CSC/MAT 483 – 001

Cryptology

Test Three

Michael Weyman

This is a test. You may not collaborate.

It is due no later than Wednesday 22 April. It may be submitted electronically or as a hard copy.

Do 6 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. Decrypt the ciphertext message

AGVXF GXGAX XDFFD XXXGD FAGAF DAXGA AFGDV DGDVV

KNAPSACKCRYPTOSYSTEM

that was encrypted using the ADFGVX square



and the keyword *Kentucky*.

2. Cryptanalyze \*skip

RNIDO ITNTB AMOEK RQOEN YRTOA DNHAC HSPQH UERAS OOAAB DCETG QECRE TKFUT NEHHN BRQRK SCHEH NJNEE OSAAQ NKUTO EBSEH NNDTA LQTTV IFCHN HRSEA MEOQN YITLN ACOEN AFBLM Q

Frequencies state that it is a permutation cipher length of 136 try length 8

RNIDOITN

47185632

INTROind

TBAMOEKR

arktoenm

3. Cryptanalyze \*skip

STJPF KSNII JYYNZ RNFRT FQSXW XTYWS ZZTMR WTNMS JYTIX UWJZF BSFNN XHNNY NWXWX LSSWQ UJIRJ DIHFJ TNYWP FRJOX XGSTY JMXPS HMYNN DMRQL FQ

\*\*4. Decipher the following ciphertext that was enciphered using a permutation cipher with permutation .

HECPI XTRET SAMSE OBGTE KQRAE

CIPHE RTEXT MESSA GETOB REAKQ

\*\*5. Use the simplified RC-4 cipher to generate 3 bits of keystream using:

Key 2, 3, 6, 7

011

\*\*6. Use the key schedule of simplified PRESENT to calculate the round keys that result from:

Key 1101 0001 1011 1111 1110

1101 1010 0011 0111 1111

0111 1010 0011 0110 1111

**K1 = 0111 1010 0011 0110**

0111 1010 0011 0110 1111

1110 1111 0100 0110 1101

0001 1111 0100 0100 1101

**K2 = 0001 1111 0100 0100**

0001 1111 0100 0100 1101

1010 0011 1110 1000 1001

1111 0011 1110 1011 1001

**K3 = 1111 0011 1110 1011**

\*\*7. Using simplified PRESENT and round keys



to encipher the plaintext message

1111 1100 0111 1000 + K1 =

0111 1010 0100 0010 S-Box =

1101 1111 1001 0110 Permu =

0123 4567 8901 2345

1110 1101 0101 1110 + K2 =

1001 1101 1001 1011 S-Box =

1110 0111 1110 1000 Permu =

0123 4567 8901 2345

1011 1110 1110 0100 + K3 =

**0100 0000 1111 1111**

\*\*8. Use simplified DES to decipher the ciphertext

1101 1010 0100

that was enciphered using key

0111 1100 1

Used excel form

0111 1011 1101