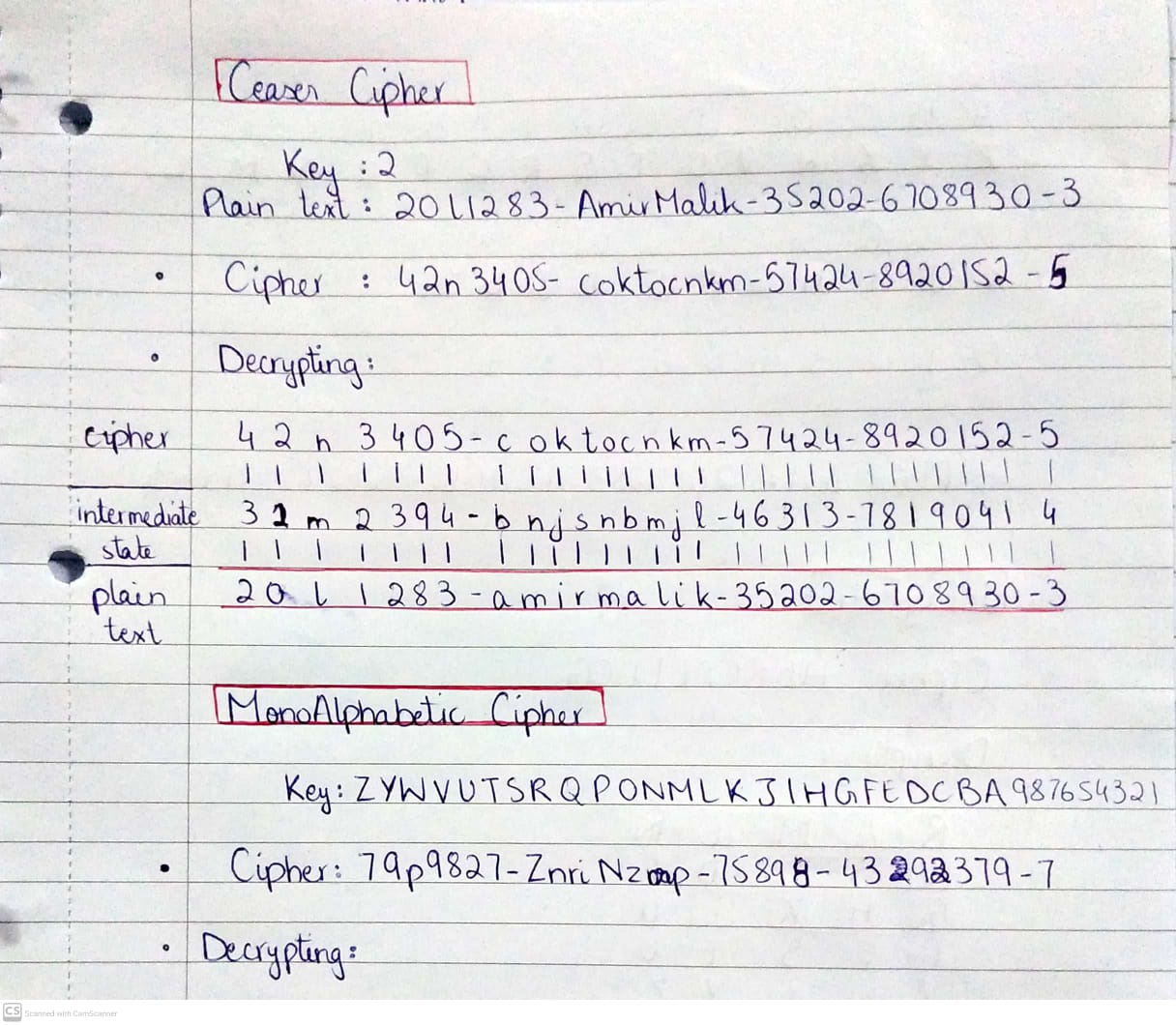
**20L-1283**

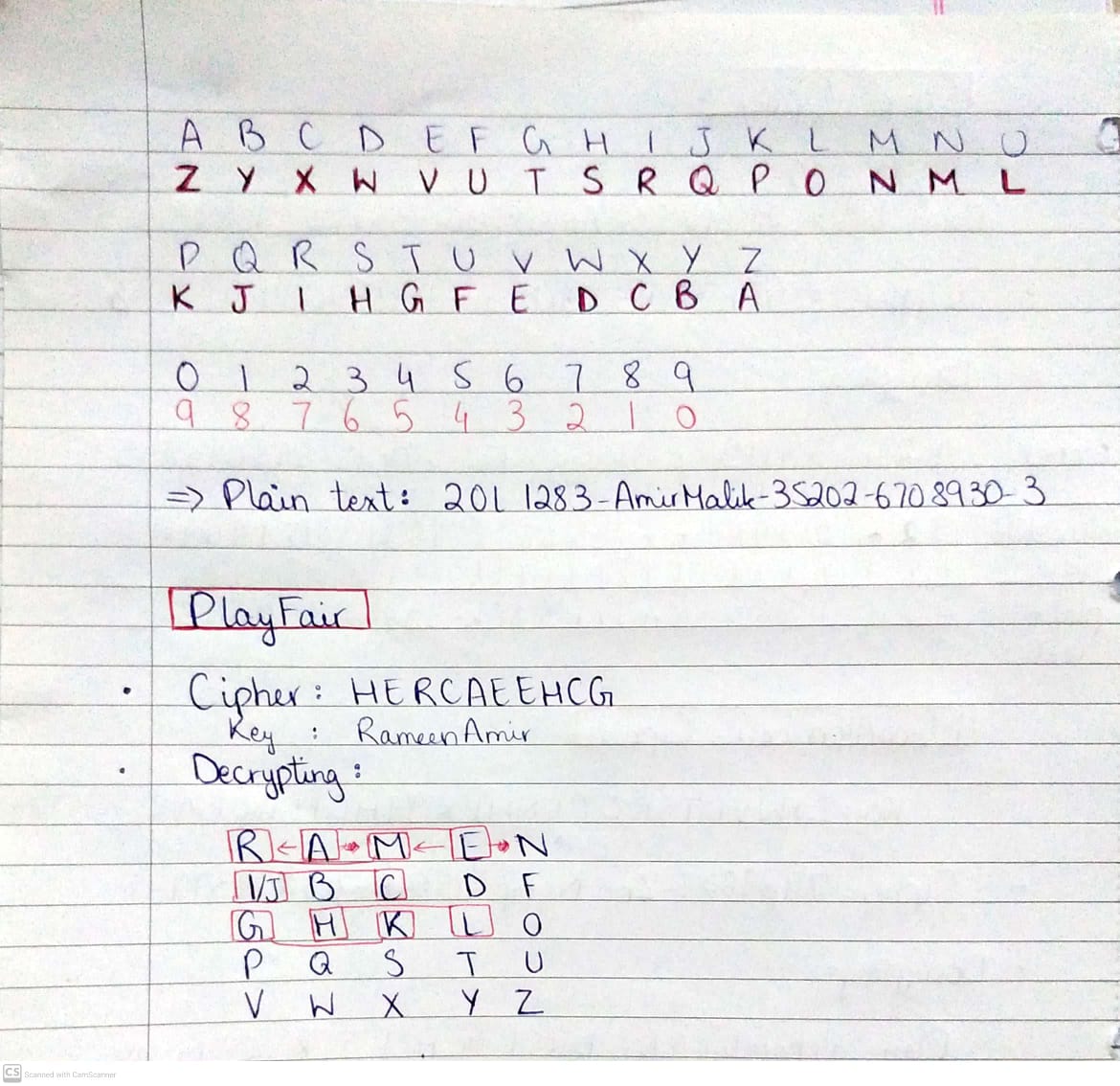
