**CS4003701 資訊安全導論 HW\_1**

**Introduction to Information Security**

**A10615003 張家成 —— 負責加密部分 （此文檔編寫者）**

A10615001 趙梓丞 —— 負責解密部分

建置環境：

MacOS 10.14 Mojave



Eclipse oxygen



Java SE – 1.7

Jdk 9.0.1

程式運行截圖：

測資：均源於HW1.pdf 檔案

1. Caesar Cipher – encrypt

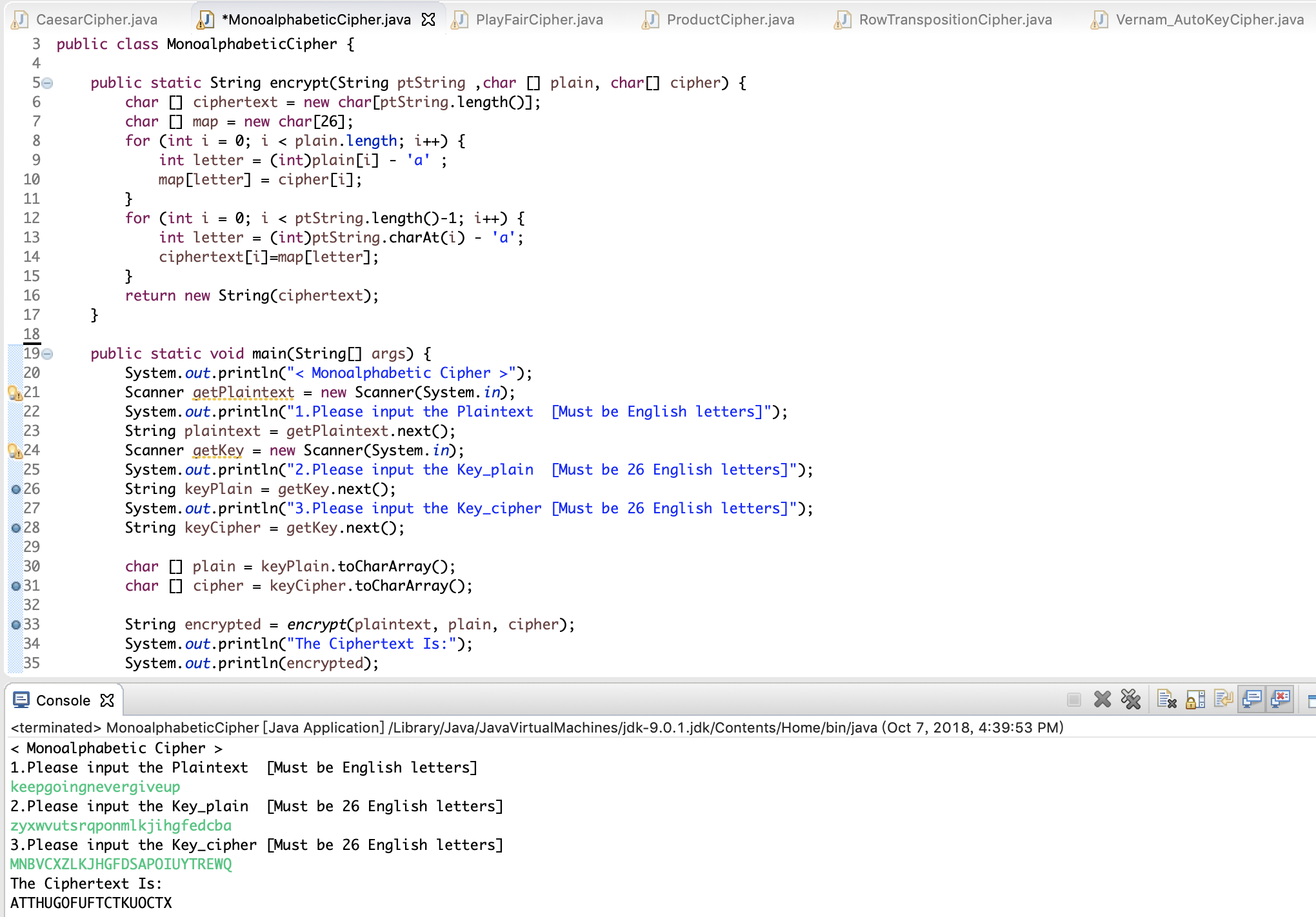


plaintext = keepgoingnevergiveup

key = 7

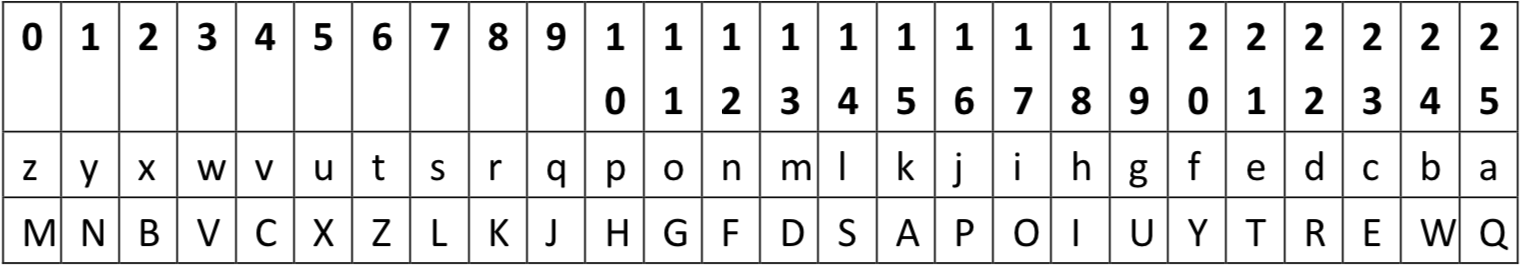
ciphertext = rllwnvpunulclynpclbw

1. Monoalphabetic Cipher – encrypt



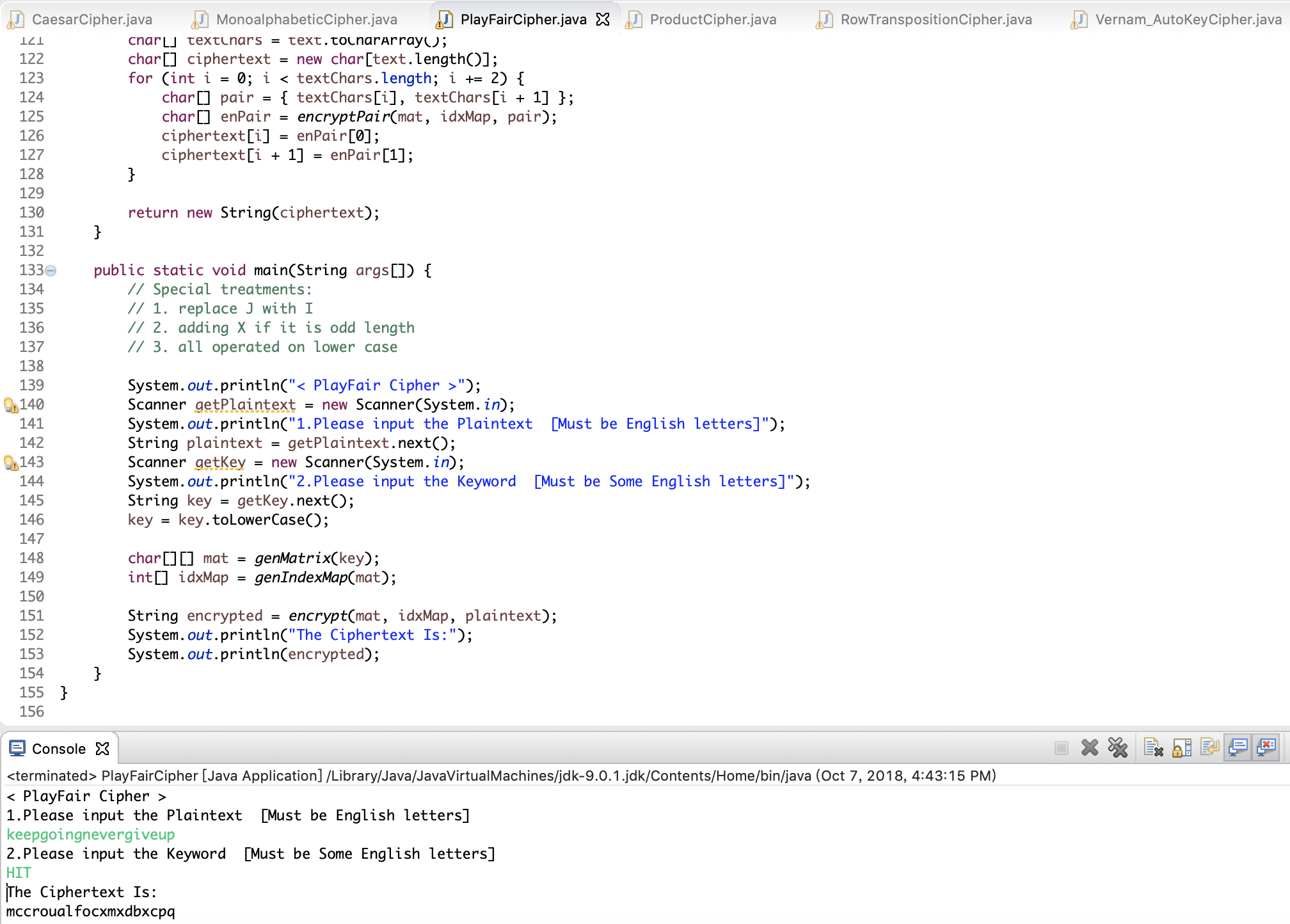
