Alan Thomas

CSI-337 Cyber Security

Exam 1

Dr. Dutta

6FEB18

Chapter 1. Problem 9

a. Steganography

b. Cryptography

c. Steganography

d. Steganography

Chapter 2. Problem 12

a. 88 and 220

220=88\*2+44

88=44\*2+0

**gcd=44**

b. 300 and 42

300=42\*7+6

42=6\*7+0

**gcd=6**

c.24 and 320

320=24\*13+8

24=8\*3+0

**gcd=8**

d. 401 and 700

700=401\*1+299

401=299\*1+102

299=102\*2+95

102=95\*1+7

95=7\*13+4

7=4\*1+3

4=3\*1+1

3=3\*1+0

**gcd=1**

Chapter 2. Problem 16

S=s1-(q\*s2) t=t1-(q\*t2)

a.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **q** | **a** | **n** | **r** | **s1** | **s2** | **s** | **t1** | **t2** | **t** |
| 1 | 7 | 4 | 3 | 1 | 0 | 1 | 0 | 1 | -1 |
| 1 | 4 | 3 | 1 | 0 | 1 | -1 | 1 | -1 | 2 |
| 3 | 3 | 1 | 0 | 1 | -1 | 4 | -1 | 2 | -7 |
|  | 1 | 0 |  | -1 | 4 |  | 2 | -7 |  |

**gcd=7 s=-1 t=2**

b.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **q** | **a** | **n** | **r** | **s1** | **s2** | **s** | **t1** | **t2** | **t** |
| 6 | 291 | 42 | 39 | 1 | 0 | 1 | 0 | 1 | -6 |
| 1 | 42 | 39 | 3 | 0 | 1 | -1 | 1 | -6 | 7 |
| 13 | 39 | 3 | 0 | 1 | -1 | 14 | -6 | 7 |  |
|  | 3 | 0 |  | -1 | 14 |  | 7 |  |  |

**gcd=3 s=-1 t=7**

c.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **q** | **a** | **n** | **r** | **s1** | **s2** | **s** | **t1** | **t2** | **t** |
| 3 | 320 | 84 | 68 | 1 | 0 | 1 | 0 | 1 | -3 |
| 1 | 84 | 68 | 16 | 0 | 1 | -1 | 1 | -3 | 4 |
| 4 | 68 | 16 | 4 | 1 | -1 | 5 | -3 | 4 | -19 |
| 4 | 16 | 4 | 0 | -1 | 5 |  | 4 | -19 |  |
|  | 4 | 0 |  | 5 |  |  | -19 |  |  |

**gcd=4 s=5 t=-19**

d.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **q** | **a** | **n** | **r** | **s1** | **s2** | **s** | **t1** | **t2** | **t** |
| 6 | 400 | 60 | 40 | 1 | 0 | 1 | 0 | 1 | -6 |
| 1 | 60 | 40 | 20 | 0 | 1 | -1 | 1 | -6 | 7 |
| 2 | 40 | 20 | 0 | 1 | -1 | 3 | -6 | 7 |  |
|  | 20 |  |  | -1 |  |  | 7 |  |  |

**gcd=20 s=-1 t=7**

Chapter 3. Problem 21

a. Encrypt the message ‘this is an exercise.’ I chose option a, additive cipher with a key equal to 20. This is assuming ‘a’ holds a value of 1 in the English alphabet.

**Encryption**

|  |  |  |
| --- | --- | --- |
| Plain text value | Encryption math used | Resulting cipher text |
| T(20) | (20+20)mod26 | N(14) |
| H(8) | (8+20)mod26 | B(2) |
| I(9) | (9+20)mod26 | C(3) |
| S(19) | (19+20)mod26 | M(13) |
| I(9) | (9+20)mod26 | C(3) |
| S(19) | (19+20)mod26 | M(13) |
| A(1) | (1+20)mod26 | U(21) |
| N(14) | (14+20)mod26 | H(8) |
| E(5) | (5+20)mod26 | Y(25) |
| X(24) | (24+20)mod26 | R(18) |
| E(5) | (5+20)mod26 | Y(25) |
| R(18) | (18+20)mod26 | L(12) |
| C(3) | (3+20)mod26 | W(23) |
| I(9) | (9+20)mod26 | C(3) |
| S(19) | (19+20)mod26 | M(13) |
| E(5) | (5+20)mod26 | Y(25) |

The resulting cipher text reads: NBCMCMUHYRYLWCMY

**Decryption**

|  |  |  |
| --- | --- | --- |
| Cipher text value | Encryption math used | Resulting cipher text |
| N(14) | (14-20)mod26 | T(20) |
| B(2) | (2-20)mod26 | H(8) |
| C(3) | (3-20)mod26 | I(9) |
| M(13) | (13-20)mod26 | S(19) |
| C(3) | (3-20)mod26 | I(9) |
| M(13) | (13-20)mod26 | S(19) |
| U(21) | (21-20)mod26 | A(1) |
| H(8) | (8-20)mod26 | N(14) |
| Y(25) | (25-20)mod26 | E(5) |
| R(18) | (18-20)mod26 | X(24) |
| Y(25) | (25-20)mod26 | E(5) |
| L(12) | (12-20)mod26 | R(18) |
| W(23) | (23-20)mod26 | C(3) |
| C(3) | (3-20)mod26 | I(9) |
| M(13) | (13-20)mod26 | S(19) |
| Y(25) | (25-20)mod26 | E(5) |

The result of the decryption reads: THISISANEXERCISE

Chapter 3. Problem 28

Brute-force the following message that uses an additive cipher. It’s given that the person who created the cipher often uses the her day of birth, the 13th.

NCJAEZRCLASJLYODEPRLYZRCLASJLCPEHZDTOPDZQLNZTY

For my method I chose to attack the first 6 characters of the string to determine if I could make out a word.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Key | N(14) | C(3) | J(10) | A(1) | E(5) | Z(26) |
| 13(significant date) | A | P | W | N | R | M |
| 10 | D | S | Z | Q | U | P |
| 11 | C | R | Y | P | T | O |

Deciding that a key of 11 is more than likely the correct key, the rest of the message was decrypted. Resulting in: **CRYPTOGRAPHY AND STEGANOPGRAPHY ARE TWO SIDES OF A COIN**

Chapter 3 Problem A:

**Cpp attached to email.**