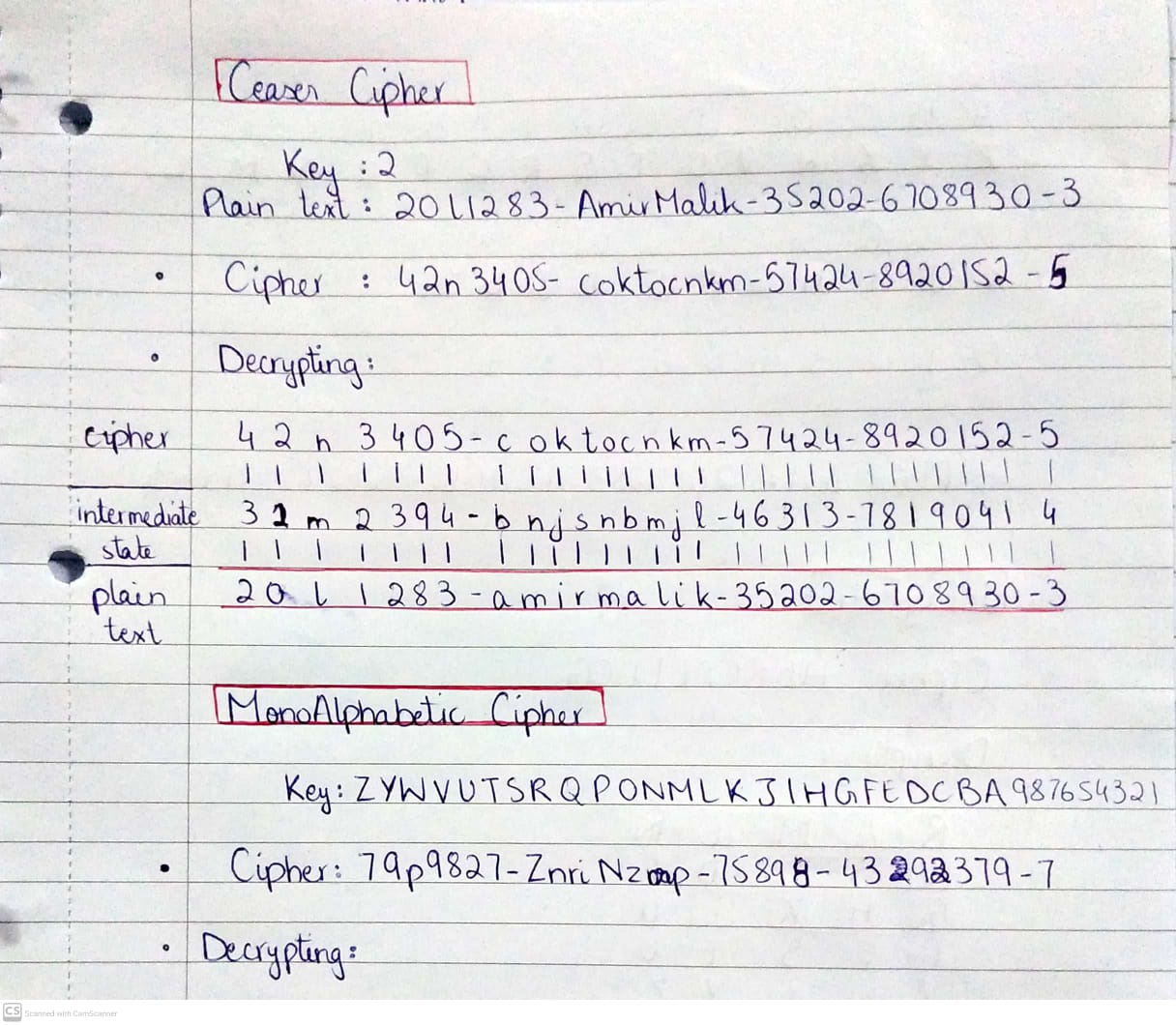
**Rameen Amir**

