Daniel Frey

CS 4920-001

Assignment 1

1/31/18

**Problem 1 CIA**:

Consider a desktop publishing system used to produce documents for various organizations.

**1a**. An example of a type of publication for which confidentiality of stored data is proprietary material because it contains confidential information that should not be available to everyone.

**1b**. An example of a type of publication for which data integrity is most important is legal documents because you do not want the documents to be modified by any other person other than the author.

**1c**. An example of a type of publication for which system availability is most important is a daily newspaper because everyone should have access to the news, that is the whole point of a newspaper.

**Problem 2 Affine Caesar Cipher:**

**2a**. There are no limitations on b for the affine Caesar cipher. If you consider E([a,b],p) = E(a,b],q), then (ap+b) mod 26 = (aq+b) mod 26, therefor a(p-q) mod 26 = 0. No value for b will satisfy.

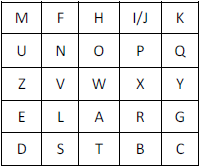
**2b**. Using the previous information in **a**, “a” should not be 0, 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20 22, and 24.

**2c**. Generally, “a” shouldn’t have common factors with 26 since it will not make the cipher one-to-one.

**2d**. Since “a” can have 12 unique values, and “b” can have 26 unique values, there are 12\*26 one-to-one ciphers, or 312.

**Problem 3 Playfair Matrix:**

**3a**. Encrypt: Must see you over Cadogan West. Coming at once.



MU ST SE EY OU OV ER CA DO GA NW ES TC OM IN GA TO NC EX

Encrypted message:

UZ TB DL GZ PN NW LG TG TU ER OV LD BD UH FP ER HW QS RZ

**3b**. Key: largest

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

Encrypt: Must see you over Cadogan West. Coming at once.

MU ST SE EY OU OV ER CA DO GA NW ES TC OM IN GA TO NC EX

Encrypted message:

UZ TB DL GZ PN NW LG TG TU ER OV LD BD UH FP ER HW QS RZ

**3c**. Each of the matrices resulted in the same encryption. The first Playfair matrix is the same as the second, except it is shifted by a column, and the rows were shifted multiple times. Therefore, if there is a shift in the matrix, rows or columns, it will result in the same mappings.

**Problem 4 Playfair Analysis:**

**4a**. Possible keys Playfair cipher: There are 25! possible keys, or 284.

**4b**. Unique keys Playfair cipher: 25! possible keys, and for a 5x5 matrix: 25!/52 = 279 unique possible keys.

**Problem 5 One-Time Pad Vigenere Cipher:**

**5a**. Encrypt: sendmoremoney using key stream 9 0 1 7 23 15 21 14 11 11 2 8 9.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Key | 9 | 0 | 1 | 7 | 23 | 15 | 21 | 14 | 11 | 11 | 2 | 8 | 9 |
| P | s | e | n | d | m | o | r | e | m | o | n | e | y |
| P# | 18 | 4 | 13 | 3 | 12 | 14 | 17 | 4 | 12 | 14 | 13 | 4 | 24 |
| C# | 1 | 4 | 14 | 10 | 9 | 3 | 12 | 18 | 23 | 25 | 15 | 12 | 7 |
| C | B | E | O | K | J | D | M | S | X | Z | P | M | H |

Ciphertext: BEOKJDMSXZPMH

**5b**. Use ciphertext from **a**, find a key to decrypt to cashnotneeded.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| C# | 1 | 4 | 14 | 10 | 9 | 3 | 12 | 18 | 23 | 25 | 15 | 12 | 7 |
| P | c | a | s | h | n | o | t | n | e | e | d | e | d |
| P# | 2 | 0 | 18 | 7 | 13 | 14 | 19 | 13 | 4 | 4 | 3 | 4 | 3 |
| Key | 1 | 22 | 4 | 23 | 4 | 11 | 7 | 21 | 7 | 5 | 14 | 18 | 22 |

Key: 1 22 4 23 4 11 7 21 7 5 14 18 22

**5c**. A brute-force attacker would not be able to decrypt the ciphertext from **a** because there are no patterns or regularities. It could be decrypted into many plaintext, but you wouldn’t know which is correct.