Name: Muhammad Laraib Akhtar

Roll No: 21L-5294

Course: Information Security

Assignment: 1

Plain Text: 21l5294-waseem rao-35302-3121800-3

Ceaser Cipher:

Key = 3

Plain: 0123456789abcdefghijklmnopqrstuvwxyz -

Cipher: 3456789abcdefghijklmnopqrstuvwxyz -012

Plain Text: 21l5294-waseem rao-35302-3121800-3

Cipher text: 54o85c72zdvhho1udr26863525454b3326

Challenges faced: Ceaser cipher is for alphabets only. So I extended the dictionary and mentioned it above.

Monoalphabetic:

Plain: 0123456789abcdefghijklmnopqrstuvwxyz -

Cipher: qwertyuiopasdfghjklzxcvbnm9876543210 –

Plain Text: 21l5294-waseem rao-35302-3121800-3

Cipher Text: ewcyept-4a8ggv 9ab-ryrqe-rwewoqq-r

Challenges faced: The plain text contain alphanumeric keys as well as special characters. So I added them to the dictionary and then mapped it

Vigenere Cipher:

Plain Text: 21l5294-waseem rao-35302-3121800-3

Alphabet: abcdefghijklmnopqrstuvwxyz0123456789 –

Key: waseemraowaseemraowaseemraowaseemr

|  |  |
| --- | --- |
| 0 | A |
| 1 | B |
| 2 | C |
| 3 | D |
| 4 | E |
| 5 | F |
| 6 | G |
| 7 | H |
| 8 | I |
| 9 | J |
| 10 | K |
| 11 | L |
| 12 | M |
| 13 | N |
| 14 | O |
| 15 | P |
| 16 | Q |
| 17 | R |
| 18 | S |
| 19 | T |
| 20 | U |
| 21 | V |
| 22 | W |
| 23 | X |
| 24 | Y |
| 25 | Z |
| 26 | 0 |
| 27 | 1 |
| 28 | 2 |
| 29 | 3 |
| 30 | 4 |
| 31 | 5 |
| 32 | 6 |
| 33 | 7 |
| 34 | 8 |
| 35 | 9 |
| 36 |  |
| 37 | - |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Key | 22 | 0 | 18 | 4 | 4 | 12 | 17 | 0 | 14 |
| Plaintext | 28 | 27 | 11 | 31 | 28 | 35 | 30 | 37 | 22 |
| Ciphertext | 12 | 27 | 29 | 35 | 32 | 9 | 9 | 37 | 36 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Key | 22 | 0 | 18 | 4 | 4 | 12 | 17 | 0 | 14 |
| Plaintext | 0 | 18 | 4 | 4 | 12 | 36 | 17 | 0 | 14 |
| Ciphertext | 22 | 18 | 22 | 8 | 16 | 10 | 34 | 0 | 28 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Key | 22 | 0 | 18 | 4 | 4 | 12 | 17 | 0 | 14 |
| Plaintext | 37 | 29 | 31 | 29 | 26 | 28 | 37 | 29 | 27 |
| Ciphertext | 21 | 29 | 11 | 33 | 30 | 2 | 16 | 29 | 3 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Key | 22 | 0 | 18 | 4 | 4 | 12 | 17 |
| Plaintext | 28 | 27 | 34 | 26 | 26 | 37 | 29 |
| Ciphertext | 12 | 27 | 14 | 30 | 30 | 11 | 8 |

Ciphertext: m1396jj- wswiqk8a2v3l74cq3dm1o44li

Challenge faced: The dictionary was becoming of a size 127 and encrypting/decrypting them was a problem. Even in encryption some characters cannot even be typed So I made my own alphabet dictionary and assigned them indexes, so the characters are no non-standard ascii.

One-Time Pad:

Plain Text: 21l5294-waseem rao-35302-3121800-3

Plain: 0123456789abcdefghijklmnopqrstuvwxyz -

Cipher: 9876543210qwertyuiopasdfghjklzxcvbnm -

Cipher text: 89s5816-vqlttd kqg-75798-798299-7\

Challenges faced. Same as in monoalphabetic Ciphers