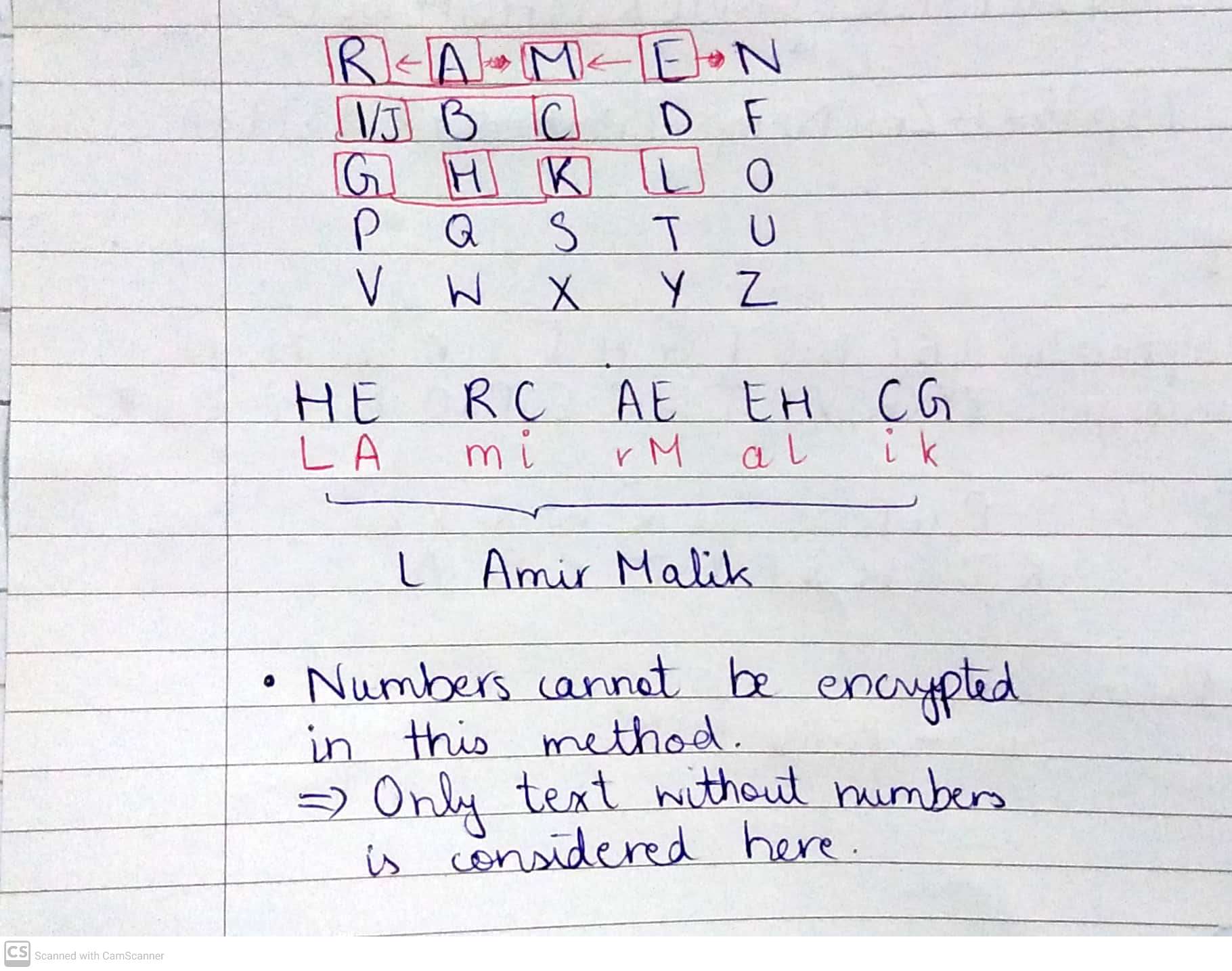
