CSC/MAT 483 – 001

**CSC/MAT 483 – 001 Spring 2015**

**Cryptology**

**Test One**

**Michael Weyman**

This is a test. You may not collaborate.

It is due no later than Monday 2 March. It may be submitted electronically or as a hard copy.

Each problem is worth 10 points. Do only 10 problems.

Explain your approach to each problem that you do.

You may use software that is posted on the class website, use *Mathematica*, use a calculator, work by hand, or use software that you wrote.

1. Cryptanalyze:

LCZQV OEWZT LEIZB EWEPM VKWVB IKBEI AUIQV BIQVM LUIQV TGJGZ ILQWK QXPMZ AXTIG MLIKW VAQLM ZIJTM ZWTMB PMGKW VABQB CBMLI BGXMW NEMIX WVBPM XWTMA XTIGM LIVMF BZMUM TGQUX WZBIV BXIZB QVMNN MKBQD MTGCB QTQHQ VOBPQ AEMIX WVQVB PMEIZ IOIQV

durin gworl dwart wowhe ncont actwa smain taine dmain lybyr adioc ipher splay edaco nside rable rolet heyco nstit uteda typeo fweap onthe poles playe danex treme lyimp ortan tpart ineff ectiv elyut ilizi ngthi sweap onint hewar again

found it was a ceaser cipher with a key of 8

2. The following message was enciphered with keyword ciphers. It was first enciphered with a keyword cipher with keyword CORAL and keyletter M and then re-enciphered with a keyword cipher with keyword PYTHON and keyletter D. Construct the composed key and decipher the message (which is a name).

ZDXRD FXKSK OPUR

Marian Rejewski

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

3. Cryptanalyze:

QSRAJ UCOHU PWOER AKUAJ EYZQR URCUH VKEKE REJQA JUCJF ERESH JOPJF EMEUA ENORE MQHVO JOQHA KEREG HQKHU HVSHJ OPPON EOHNR UHMER EJSRH EVJQA QYEAQ RJQNH QRYUP JOC

OURST AYINA LGIER SWAST EMPOR ARYAN DWEWE RETOS TAYTH EREUN TILTH ECEAS EFIRE CONDI TIONS WEREK NOWNA NDUNT ILLIF EINFR ANCER ETURN EDTOS OMESO RTOFN ORMAL TIY

Tried the affine plain text attack to find the key.

JFE = The so the multi key = 9 and the add key = 12

4. Cryptanalyze:

V EO WYP SAUL YG PQL YUFLU YG YAU GAUPQLU MUCHPYDUEHQVM FAPVLS WYU MEW V ULOLOKLU BQLPQLU BL SPVTT FLETP BVPQ PQL LWVDOE MVHQLU.

IAMNOTSUREOFTHEORDEROFOURFURTHERMRCGTOPRAGHIMBUTIESNORMANIREDEDVERWHETHERWESTILLBEALTWITHTHEENIPDAMIGHER

Used a dictionary substitution attack to find solution

5. Cryptanalyze:











|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 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 |

AOLTI AOVKA OHADH ZBZLK AVLUJ

PWOLY AOPZT LZZHN LDHZA VLUJP

WOLYD PAOHZ OPMAH UKAOL UZBIZ

APABA LZFTI VSZAO LTVZA JVTTV

UAYPN YHWOP ZAOL

themb thodt hatwa sused toenc ipher thism essag ewast oenci pherw ithas hifta ndthe nsubs titut esymb olsth emost commo ntrig raphi sthe

was a ceaser cipher with key = 7

6. Complete the following keyword cipher key:



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

7. Determine the key for the following Playfair cipher:

ak ey wo rd ci ph er is ce rt ai nl ys tr on ge rt ha

LI FX VP PF AH OI FQ NA LB TO DP KS ZU OT TH BF TO IC

nt he si mp le sh if tc ip he r

TZ KB AN IR EK CN MD OS PW KB QY

Skip #7

8. Decipher the following ciphertext that was enciphered with a Hill cipher:

AR MJ WG YA TS was enciphered with .

CRYPTOLOGY

9. Cryptanalyze:

VLHVD KHQLK QVFKR QYRQZ HLWHP DXIVL FKCXN RPPHQ GHQQH UILHO DXIHU KDWWH HLQJD QCDOW HVJHV LFKWD EHUZL HHUJL QJGDU DQVDK PDQGD VVHUH UVWCZ DQCLJ ZDUHU VHWCW HVLFK PLWVH LQHPD OWHQJ HVLFK WCXLK QHQDX IGLHE DQNXQ GGDQQ CHLJW HHULK QHQZD VHULQ GHUKD QGWUX J

Can’t solve tried mulitiplicative and affine with no solutions

So skip.

10. Determine the key for the Hill cipher that enciphers

 and .

Solve[20a + 5b == 1 && 9a + 15b == 6, {a,b}, Modulus -> 26]

|  |  |
| --- | --- |
| 3 | 9 |
| 10 | 21 |

11. Cryptanalyze the following cipher. “jellybean” appears in the plaintext message.

lfyvq dfklg aklfj avekx felze ylgvl rzccq wzvek ozjzs

T AY TH T AN NTEN THAT JELLY BEAN E E

ajklc aebzy oalgx zczwj vlafe kfszv klzja elgzm ealzy

TL N E TH ELEB AT N EA T NTHE N TE

klvlz kkfdz ladza elgze aezlz zelga jlazk

TATE E T E NTHE N T ENTH T E

ABCDEFGHIJKLMNOPQRSTUVWXYZ

l n h t yj ab e

12. Cryptanalyze the following message. “nomenclator” appears in the plaintext message.

EZGNM TAMDA EZEZM UEZEM PJVMR GDAWW AJVGT DVMDS MYIYG BDVTE

one a r at onona monoa l a et cc er t a e t ro IQVEI DGITE JGAYW MPPGB MZEUG ZWPMD ET

o te ro e c a e anome nclat or