Discrete Math

Task 3 Analysis

Name : Youssof Waleed Fathi

ID : 2101734

Group : 28

● Ciphering Overview :

- ❖ Ciphering is the process of converting a plain message into an unreadable format to protect its content from unauthorized access.

- ❖ It involves using a specific algorithm and ciphering keys to transform the original message (plain text) into an encoded message (cipher text).

- ❖ This ensures that only those with the correct keys can decode the message and retrieve its original meaning.

- ❖ Affine Encryption Rule :

$$C = (a(X) + b) \bmod len$$

- ➢ X : index of character to be ciphered
- ➢ a : first cipher key
- ➢ b: second cipher key
- ➢ len : length of the alphabet provided
- ➢ C : index of encrypted character

$$e_k(m) \equiv k_1 \cdot m + k_2 \pmod{p},$$

- Project Overview :

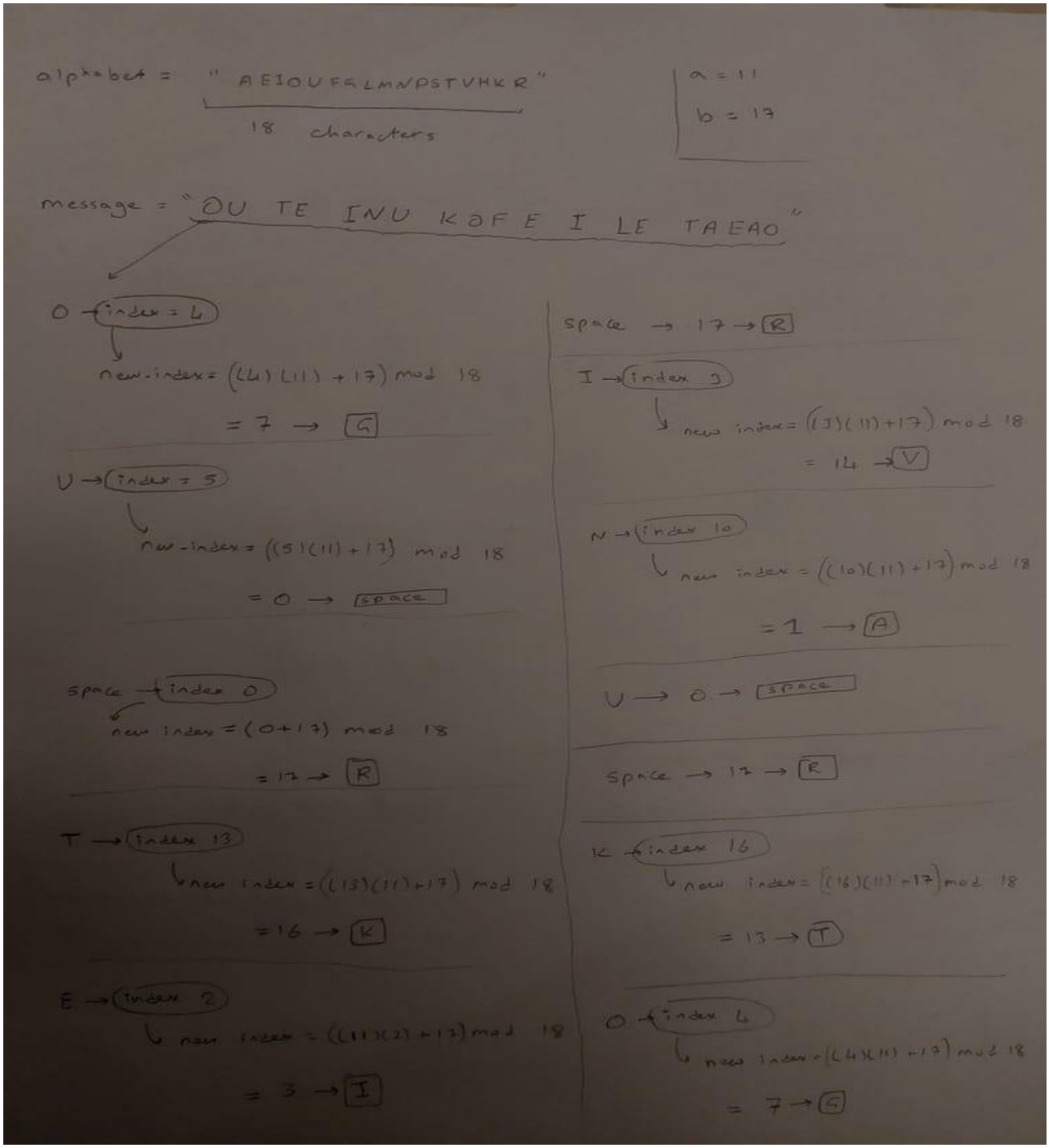
- The project addresses implementing a cpp code for cipher encryption algorithm .