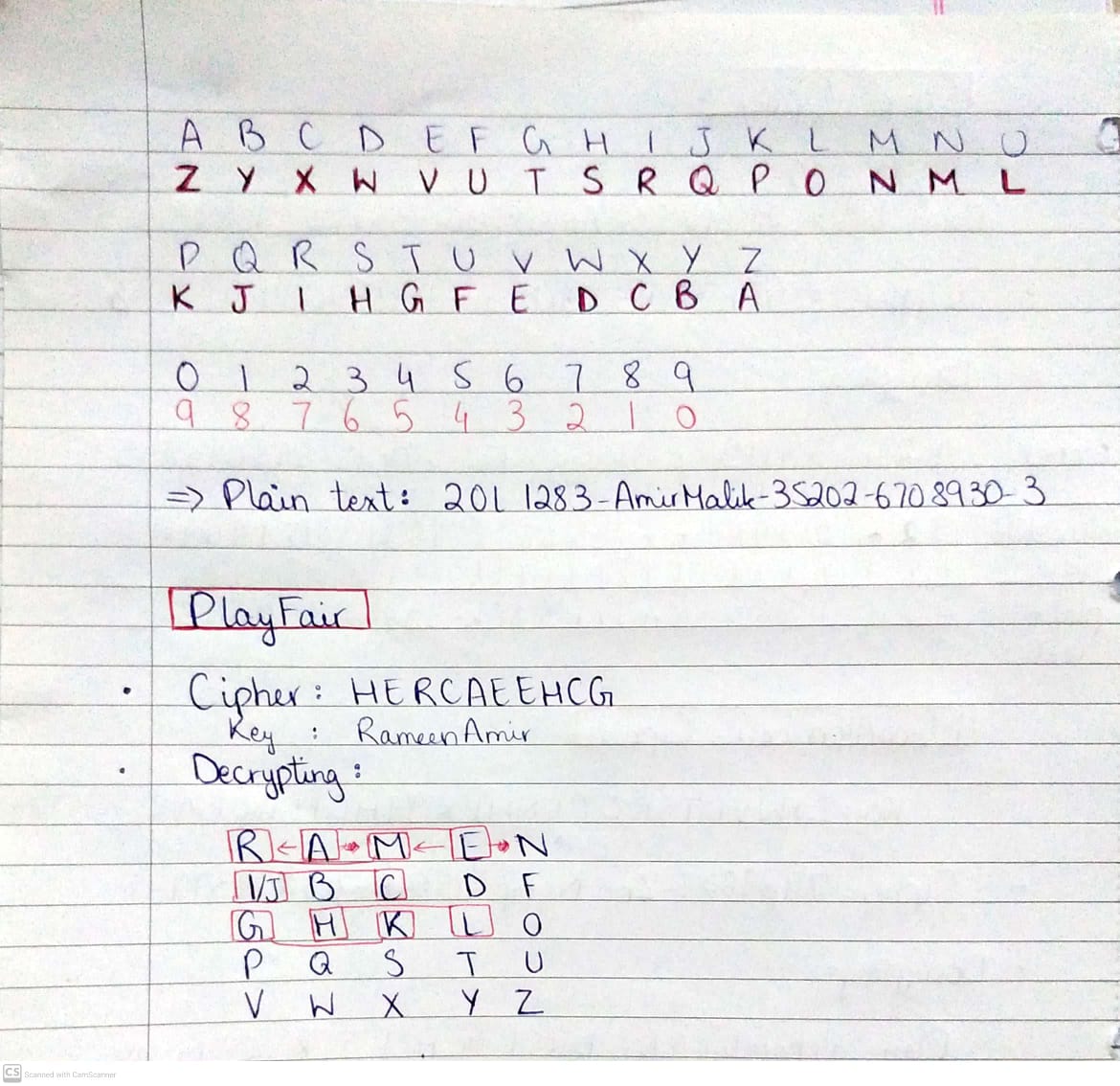
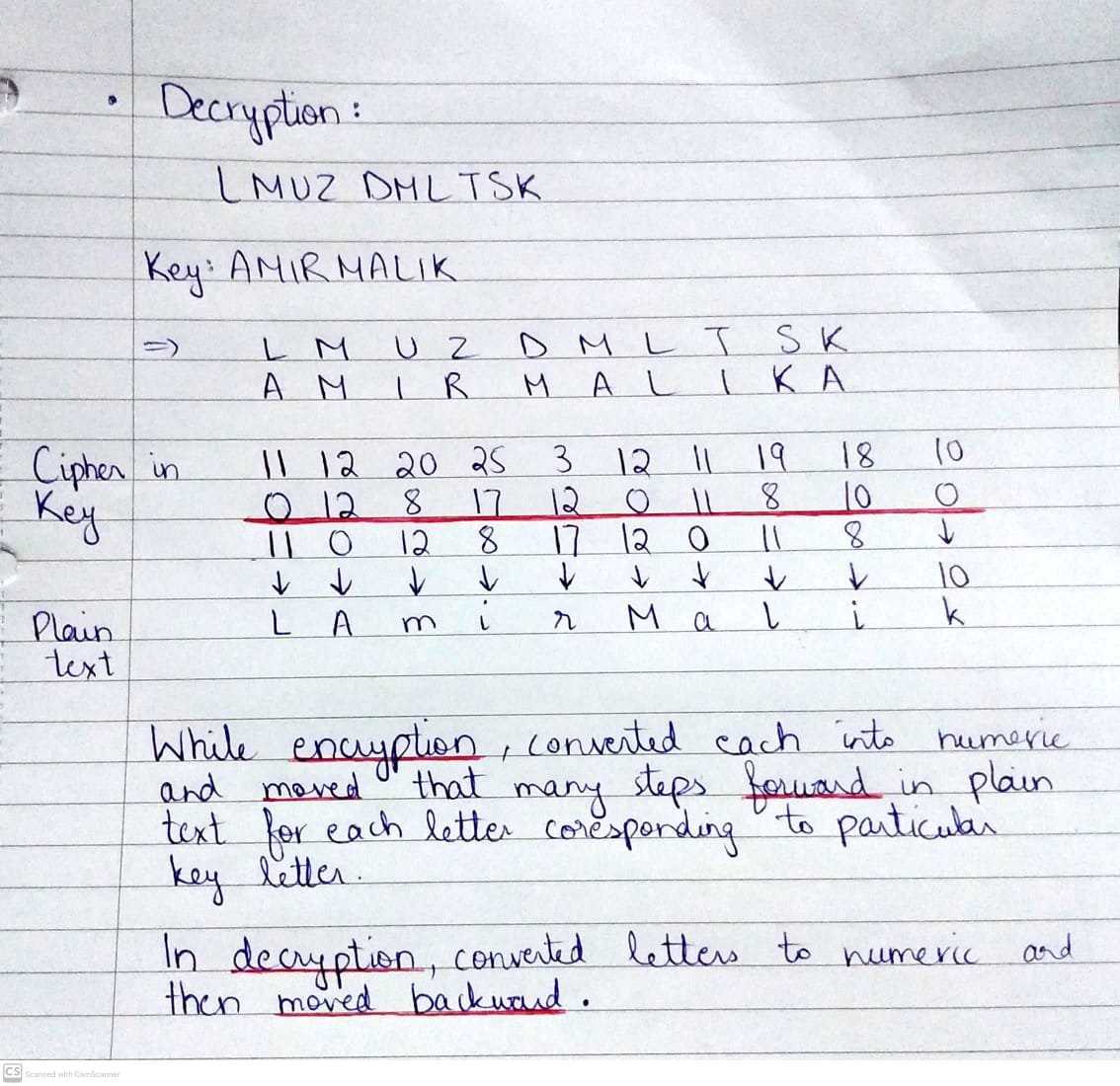
