作業二：加密

學號：C24106082
姓名：陳宏彰

2022-09-20

1 原理

1.1 加密

金鑰的六個數字依序為 $a\ b\ c\ d\ e\ f$，明文的每兩個字為 $x\ y$，帶入 $X = ax+by+c\,Y = dx+ey+f$，得到的數字再用 62 進位編碼($0-9a-ZA-Z$)。在輸出的時候再加上每個字加密後的位數用 62 位元編碼當前綴，例如 $4Y$ $8R$ 會各加上 2 後再串起來，變成 $24Y28R$，全部串起來就得到密文

1.2 解密

依照位數前綴將密文差開、轉成 10 進位用克拉瑪公式解出 $x\ y$，就得到原本的明文

2 使用範例

2.1 加密

$ go run . encrypt 1 2 3 4 5 6 'ncku information security'
2512fb25y2gr23X2aD2572fq25w2gs24W2eX25j2g325o2g824h2br24S2eB25C2gQ25u2ge2322au

2.2 解密

```
$ go run . decrypt 1 2 3 4 5 6 '2512fb25y2gr23X2aD2572fq25
w2gs24W2eX25j2g325o2g824h2br24S2eB25C2gQ25u2ge2322au'
ncku information security
```

3 程式碼

完整程式碼在 https://github.com/simbafs/NCKU-IS-HW2，以下僅擷取部份

3.1 加密

```
func Encrypt(e1, e2 *Equation, secret string) string {
        if len(secret)%2 == 1 {
                secret += " "
        }

        var encrypted string
        for i := 0; i < len(secret); i += 2 {
                x, y := secret[i], secret[i+1]
                X, Y := e1.CalcText(x, y), e2.CalcText(x, y)
                // fmt.Println(x, y, X, Y)
                lX, lY := to62(int64(len(X))), to62(int64(len(Y)))
                encrypted += lX + X + lY + Y
        }

        return encrypted
}
```

3.2 解密

```
func Decrypt(e1, e2 *Equation, secret string) string {
        s := ""

        for i := 0; i < len(secret); {
                lX := toDec(string(secret[i]))
                i++
                X := toDec(secret[i : i+int(lX)])
                // fmt.Println("\t")
```

```
                i += int(lX)
                lY := toDec(string(secret[i]))
                i++
                Y := toDec(secret[i : i+int(lY)])
                i += int(lY)
                x, y := e1.Solve(e2, X, Y)
                // fmt.Println(lX, X, lY, Y, x, y)
                s += string(x) + string(y)
        }

        return s
}
```