWI
TSMRXW. EX XLI IRH SJ XLI CIEV XLI LSYWI AMXL XLI QSWX TSMRXW
MW EAEVHIH XLI LSYWI GYT, E KVIEX LRSYV. M LSTI IEGL SJ CSY
AMPP FI E GVIHMX XS ALMGLIZIV LSYWI FIGSQIW CSYVW.

University of Southampton National Cipher Challenge Lesson Plans

OHP Slide for lesson 1

Ciphertext

WKH HDVLHVW PHWKRG RI HQFLSKHULQJ D WHAW PHVVDJH LV WR
UHSODFH HDFK FKDUDFWHU EB DQRWKHU XVLQJ D ILAHG UXOH, VR
IRU HADPSOH HYHUB OHWWHU D PDB EH UHSODFHG EB G, DQG
HYHUB OHWWHU E EB WKH OHWWHU H DQG VR RQ.

Partial decrypt: Guess that the first word is “the” so that t is enciphered as W, h as K and e as H. This suggests a shift by 3:

the eDVLeVt PethRG RI eQFLSheULQJ D teAt PeVVDJe LV tR UeSODFe eDFh
FhDUDFteU EB DQRtheU XVLQJ D ILAeG UXOe, VR IRU eADPSOe eYeUB
OetteU D PDB Ee UeSODFeG EB G, DQG eYeUB OetteU E EB the OetteU e DQG
VR RQ.

The word teAt could be tent, test or text, with text fitting with the shift by 3; the word OetteU which occurs twice, would decipher to “letter” confirming our guess.

Code: Caesar shift by 3

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
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

The easiest method of enciphering a text message is to replace each character by another using a fixed rule, so for example every letter a may be replaced by d, and every letter b by the letter e and so on.







Cryptography Lesson Plan 2

Class: Cracking keyword substitution ciphers – emphasises letter frequency analysis and team work.

Resources:

Leaflet “On substitution ciphers”.

OHP 1 containing ciphertext

OHP 2 Containing expected frequency table and incomplete actual frequencies.

Handout summarising details of deciphering technique.

OHP 3 With further thoughts on disguising the text.

Starter: (10 minutes approximately) (Uses OHP 1)

Split the class into teams and get them to count the letter frequencies in the ciphertext. Emphasise the need for speed and accuracy. Maybe set the scene as a race against time.

Main activity: (30 minutes approx) (Uses OHP 1 and OHP 2 and handout)

- *Introduce the idea of a keyword cipher to make encryption more secure and more memorable (see “On substitution ciphers”).*
- *Discuss the hunt for common words and letters and introduce frequency analysis – show a table of common frequencies and check it against the examples in lesson 1.*
- *Discuss the speed improvements given by parallel processing of the text. Split into 26 teams to do a frequency analysis of the given ciphertext on OHP 1. {It may be worth remarking that standard computer attacks on ciphers use this idea of parallel processing to speed up the attack.}*
- *Whole class session to construct frequency table, compare with expected frequencies (computed from percentages) and identify the letters “e”*

Plenary (20 minutes approx) (Uses OHP 2 and, time permitting OHP 3)

Draw together the intelligence gained by the groups and crack the cipher together. (You may wish to give out the handout summarising the technique after completing the exercise.)

If time permits (OHP 3):

- *Discuss how to make the code harder to crack by disguising the letter groups.*
- *Remark that the frequency table can mislead for non-standard or foreign language texts! Examine the extract from the book “A Void” by Georges*



OHP Slide 1 for lesson 2

Ciphertext

VEP HYXHLVHTP MO AWFJYFLT H RFNEPS HJNEHAPV FL VEFU ZHC FU
VEHV FV FU PHUC VM KPKMSFUP VEP IPCZMSY MS IPCNESHUP, HLY
EPLRP VEP RFNEPS HJNEHAPV. VEFU FU FKNMSVHLV, APRHWUP FO
VEP UPLYPS EHU VM IPPN VEP RFNEPS HJNEHAPV ML H NFPRP MO
NHNPS, VEP PLPKC RHL RHNWVSP VEP NHNPS, YFURMXPS VEP IPC, HLY
SPHY HLC RMKKWLF RHVFMLU VEHV EHXP APPL PLRSCNVPY ZFVE FV.
EMZPXPS FO VEP IPC RHL AP RMKKFVVPY VM KPKMSC FV FU JPUU
JFIPJC VM OHJJ FLVM PLPKC EHL YU.