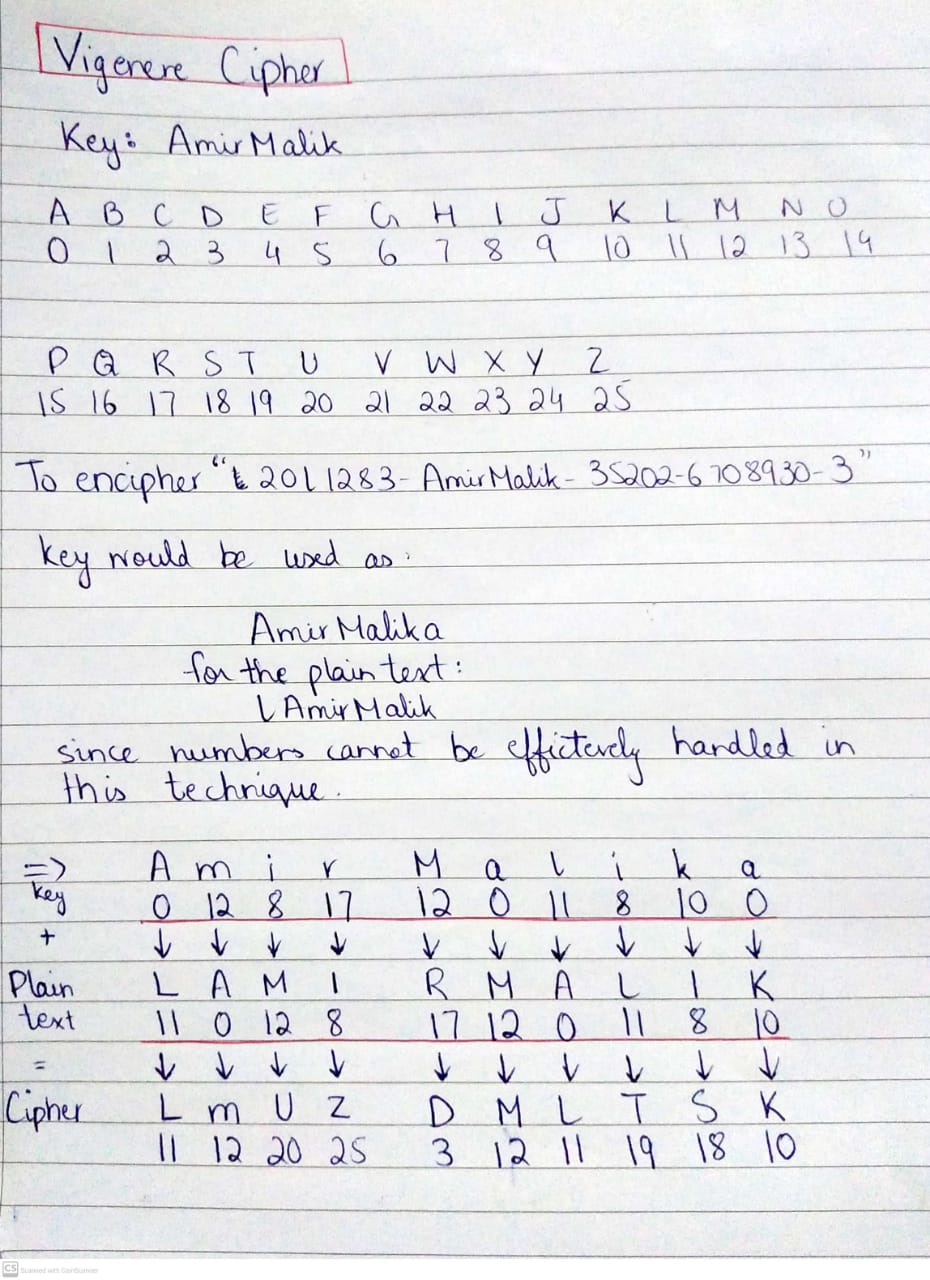
**BSSE-7B**