plaintext = keepgoingnevergiveup

key =



ciphertext = ATTHUGOFUFTCTKUOCTX

1. Playfair Cipher – encrypt

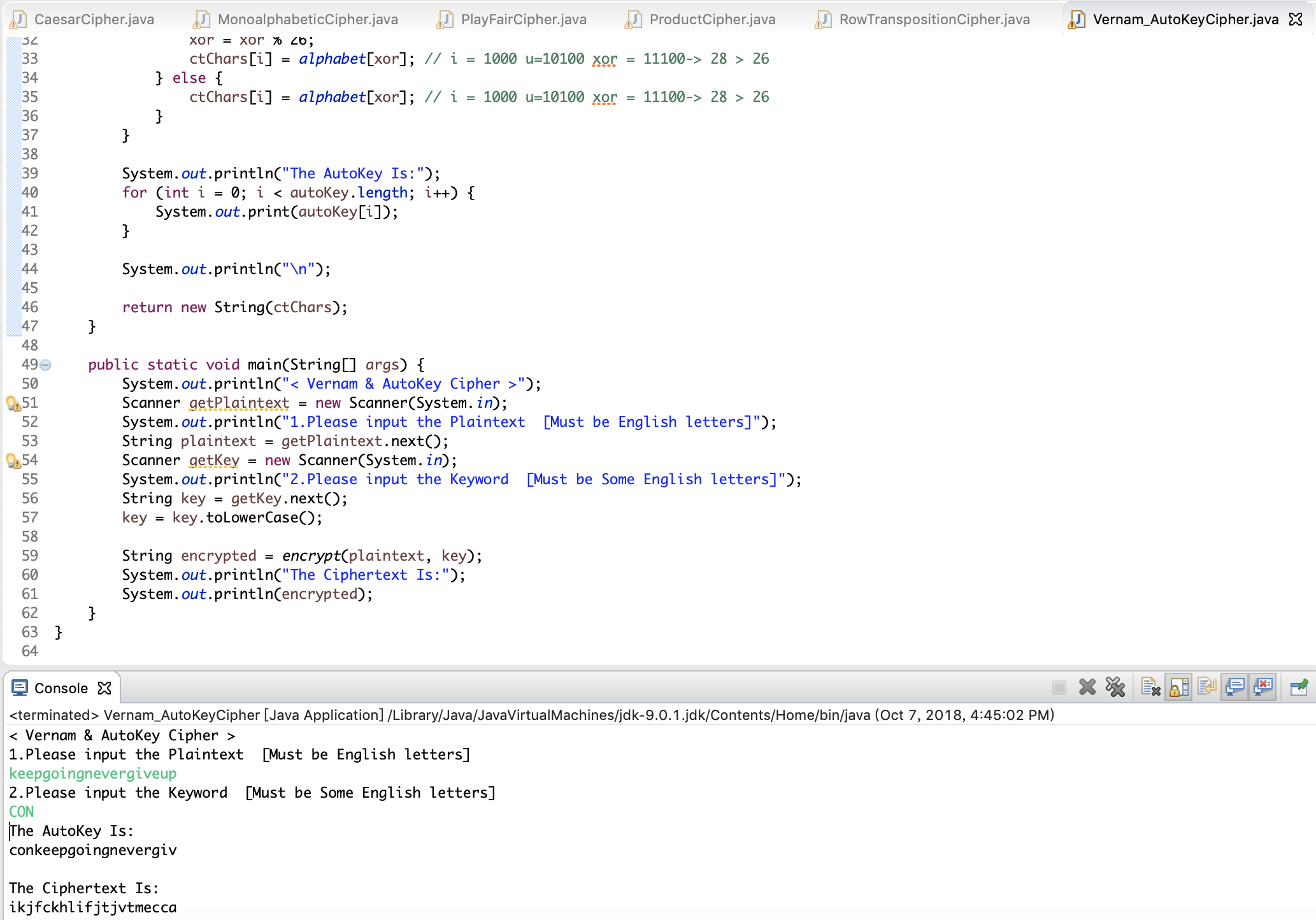


plaintext = keepgoingnevergiveup

key = HIT

ciphertext = mccroualfocxmxdbxcpq

1. Vernam\_AutoKey Cipher – enctypt



PS:

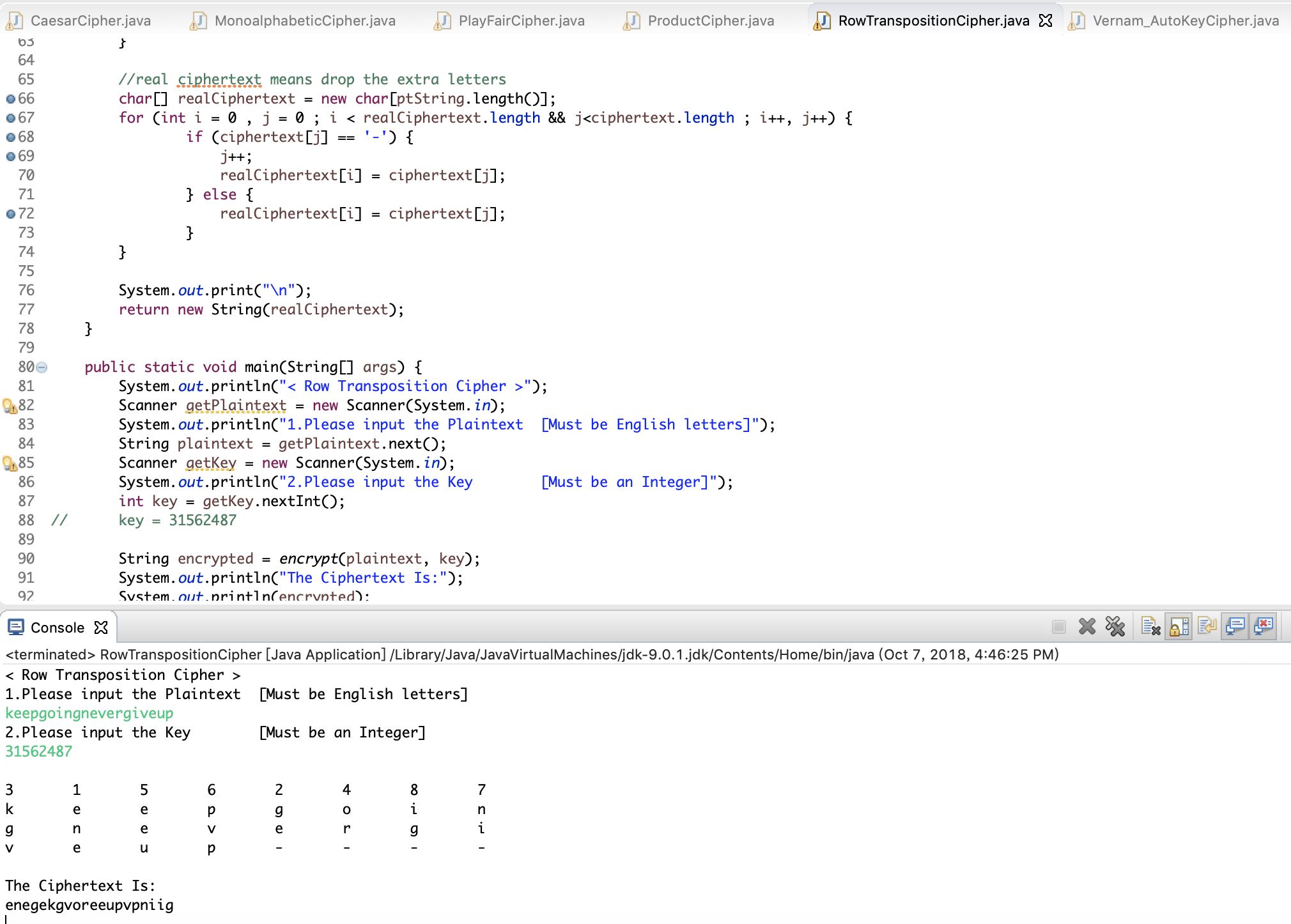
超出26的部分使用%運算。

plaintext = keepgoingnevergiveup

key = CON

ciphertext = ikjfckhlifjtjvtmecca

1. Row Transposition Cipher – encrypt



PS:

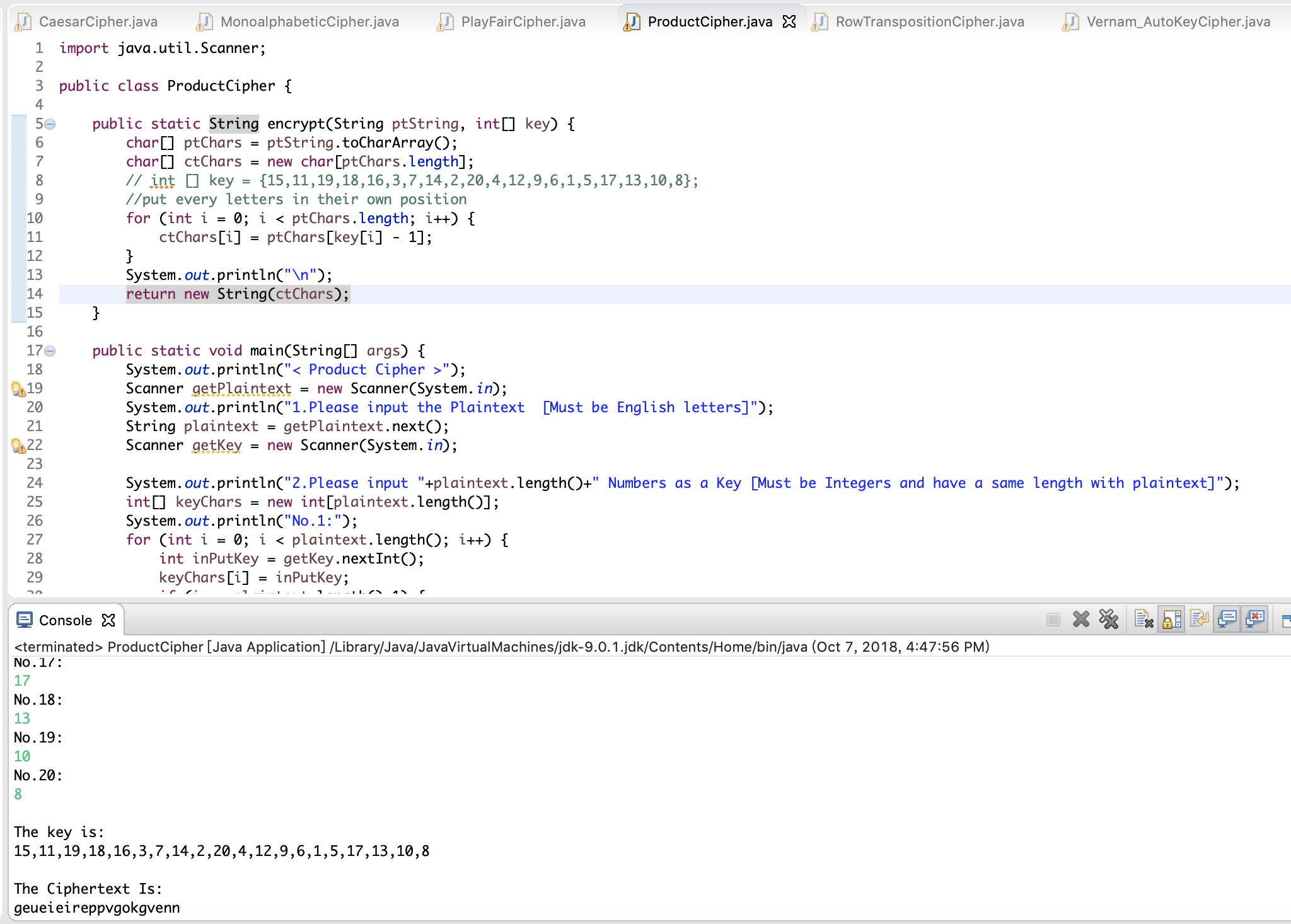
使用‘-’符號來填充空餘部分，不影響加解密。

plaintext = keepgoingnevergiveup

key = 31562487

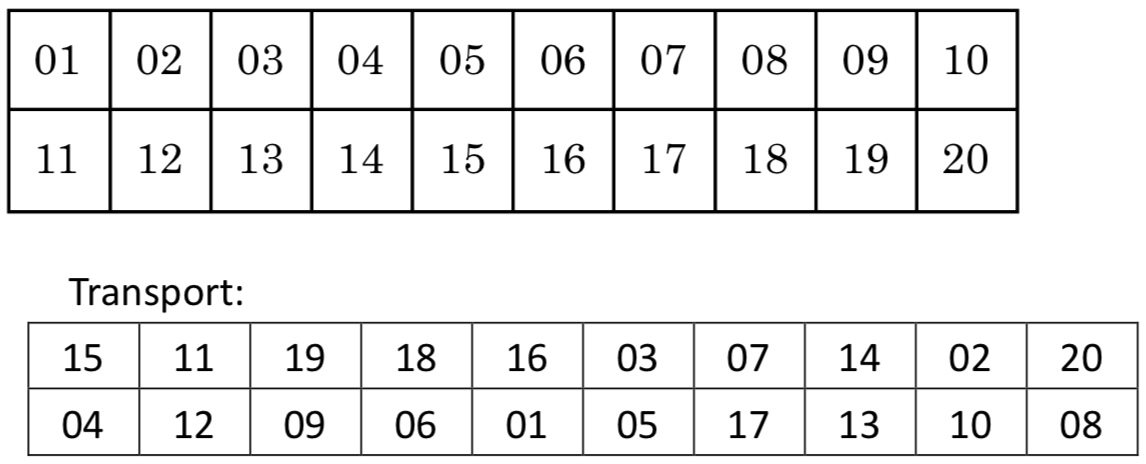