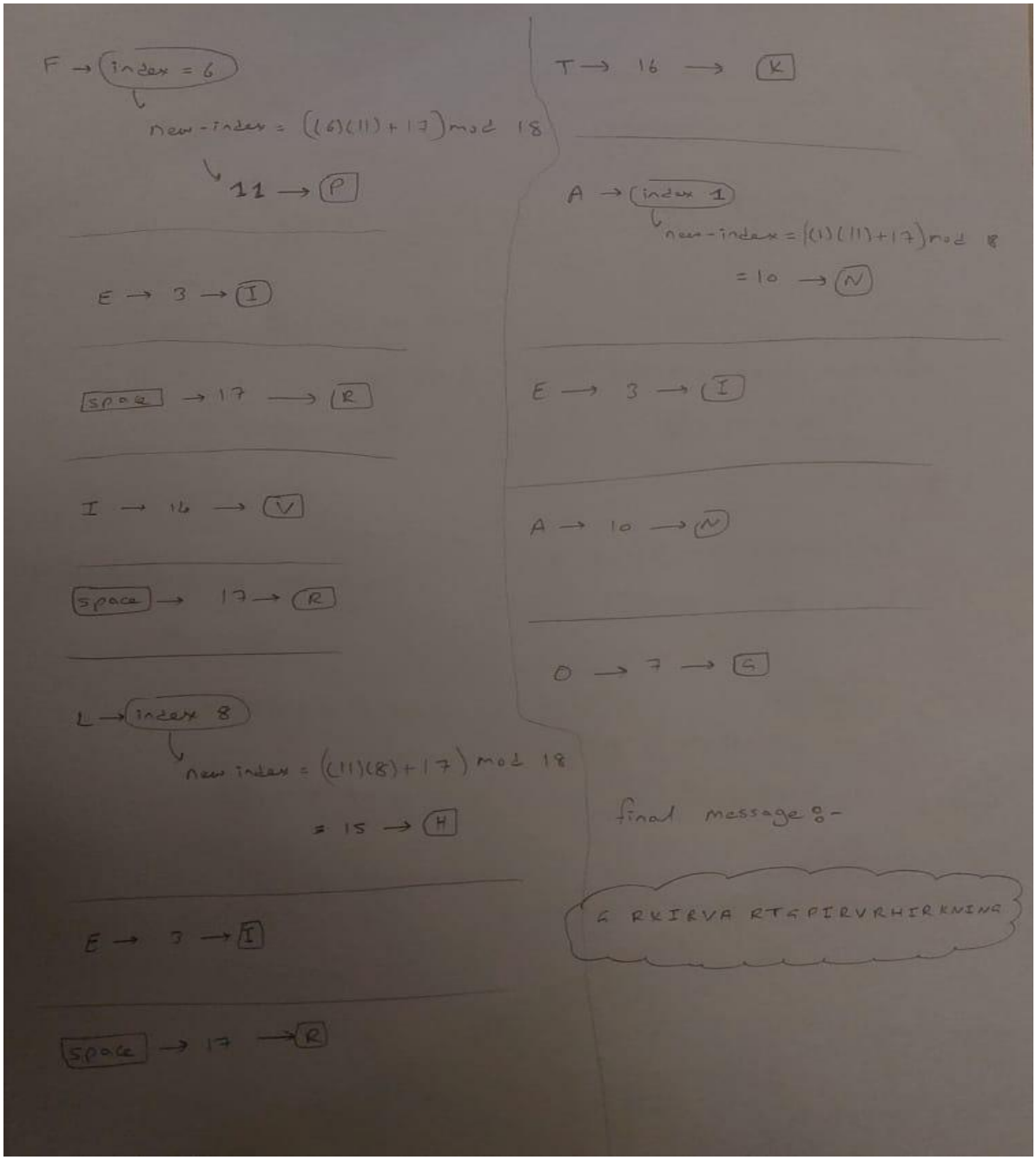
- Implementing 2 functions in order to do so (clean code) ,one function that encrypts characters and other function encrypts the whole function using the first function.