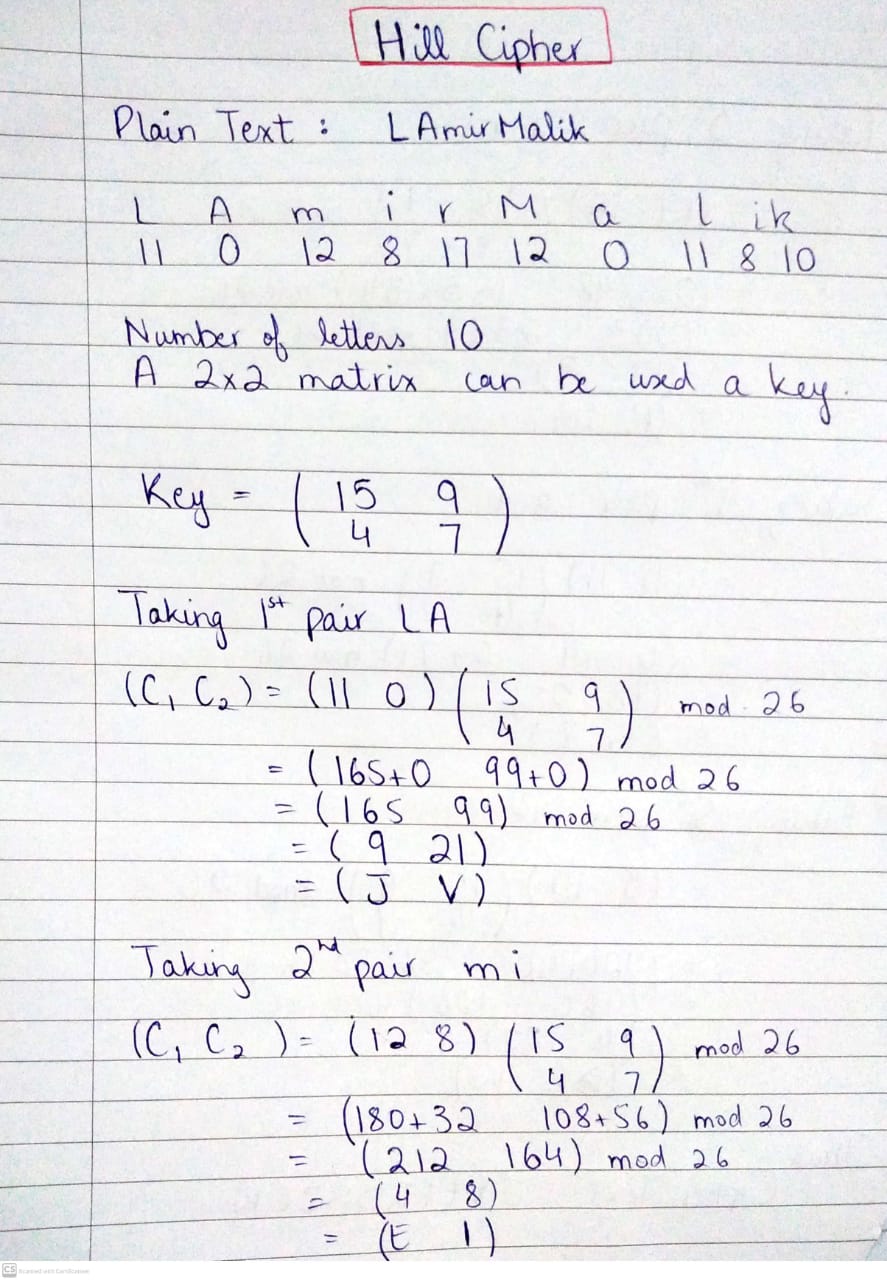
