BUỔI 3: MẬT MÃ PLAYFAIR VÀ HILL

1. Mật mã Playfair

Cho các đoạn chương trình bên dưới

- Đoạn 1

```
// Ham lay phan du cua a va b
8 references
public static int mod(int a, int b)
{
    return (a % b + b) % b;
}
//Tim cac truong hop trung ky tu
1 reference
public static List<int> timTatCaTruongHop(string str, char value)
{
    List<int> indexes = new List<int>();
    int index = 0;
    while ((index = str.IndexOf(value, index)) != -1)
    {
        //Neu tim duoc ky tu trung voi value, them vi tri trung vao danh sach
        indexes.Add(index++);
    }
    return indexes;
}
//Xoa cac ky tu trung
1 reference
public static string xoatrung(string str, List<int> indexes)
{
    string retVal = str;
    for (int i = indexes.Count - 1; i >= 1; i--)
        retVal = retVal.Remove(indexes[i], 1); // Xoa cac ky tu trung, chi giu lai ky tu o vi tri dau tien

    return retVal;
}
```

- Đoạn 2

```
//Sinh ma tran khoa
2 references
private static char[,] sinhMTKhoa(string key)
{
    char[,] keySquare = new char[5, 5];
    //Xac dinh chuoi ky tu trong ma tran khoa
    string chuoiABC = "ABCDEFGHIKLMNOPQRSTUVWXYZ";
    //Neu khong nhap khoa, thi khoa mac dinh la CIPHER
    string tempKey = string.IsNullOrEmpty(key) ? "CIPHER" : key.ToUpper();
    //Thay the ky tu J bang I
    tempKey = tempKey.Replace("J", "I");
    tempKey += chuoiABC;
    //Xoa cac ky tu trung trong khoa
    for(int i = 0; i < 25; ++i)
    {
        List<int> indexes = timTatCaTruongHop(tempKey, chuoiABC[i]);
        tempKey = xoatrung(tempKey, indexes);
    }
    tempKey = tempKey.Substring(0, 25);
    //Xep vao ma tran tu phai qua trai, tren xuong
    for (int i = 0; i < 25; ++i)
    {
        keySquare[(i / 5), (i % 5)] = tempKey[i];
    }
    return keySquare;
}
```

- Đoạn 3

```
//Tim vi tri cua ky tu ch trong ma tran khoa keySquare, tra ve dong row va cot col
3 references
private static void timVitri(ref char[,] keySquare, char ch, ref int row, ref int col)
{
    if (ch == 'J')
        timVitri(ref keySquare, 'I', ref row, ref col);
    for (int i = 0; i < 5; ++i)
        for (int j = 0; j < 5; ++j)
            if(keySquare[i, j] == ch)
            {
                row = i;
                col = j;
            }
}
```

- Đoạn 4

```
1 reference
private static char[] cungDong(ref char[,] keySquare, int row, int col1, int col2, int encipher)
{
    return new char[] { keySquare[row, mod((col1 + encipher), 5)], keySquare[row, mod((col2 + encipher), 5)]};
}
1 reference
private static char[] cungCot(ref char[,] keySquare, int col, int row1, int row2, int encipher)
{
    return new char[] { keySquare[mod((row1 + encipher), 5), col], keySquare[mod((row2 + encipher), 5), col] };
}
1 reference
private static char[] cungDongCot(ref char[,] keySquare, int row, int col, int encipher)
{
    return new char[] { keySquare[mod((row + encipher), 5), mod((col + encipher), 5)], keySquare[mod((row + encipher), 5),
        mod((col + encipher), 5)] };
}

1 reference
private static char[] khacDongCot(ref char[,] keySquare, int row1, int col1, int row2, int col2)
{
    return new char[] { keySquare[row1, col2], keySquare[row2, col1] };
}
```

- Đoạn 5

```
//Xoa cac ky tu khac ABC
3 references
private static string xoaKytuKhac(string input)
{
    string output = input;

    for (int i = 0; i < output.Length; ++i)
        if (!char.IsLetter(output[i]))
            output = output.Remove(i, 1);

    return output;
}
//Dieu chinh ket qua tra ve dung khoang trang da cho
1 reference
private static string tuychinhOutput(string input, string output)
{
    StringBuilder retVal = new StringBuilder(output);

    for (int i = 0; i < input.Length; ++i)
    {
        if (!char.IsLetter(input[i]))
            retVal = retVal.Insert(i, input[i].ToString());

        if (char.IsLower(input[i]))
            retVal[i] = char.ToLower(retVal[i]);
    }

    return retVal.ToString();
}
```

- Đoạn 6

```
private static string Cipher(string input, string key, bool encipher)
        {
            string retVal = string.Empty;
            key = xoaKytuKhac(key);
            char[,] keySquare = sinhMTKhoa(key);
            string tempInput = xoaKytuKhac(input);
            int e = encipher ? 1 : -1;

            if ((tempInput.Length % 2) != 0)
                tempInput += "X";

            for (int i = 0; i < tempInput.Length; i += 2)
            {
                int row1 = 0;
                int col1 = 0;
                int row2 = 0;
                int col2 = 0;

                timVitri(ref keySquare, char.ToUpper(tempInput[i]), ref row1, ref col1);
                timVitri(ref keySquare, char.ToUpper(tempInput[i + 1]), ref row2, ref
col2);

                if (row1 == row2 && col1 == col2)
                {
                    retVal += new string(cungDongCot(ref keySquare, row1, col1, e));
                }
                else if (row1 == row2)
                {
```

```
                    retVal += new string(cungDong(ref keySquare, row1, col1, col2, e));
                }
                else if (col1 == col2)
                {
                    retVal += new string(cungCot(ref keySquare, col1, row1, row2, e));
                }
                else
                {
                    retVal += new string(khacDongCot(ref keySquare, row1, col1, row2,
col2));
                }
            }

            retVal = tuychinhOutput(input, retVal);

            return retVal;
        }
        public static string Encipher(string input, string key)
        {
            return Cipher(input, key, true);
        }

        public static string Decipher(string input, string key)
        {
            return Cipher(input, key, false);
        }
```

- Đoạn 7

```
static void Main(string[] args)
        {
            Console.Write("Nhap vao ban ro: ");
            string text = Console.ReadLine().Trim();
            Console.Write("Nhap vao khoa: ");
            string key = Console.ReadLine().Trim();

            char[,] keysquare = sinhMTKhoa(xoaKytuKhac(key));
            for(int i = 0; i < keysquare.Length; i++)
                Console.Write((i % 5 == 0 ? "\n" : " ") + keysquare[i / 5, i % 5]);
            Console.WriteLine();

            string banma = Encipher(text, key);
            string banrogoc = Decipher(banma, key);

            Console.WriteLine("Ban ma: " + banma);
            Console.WriteLine("Ba ro goc: " + banrogoc);
            Console.ReadKey();
        }
```

- Cho biết đoạn 1, 2, 3 và 4 được sử dụng để làm gì?

- Dựa trên các đoạn chương trình xây dựng một ứng dụng winform cho phép người dùng nhập vào bản rõ, khóa. Ứng dụng hiển thị kết quả mã hóa theo playfair và ma trận khóa

2. Mật mã Hill

Tìm hiểu và viết đoạn chương trình mã hóa đối với hệ mật mã Hill