Handout for lesson 2

STAGE 1 – P is the commonest letter in the ciphertext so could stand for e - may the first word is the:

the HYXHLtHTe MO AWFJYFLT H RFNheS HJNhHAet FL thFU ZHC FU thHt Ft
FU eHUC tM KeKMSFUe the IeCZMSY MS IeCNhSHUe, HLY heLRe the RFNheS
HJNhHAet. thFU FU FKNMStHLt, AeRHWUe FO the UeLYeS hHU tM IeeN the
RFNheS HJNhHAet ML H NFeRe MO NHNeS, the eLeKC RHL RHntWSe the
NHNeS, YFURMXeS the IeC, HLY SeHY HLC RMKKWLFRRHtFMLU thHt hHXe
AeeL eLRSCNteY ZFth Ft. hMZeXeS FO the IeC RHL Ae RMKKFtteY tM
KeKMSC Ft FU JeUU JFIeJC tM OHJJ FLtM eLeKC hHLYU.

STAGE 2 We see the single letter word H, and the four letter word thHt in the first line - guess that H encodes the letter a.

the aYXaLtaTe MO AWFJYFLT a RFNheS aJNhaAet FL thFU ZaC FU that Ft FU
eaUC tM KeKMSFUe the IeCZMSY MS IeCNhSaUe, aLY heLRe the RFNheS
aJNhaAet. thFU FU FKNMStaLt, AeRaWUe FO the UeLYeS haU tM IeeN the
RFNheS aJNhaAet ML a NFeRe MO NaNeS, the eLeKC RaL RaNtWSe the NaNeS,
YFURMXeS the IeC, aLY SeaY aLC RMKKWLFRRatFMLU that haXe AeeL
eLRSCNteY ZFth Ft. hMZeXeS FO the IeC RaL Ae RMKKFtteY tM KeKMSC Ft
FU JeUU JFIeJC tM OaJJ FLtM eLeKC haLYU.

STAGE 3 The two 2 letter words Ft FU are probably it is meaning that F encodes i and U encodes s:

the aYXaLtaTe MO AWiJYiLT a RiNheS aJNhaAet iL this ZaC is that it is easC tM
KeKMSSise the IeCZMSY MS IeCNhSase, aLY heLRe the RiNheS aJNhaAet. this is
iKNMStaLt, AeRaWse iO the seLYeS has tM IeeN the RiNheS aJNhaAet ML a
NieRe MO NaNeS, the eLeKC RaL RaNtWSe teh NaNeS, YisRMXeS the IeC, aLY
SeaY aLC RMKKWLiRatiMLs that haXe AeeL eLRSCNteY Zith it. hMZeXeS iO
the IeC RaL Ae RMKKitteY tM KeKMSC it is Jess JiIeJC tM OaJJ iLtM eLeKC
haLYs.

STAGE 4: haXe = have, easC = easy and so on - we get the following extract from Simon Singh's excellent history of codes and ciphers, The Code Book:

"The advantage of building a cipher alphabet in this way is that it is easy to memorise the keyword or keyphrase, and hence the cipher alphabet. This is important, because if the sender has to keep the cipher alphabet on a piece of paper, the enemy can capture the paper, discover the key, and read any communications that have been encrypted with it. However if the key can be committed to memory it is less likely to fall into enemy hands."