ciphertext = enegekgvoreeupvpniig

1. Product Cipher – encrypt



plaintext = keepgoingnevergiveup

key =



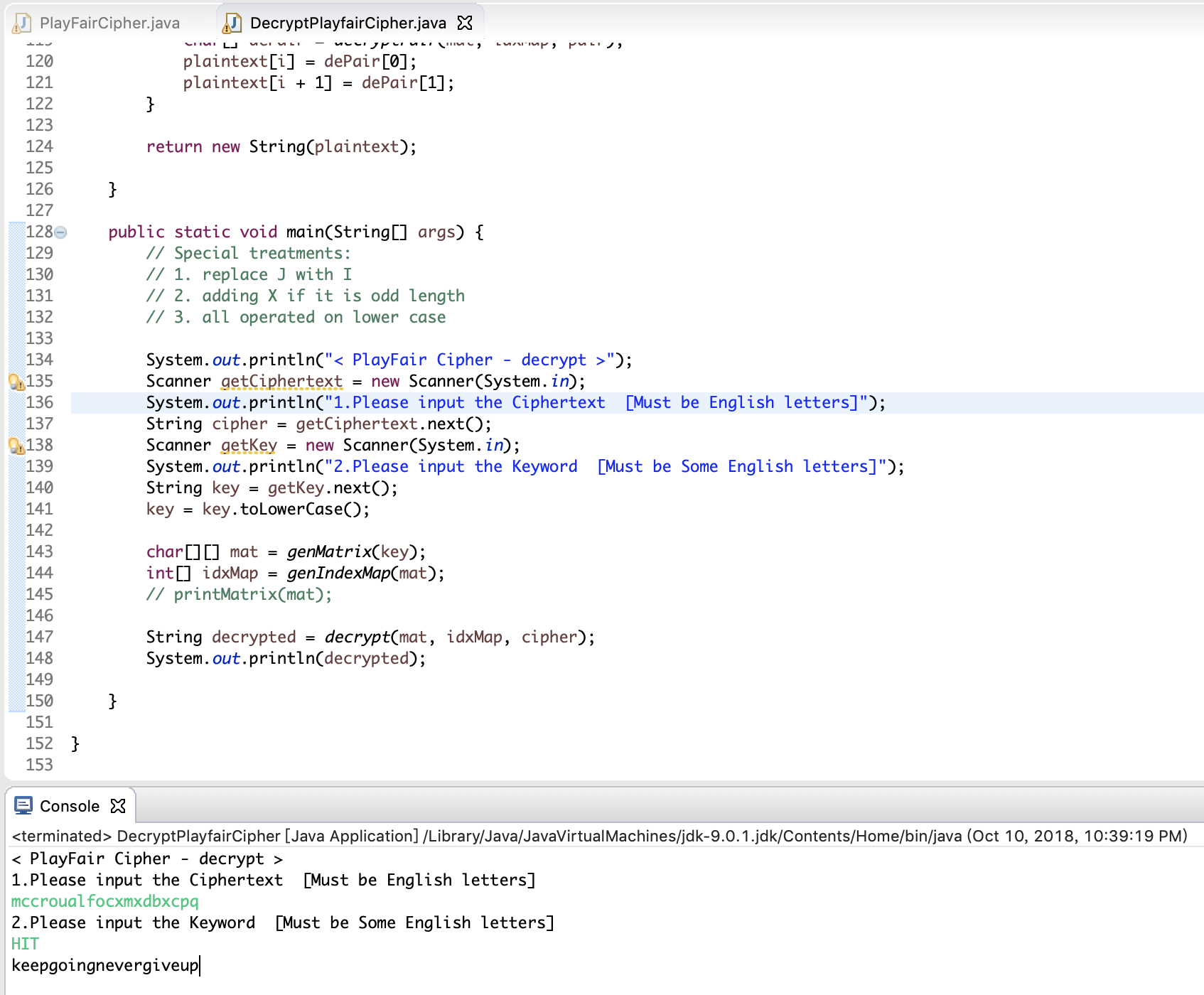
ciphertext = geueieireppvgokgvenn

Extra.

Playfair Cipher – decrypt

負責解密部分的組員在實作playfair解密時遇到了困難，

於是我嘗試著完成playfair Cipher的解密。



ciphertext = mccroualfocxmxdbxcpq

key = HIT

plaintext = keepgoingnevergiveup