MAS345 Cipher challenge

Dan Fretwell (daniel.fretwell@sheffield.ac.uk)

Cryptography can be such an exciting thing...not only to learn about but to practice. It is a good feeling to start with a few lines of gibberish and to know that by your own efforts you have turned this gibberish into something meaningful. To aid this I have put together a small cipher trail. Each cipher, once decrypted, contains a quote from a famous mathematician along with hints for subsequent ciphers. Your task is to decrypt each of the six ciphers (the first one being the easiest) and to email me the complete list of surnames of the mathematicians that have been quoted. The first to do so will get a prize.

None of the encryption methods used here are very demanding, in fact every cipher on this sheet can be broken using only pencil and paper. See the classical methods section of your notes for some of the cipher types used in this trail.

Cipher 1

TVIRZRNCYNPRGBFGNAQNAQVJVYYZBIRGURRNEGUPVCUREGJ
BVFNFVZCYRNSSVARFHOFGVGHGVBAJVGUNARAPELCGVBAXRL
PBAFVFGVATBSCEVZRAHZOREF

Cipher 2

WABOBRFYPOPDLQOPLKWPJBPHBWODTRGABOWAOBBRFLHPY
PLQGALCBWRTFNCFWRWNWRPY

Cipher 3

TL HSVSHI A CURI SKTL TWL LTDIP CURIQ A MLUPTD NLWIP
LP SK EIKIPAG AKY NLWIP WDATIVIP SKTL TWL NLWIPQ LM
TDI QAJI HIKLJSKATSLK ARLVI TDI QICLKH SQ SJNLQQSRGI AKH
S DAVI AQQUPIHGY MLUKH AK AHJSPARGI NPLLM LM TDSQ RUT
TDI JAPESK SQ TLL KAPPLW TL CLKTASK ST CSNDIP MLUP SQ
A VSEIKIPI CSNDIP TDI FIY SQ A QUPKAJI TDAT NPIVSLUQGY
ANNIAPIH

Cipher 4

KIFNZHENGOBKICPEMJILULTOXBGCMVXCUEPHAI
TVWIQUPNQSLYTQQYICULKRQVKYIWMIPZNWAIET
XKILVJXHWNJLBDTJGLZHHVGQWUINJPSHCMCCM
WLYEZZUIMRZVGMHIDCURUOPA

Cipher 5

TWGPELPWUBUTXUOVOCCHGHQAVIXKIGDIWCTR
SWGQPMAIRCNONONOKRBJEFGWAWTKPTCEVZER
CCDNRKPVRACXNPGQEICHSLPUMEGAHZVPMLJHCT
OCEKPWUVBECELPHBEBFPJMLEDBCYFEMCWCCTO
WHSNTGKZOIJMCWTKPTCEFUWRZREFEONOKVGXY
OKIXCZIRAGCZUUHETCWNUELAREFGCOESNBYQO
DVXHKIGQPMCGGKRZGCNETBVJOD

Cipher 6

Part 1:

(1,8,1), (4,1,3), (7,6,3), (3,2,1), (6,3,1), (3,3,6),
(1,1,1), (1,2,2), (3,2,6), (7,6,2), (4,1,3), (3,9,3),
(6,2,3), (1,3,1), (5,5,2), (3,3,3), (3,4,4), (6,1,5),
(6,1,9), (6,4,2), (1,1,1), (4,4,5), (1,3,2), (3,2,9),
(3,7,3), (6,2,5), (5,7,3), (1,5,2), (6,1,4), (4,3,6),
(7,1,4), (1,7,2), (7,3,3).

Part 2:

UNMOMEMXBJGLOXBWUUTMRQJHMXWZBJEQQSBB
RXIDXLVKLZSIGVHEHGUIJXUSUQRBVHUCMMZLOYNSDGXID
YVZBIYUMLQXFCKGLPZXYEXHDQADANMAKKLIPJRJAXVUR