OHP Slide 3 for lesson 2

Obscuring a substitution cipher

1. We can disguise the word structure by regrouping the letters into blocks:

VEPHY XHLVH TPMOA WFJYF LTHRF NEPSH JNEHA PVFLV EFUZH
CFUVE HVFVF UPHUC VMKPK MSFUP VEPIP CZMSY MSIPC NESHU
PHLYE PLRPV EPRFN EPSHJ NEHAP VVEFU FUFKN MSVHL VAPRH
WUPFO VEPUP LYPSE HUVMI PPNVE PRFNE PSHJN EHAPV MLHNF
PRPMO NHNPS VEPPL PKCRH LRHNV WSPVE PNHNP SYFUR MXPSV
EIPIC HLYSP HYHLC RMKKW LFRHV FMLUV EHVEH XPAPP LPLRS
CNVPY ZFVEF VEMZP XPSFO VEPIP CRHLA PRMCK FVVPY VMKPK
MSCFV FUJPU UJFIP JCVMO HJJFL VMPLP KCEHL YU

2. We can distort the frequency table – this text was adapted for last years cipher challenge!

Augustus, who has had a bad night, sits up blinking and purblind. Oh what was that word (is his thought) that ran through my brain all night, that idiotic word that, hard as I'd try to pin it down, was always just an inch or two out of my grasp - fowl or foul or Vow or Voyal? - a word which, by association, brought into play an incongruous mass and magma of nouns, idioms, slogans and sayings, a confusing, amorphous outpouring which I sought in vain to control or turn off but which wound around my mind a whirlwind of a cord, a whiplash of a cord, a cord that would split again and again, would knit again and again, of words without communication or any possibility of combination, words without pronunciation, signification or transcription but out of which, notwithstanding, was brought forth a flux, a continuous, compact and lucid flow: an intuition, a vacillating frisson of illumination as if caught in a flash of lightning or in a mist abruptly rising to unshroud an obvious sign - but a sign, alas, that would last an instant only to vanish for good.

From "A Void" by Gilbert Adair. The letter "e" does not appear even once in the book!





Cryptography Lesson Plan 3

Class: Affine shift ciphers – emphasises clock arithmetic and gives more practice frequency analysis.

Resources:

Leaflet “On substitution ciphers”.

OHP 1, giving partial encryption table for the $3x+5$ affine shift cipher together with teachers' solution.

OHP 2-4, with cipher text to crack, method and solution.

Starter: (10 minutes approximately) Uses handout

Complete the encryption table on the OHP (the affine shift cipher $x \rightarrow 3x+5$ is discussed in the teachers' notes).

Encourage them to try to spot the pattern and guess the rule which should be concealed.

Main activity: (40 minutes approx) Uses OHP

- *Introduce the class of affine shift ciphers mentioning “clock arithmetic” mod 26*
- *Show them that the cipher table arises from the affine shift $x \rightarrow 3x + 5$.*
- *Discuss the fact that you only need to know the value of two letters to deduce the affine shift (solving two simultaneous equations mod 26).*
- *Use frequency analysis and modular arithmetic to decipher an affine shifted text together or in groups.*

Plenary (approx 10 minutes)

Discuss generalisations to modular arithmetic mod n .



OHP slide 1 for lesson 3.

Spot the pattern?

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
H	K	N					C																		

$$x \rightarrow 3x + 5$$

1	2	3	4	5	6	7	8	9	10	11	12	13
8	11	14	17	20	23	26	3	16	9	12	15	18
14	15	16	17	18	19	20	21	22	23	24	25	26
21	24	1	4	7	10	13	16	19	22	25	2	5