- Then using the example and alphabet provided , I have encrypted the original given message.

Task 3	**Affine Cipher keys**	**(a= 11, b=17)**
	Language	**Samoan Alphabet** https://blackboardjungle.co.nz/products/samoan-alphabet
	Text to be Ciphered	"OU TE INU KOFE I LE TAEAO"

- Analytical Paperwork :





❖ The final message : **G RKIRVA RTGPIRVRHIRKNING**

- Cpp Code :

```cpp
#include <iostream>
#include <string>

using namespace std;
```

- includes the necessary libraries for input/output operations (iostream) and string handling (string), and it uses the standard namespace for easier access to standard functions like cin and cout.

```cpp
//encrypt a single character function
char encryptChar(char ch, int a, int b, const string &alphabet) {
    int length = alphabet.length();
    int index = 0;
    bool check = false;

for(int i = 0; i<length;i++){ //loop to make sure character exists in alphabet
    if(alphabet[i]==ch){
        index = i;
        check = true; }
}

    if (check) { //checking if find function returned no position
        int new_index = (a * index + b) % length;
        return alphabet[new_index];
    }
    return ch; //if didn't exist -> return character itself without modification
}
```

- **encryptChar** function encrypts a single character using the Affine Cipher. It takes a character (ch), two ciphering keys (a and b), and an alphabet string as input and outputs a character .

- The function first loops through the alphabet to find the index of the character to ensure it exists.

- If the character is found, it calculates a new index using the formula (a * index + b) % length and returns the encrypted character at that new index.

- If the character is not found in the alphabet, it returns the character unchanged.

```
25  //encrypt the message using encryptChar function
26  string encryptMessage(const string &message, int a, int b, const string &alphabet) {
27      string final = "";
28      for (char ch : message) {
29          final += encryptChar(ch, a, b, alphabet);
30      }
31      return final;
32  }
33
```

- **encryptMessage** function encrypts an entire message using the encryptChar function. It takes the message to be encrypted, the ciphering keys (a and b), and the alphabet as inputs and returns the encrypted message.

- The function loops through each character of the message, encrypts it using encryptChar, and appends the encrypted character to string (final).

- Once all characters are processed, it returns the fully encrypted message.

```cpp
int main() {
    //samoan alphabet --> length : 18 (17 characters + space ( index 0 ) )

    string alphabet = " AEIOUFGLMNPSTVHKR"; // changing alphabet to be generic and fit different cases


    //example
    string message = "OU TE INU KOFE I LE TAEAO";

    //cipher keys
    int a = 11;
    int b = 17;

    string final = encryptMessage(message, a, b, alphabet);
    cout << "Original Message:" << message << endl;
    cout << "Encrypted Message:" << final << endl;

    return 0;
}
```

- **Main** function , used in order to run the given example and check if the code's functionality is correct.

- The function defines Samoan alphabet, an example message "OU TE INU KOFE I LE TAEAO" to be encrypted, and ciphering keys a = 11 and b = 17 are used for the Affine Cipher.

- The encryptMessage function is called to encrypt the message, and the original and encrypted messages are printed to the console.

```
Original Message:OU TE INU KOFE I LE TAEAO
Encrypted Message:G RKIRVA RTGPIRVRHIRKNING
```

- Final Output is the same as the analytical paperwork (**Validation**).