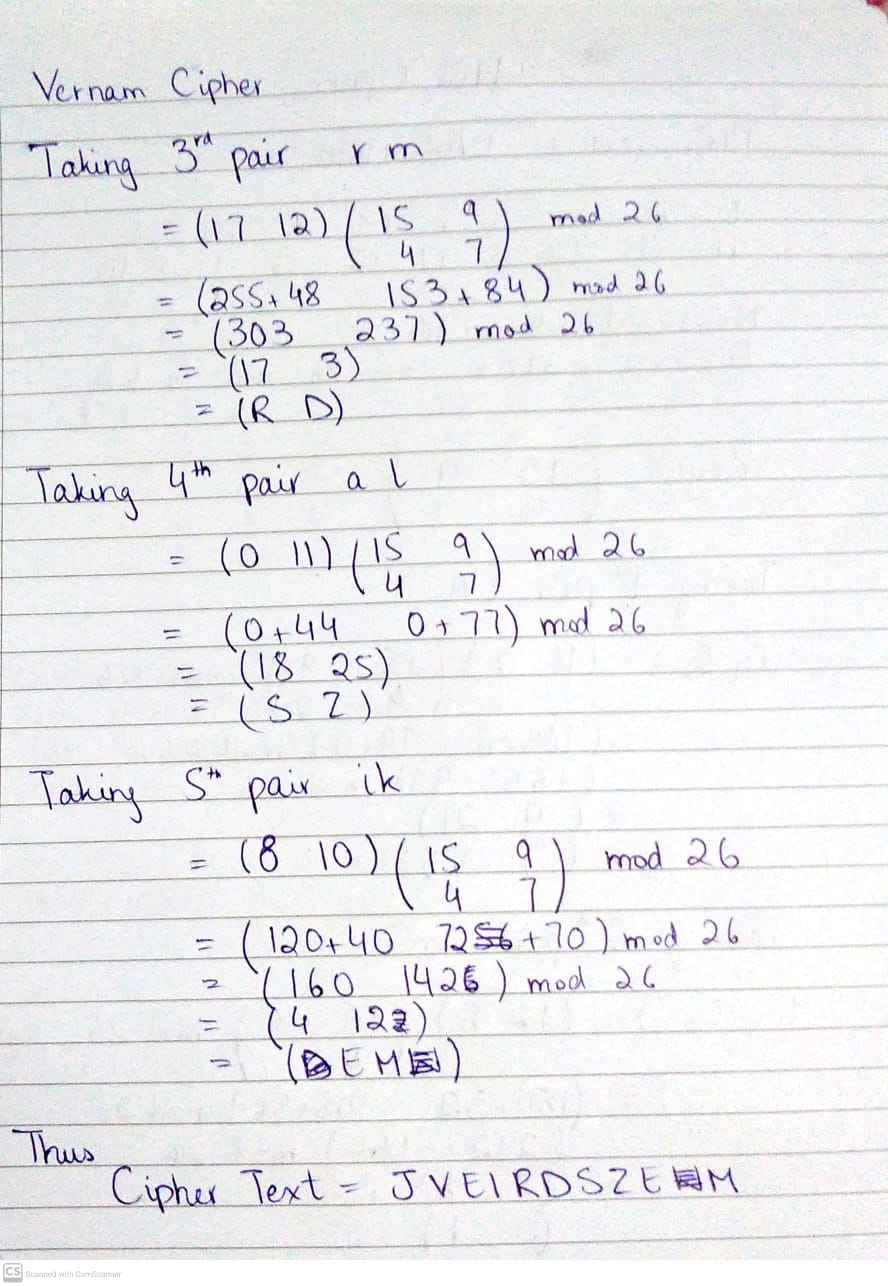
**Assignment 1**