Encryption table

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



OHP Slide 2 for lesson 3

Ciphertext

LMYFU BKUUS DDYFA XWCLA OLPSF AOLMJ FASDS NSFGJ FAOEL
 SOMYT DJLAX EMHJM BFMIB JUMIS HFSUL AXUBA FKJAM XLSKF
 FKXWS DJLSO FGBJM WFKIU OLFMX MTMWA OKTTG JLSXL SKFFK
 XWSDJ LSIZG TSXWJ LJLSX LSUMF JSDJL SIZGH FSQYS XOGLS DMMDT
 SDMXJ LSBAT SMHBK BSFLS BFMCT SDKFM YXDJL SLYJM ZTANA
 MYUXM CJMCL MCKUT MMEAX WKJLA IKXDC LMCKU XJJLA UCKUC
 LKJAJ LKDZS SXTAE SHMFJ SXAXJ SFIAX KZTSI MXJLU TKUJG SKFXM
 CMXDS FLSLK DWMXS IKDJL SOLMF YUTAX SMHIS KXAXW TSUUT
 SJJSF UDKXO SDZSH MFSLA USGSU ZYJLJ SGCSF SXMJI SKXAX WTSUU
 JLJGC SFSTM KSDSC AJLJL SIMUJ NAJKT ISKXA XWAIK WAXKZ TSAHM
 XTGLS OMYTD HAXDA JZYJC LSFSC KUJLS BKJJS FXCLS FSCKU JLSBK
 JJSFX CLSFS CKUJL SBKJJ SFXHF MISXA WIKZG FMZSF JLKFF AU

Occurrences table:

A	B	C	D	E	F	G	H	I	J	K	L	M
34	12	19	23	4	41	12	10	16	50	38	46	42
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	11	1	1	0	78	22	28	0	13	41	11	11



OHP Slide 3 for lesson 3

Use frequency analysis to guess that S enciphers for e, and J for t.

This tells us that for an affine shift cipher

$$x \rightarrow ax + b$$

$$a.5 + b = 19 \quad (e \rightarrow S)$$

$$a.20 + b = 10 \quad (t \rightarrow J)$$

Solving mod 26 we see that $15.a = -9 \pmod{26}$. Now 7.15 is congruent to $1 \pmod{26}$ since $7.15 = 105 = 104 + 1 = 4.26 + 1$. It follows that $7.15.a = 7.-9$, or a is congruent to -63 .

Now $-63 = -52 - 11$, so a is congruent to -11 , or equivalently to $15 \pmod{26}$. Hence $a = 15$. Now from $a.5 + b = 19$ we get

$75 + b$ is congruent to 19 , or b is congruent to $-56 \pmod{26}$.

Since $-56 = -2.26 - 4$, b is congruent to $-4 \pmod{26}$ so $b = 22$.

To check this $20.a + b = 300 + 22 = 322 = 12.26 + 10$, so

$a.20 + b = 10$ as required. So the affine shift is $x \rightarrow 15x+22$ and the decrypt is given by the inverse function $y \rightarrow 7(y-22)$

[It might look strange but “dividing by 15” is the same as multiplying by 7 in mod 26 arithmetic.]

Equivalently the decryption is achieved by the affine shift

$$y \rightarrow 7y+2.$$

Encryption table:

a	b	c	d	e	f	g	h	i	j	k	l	m
I	P	W	D	K	R	Y	F	M	T	A	H	O
n	o	p	q	r	s	t	u	v	w	x	y	z
V	C	J	Q	X	E	L	S	Z	G	N	U	B



OHP Slide 4 for lesson 3

Decrypt

hours passe dduri ngwhi chjer ichot riede veryt rickh ecoul dthin kofto promp tsome
fresh inspi ratio nhear range dthec rypto grams chron ologi cally thenh earra ngedt
hemby lengt hthen hesor tedth embyf reque ncyhe doodl edont hepil eofpa perhe
prowl edaro undth ehuto blivi ousno wtowh owasl ookin gathi mandw howas ntthi
swasw hatit hadbe enlik efort enint ermin ablem onths lasty earno wonde rheha dgone
madth echor uslin eofme aning lessl etter sdanc edbef orehi seyes butth eywer enotm
eanin gless theyw erelo adedw ithth emost vital meani ngima ginab leifo nlyhe could
findi tbutw herew asthe patte rnwhe rewas thepa ttern where wasth epatt ernfr omeni
gmaby rober tharr is