**CSC/MAT 483 – 001 Cryptology**

**Comprehensive Exam**

**Michael Weyman**

This is a test. You may not collaborate.

It is due no later than noon on Friday, 8 May. It may be submitted electronically or as a hard copy.

Do 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.

WYKRX QXEPW HXQDJ OAHOJ XRWJH MWHXE IMGEH YLWJQ YXGWU JHWPJ WIOKH YXYOH UXXRW MJGVX OQIJG VXUHU TGQYQ IOAVW XYXYO HVJWQ WHXWP BGXRW VUIYD YIHOJ XRSWQ XQWIX YOHOD XRWAU XRWAU XYIUT UQQOI YUXYO HODUA WJYIU UVJYT OLWJX RWSWW MWHPR OQXWP BGIWH XJUTS UQRYH KXOHE HYLWJ QYXG

EIGHT STUDE NTSFR OMNOR THERN KENTU CKYUN IVERS ITYEA RNEDR ECOGN ITION ATTHE KRYPT OSCRY PTANA LYSIS COMPE TITIO NPRES ENTED BYTHE PACIF ICNOR THWES TSECT IONOF THEMA THEMA TICAL ASSOC IATIO NOFAM ERICA APRIL OVERT HEWEE KENDH OSTED BYCEN TRALW ASHIN GTONU NIVER SITY

Used vbreaker to notice it was a simple substitution cipher then used crypto helper to search for the word “the”, and received that it was an affine cipher with multi key = 7 and add key = 14.

\*\*2. Cryptanalyze. The word “statistics” appears in the plaintext.

LRGZV LRGFT DREUD GRGFD GFTDR TGHRC PDGHU VEGDR EUWRT

S tatis tics

HAGPR GGVEU VUGZV KVDGV CEREU DXHGZ VCEWF ERETF RAYCX HMRTG HRCFR ATXEE VTGFX EVJVE GDGHU VEGDK VCVRS AVGXL VVGRE UEVGK XCNKF GZTHC CVEGR TGHRC FVDRE URTGH RCPDG HUVEG DWCXL XGZVC HEFJV CDFGF VDKZF TZYRJ VGZVL RWFCD GZREU XMMXC GHEFG PGXDM VRNUF CVTGA PKFGZ RTGHR CFVDR EUAVR CEGZV FCMVC TVMGF XEDFE GZVKX CNWXC TV

I found statistics in the cipher text then used substitution solver to solve the rest of the message

MATHEMATICSANDSTATISTICSACTUARYSTUDENTSANDFACULTYATTENDEDTHEWESTERNANDSOUTHERNFINANCIALGROUPACTUARIALCONNECTIONEVENTSTUDENTSWEREABLETOMEETANDNETWORKWITHCURRENTACTUARIESANDACTUARYSTUDENTSFROMOTHERUNIVERSITIESWHICHGAVETHEMAFIRSTHANDOPPORTUNITYTOSPEAKDIRECTLYWITHACTUARIESANDLEARNTHEIRPERCEPTIONSINTHEWORKFORCE

Skip 3. Construct the Playfair square.

Plaintext

The Amazing Race is a one day event that the Mathematics and Statistics Department puts on every year. Students and faculty team up to tackle multiple challenges that will mentally test them.

Ciphertext

PKARE RXLML NRBAG CMQMA CRWRW MRUPK RQPKA ERQPB ERQKD BRMFB QRQKD OQIBF BWRNO RAMUQ OUGVM AWMDR WRRND OTFAM ODRMF SCIZU YRPRR EOQUP QRDIH NNOKU HQHNB INIHN MLMBP KRQXH IZGNA MQRIZ KZPRD OPKAE

4. Cryptanalyze.

PRAJE HQNSC WZGRJ SVIAX LYOCH JTLIA NFFGB JRILL WSFTG MENBJ NVMEA CYHGG PHDYH GWZGR JSVCD VCSTG LPWYW OWHOM FJBTY LDGSG QLNKW UTCHL EWXIU IQVGU HGLDL CHRGN HKGYI PAPTA MCJUW ECSGG JCXQJ NVMNH LYEUN LGRXW KNSTZ WIGZD VCSAT CZMML EVBPK UNTJM ZFCHI RBPKR JXVYY VMIEF GPLQF GGNSX ETANC DMMII UWZOC WTJYZ KGLIP UWXLL LKMSI JFIPN PQRRE UMLZC

Found it was not a simple substitution cipher could not figure out how to move forward

Skip 5. Cryptanalyze the following message that was enciphered with a running key cipher. “codebreakers” appears in the plaintext.

ROMKW TQFHE OUWEF IEQER VLHUG SQYTS HSZVV BCZNN YXJQY TSZRG NMKCB QTZRV RVOTR EMEWI GNEVV GZQIK WPREC SMEZJ EIHOS IIEHB IYXAX UX

6. Cryptanalyze.

nitce svsse pynyn ebqme ssscn lqsch uotea qhsao ailoq aiesf dcnqt sdgdt lrqan fomtg eqanr nosap qmaii tihdq tdomo iemq

Permutation cipher with length 9

\*\*7. Use simplified DES to decipher the ciphertext

1001 1010 1001

that was enciphered using key

101 101 011

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **1** | **1** | **1** | **0** | **1** | **0** | **1** | **0** | **1** | **1** | **0** |

\*\*8. Using simplified PRESENT and round keys



to encipher the plaintext message

1000 1110 1011 1110

+ K1 = 0000 1000 1000 0100

->s = 1100 0011 0011 1001

P -> = 1001 1000 0110 0111

+ K2 = 1110 1000 1010 0010

->S= 0001 0011 1111 0110

P->= 0010 0011 0111 1110

+K3= 1101 1101 0110 0101

**1101 1101 0110 0101**

\*\*9a. Generate an RSA key. Use primes in the range between 20 000 000 and

30 000 000.

n = (200000003 \* 20000033)

n = 4000006660000099

e = 37

plaintext = micha 13 09 03 08 01

PowerMod[1309030801, 37, n]

9b. Then use the RSA key that you generated in to encipher at least 5 characters of your first name. (Pad with X’s is necessary.)

Use

a = 0, b = 1, c = 2, …, z = 25

to substitute for the letters. (*Mathematica* may be used for 11a and 11b,)

**\*\*10. Diffie-Hellman Key exchange.**

We’re planning on sending enciphered messages between us, and we need to agree on a key. We’re going to use the Diffie-Hellman key exchange to exchange a key. (*Mathematica* may be used.)

We select the prime *p* = 100000007 and the primitive root  = 180989.

I send you. 51952136.

Send your response.

What key have we agreed to?

**\*\*11. Break RSA.**

The modulus *n* = 218537879591567. The encryption exponent *e* = 1103. Break the message 164726505417492. Use a = 01, b = 02, …, z = 26 to convert letters to numbers. (*Mathematica* may be used.)

PowerMod[164726505417492, 1103, 218537879591567]

103334588144615

**\*\*12. Simplified AES key.**

The user-supplied key to simplified AES is 1101110100110001. Construct the round keys using the key schedule.

1101 1101 0011 0001

W[0] = 1101 1101

W[1] = 0011 0001

0001 0011

0100 1011

+ Round 1000 0000

1100 1011

Add w[0]

W[2] = 0001 0000

Add w[1]

W[3] = 0010 0001

0001 0010

0100 1010

+ Round 0011 0000

0111 1010

Add W[2]

W[4] = 0110 1010

Add w[3]

W[5] = 0100 1011

**K1 = 1101 1101 0011 0001**

**K2 = 0001 0000 0010 0001**

**K3 = 0110 1010 0100 1011**