**Plain Text:** 20l1283-Amir Malik-35202-6708930-2





### 

### 

### 

### 

### **Vernam Cipher**

**Plaintext**: lAmirMalik

**Key:** secretkeyy

Encryption:

| **Plain Text Letter** | **ASCII** |
| --- | --- |
| l | 108 |
| A | 65 |
| m | 109 |
| i | 105 |
| r | 114 |
| M | 77 |
| a | 97 |
| l | 108 |
| i | 105 |
| k | 107 |

**Key**

| s | 115 |
| --- | --- |
| e | 101 |
| c | 99 |
| r | 114 |
| e | 101 |
| t | 116 |
| k | 107 |
| e | 101 |
| y | 121 |
| y | 121 |

Plaintext:

01101100 01000001 01101101 01101001 01110010 01001101 01100001 01101100 01101001 01101011

Key:

01110011 01100101 01100011 01110010 01100101 01110100 01101011 01100101 01111001 01111001

Decimal: 31 36 14 27 21 57 10 9 16 18

Ciphertext: \x1F $ \x0E \x1B \x15 9 \n \t \x10 \x12

### **One Time Pad**

One time Pad is an advanced form of the Vernam Cipher.

**Plaintext:** "lAmirMalik"

**Key:** Key1234567

Plaintext:

01101100 01000001 01101101 01101001 01110010 01001101 01100001 01101100 01101001 01101011

Key:

01001011 01100101 01111001 00110001 00110010 00110011 00110100 00110101 00110110 00110111

Result:

00100111 00100100 00010111 01011000 01000010 01111110 01010101 01011000 01011110 01011100

Converting the binary ciphertext to decimal:

39 36 23 88 66 126 85 88 94 92

**Cipher:** &$wB~U^\\

As the name suggests all these classical ciphers designed in early times were used for encrypting alphabets. Hence for most of these there are no techniques defined for converting numbers, hyphens and other symbols into cipher.

However, it’s not entirely impossible. Several techniques can be applied in each method.

For example, in Caesar cipher, I have shifted numbers in the same manner as alphabets. That is, if the key is 2 then I have encoded 6 as 8 in my cipher.