Michael Weyman

CSC/MAT 483 – 001

Cryptology

Test Two

This is a test. You may not collaborate.

It is due no later than Monday 6 April. It may be submitted electronically or as a hard copy.

Do 9 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.

To convert text to bit strings, Baudot code was used.

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

**\*1. Cryptanalyze the following ciphertext.**

LAVVBAJEFBTIWKVABTQPZZYXWVFUAORXKVRGUAZSIKEXEHFUXMYSFIZHFZOGKXUGPNGERFFVSKKWPOHTEHFGFWNWYRXXRHHXWKVANXCLSMAQMIISFOVXEHTKGYWFREEXRFAYXHCZBCAGXHUKUXISZUFRJHHJWGKGJODESSNHDXKCNZLXERNSSCFFSGAKKVNZKAFKPGKXJHUKOBUSIGJBVHLUXGBINISWVAVIHKFUEGELRBQGKXIWRYGYGCFZWKGFRYWGKOGOGGJPLTCNJHHJWGKGFZMWVBGYOBCZNRKHYOIKLAVCCVGKKIAOLRKCGUMKEYHYUTDDHY

Keyword length 12

I used Vandal to find that they keyword was most likely 12 characters long but could not find the solution to the cipher

**2. Cryptanalyze autokey extended by ciphertext.**

WLJHVJERMDNHYMFXLPERLFCXVOFNXMUJFZMFNHXNJEHQGJGRJNRYNNRB

**3. Cryptanalyze the following ciphertext that was generated by a running key cipher. The letter-string “analysis” appears somewhere in the plaintext**

YYCCBNGHPAGCJAWHMLMFUQCJJRGUZRQXGRYIKFEIIK

**\*4. Cryptanalyze the following ciphertext.**

DCOVZ UBMHU VPUIU HYSFO WFJSN UNTMR SFNVP UTMRU OYUVQ WVPVP UBHUF GPSFN ZHWVW OPWFS OCZCH ZMBQS HOSQ

I also used vandal to try to get a length of keyword and found it was probably 13, but could not solve after this.

**\*5. Generate a LFSR keystream.**

Determine the first 20 bits of the keystream generated by an 8-bit LFSR with taps B6 and seed A5. Do not include the first 8 bits, which are the seed.

Taps = 10011110

Seed = 11000101

Tap tap tap tap tap

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

01100010101100010101

**\*6. Composed Vigenère key.**

6a. A message is first enciphered with a Vigenère cipher with keyword “cypher” and then re-enciphered with a Vigenère cipher with keyword “victory.” What is the keyword for the composed cipher?

6\*7=42=length of keyword

XGRASIATXJXFTWKPGKQPNCMTVMGFZZERDYCMKAIVVP

6b. A message is first enciphered with a Vigenère cipher with keyword “enigma” and then re-enciphered with a Vigenère cipher with keyword “composed.” What is the keyword for the composed cipher?

6 \* 8 = 48 = length of keyword

GBUVASIQKUYPSFMJOOQCWYQDGBUVASIQKUYPSFMJOOQCWYQD

**\*7. Decipher autokey extended by plaintext.**

The following message has been enciphered using an autokey cipher extended by plaintext. The key is “Rejewski.” Decipher the message.

KLNTKDOABUZTBEIVUNXLVGIVFHGFKNPDXKFMOBJ

-Used cryptohelper to decipher.

-thepo lesin vente dmach inest heyca lledb omby

**\*8. Decipher a stream cipher.**

A message in Baudot code is enciphered using the keystream:

00110 01111 10100 01011 00000 10011

The ciphertext stream is

10010 01110 11110 11011 11000 10100

Decipher the message.

10100 00001 01010 10000 11000 00111

Stream

**\*8. Decipher running key.**

WBEYSCEPTKVMGHKPGNCNRZHMEAAMGDFAEGCRSMZKRGWRPIFF

which was enciphered using the key:

The Northern Kentucky University Board of Regents approved today the schedule of tuition and fee rates, in accordance with the Council on Postsecondary Education’s tuition-setting policy and guidelines.

-I used Cryptotool’s Vigenere dephipher tool to find message.

-duale llipt iccur vedet ermin istic rando mbitg enera tor

**\*9. Determine the taps of a LFSR.**

The following keystream was generated by a 4-bit LFSR

… 0110 1101 101 …

determine the taps.

|  |  |  |  |
| --- | --- | --- | --- |
| \_ | \_ | tap | tap |

**\*10. Depth of Two.**

Cryptanalyze the following messages that were enciphered using the same keystream. The word “battle” appears in one of the messages.

Ciphertext #1

10101 01010 11110 01010 01000 10000 11100 01101 10111 10101 01001 10100 01001 00000 00101 00000 11000 01001 00011 00011 10011 10110

Ciphertext #2

10101 01010 00100 01010 01100 11010 11000 00111 11011 10111 11110 10000 11100 00000 11011 00000 11101 11011 10101 11011 00111 10010

T H E B A T T L

10101 01010 11110 01010 01000 10000 11100 01101

10101 01010 00100 01010 01100 11010 11000 00111

10111 10101 01001 10100 01001 00000 00101 00000

11011 10111 11110 10000 11100 00000 11011 00000

11000 01001 00011 00011 10011 10110

11101 11011 10101 11011 00111 10010