# Exercise 01

## Overview

This exercise provides hands-on experience with Cryptography to perform simple cryptanalysis attacks on a variant of Julius Ceaser rotation cipher.

## Learning Objectives

- Understand basics of cryptography
- Understand ciphertext only attacks
- Ability to apply basic cryptanalysis technology to identify algorithmic weakness in simple transformation based on Ceaser's transformation

## Reading Material

1. https://en.wikipedia.org/wiki/Caesar_cipher
2. https://en.wikipedia.org/wiki/Polyalphabetic_cipher

## Prerequisites and environment familiarity

Student should be familiar with Linux and command line terminal usage.
Student should be familiar with rotation cipher as used in Ceaser's cipher

## Description

The assignment is to carry out a ciphertext only cryptanalysis attack. You are given a ciphertext consisting of approximate 600 characters. The ciphertext uses a variation of Ceaser's cipher and polyalphabetic cipher. The plaintext consists of Alphabets (both upper case and lower case), SPACE (' ') character and dot('.'). Thus, a total of 54 characters are used in the plaintext. It is not necessary that all 54 characters are present in plaintext.

The substitution cipher works as follows. Each upper-case alphabet is substituted by another upper case alphabet chosen randomly and similarly each lower case alphabet is substituted by another lower case Chosen randomly. For example, letter 'A' is substituted by 'B', 'C' is substituted by 'O', 'a' is substituted by 'c', 'c' is substituted by 'm', and so on. The non-alphabetic characters SPACE(' ') and DOT('.') are substituted by either by '_' and '@' or by '@' and '_'.

Your job is to decipher the ciphertext to plaintext. The useful approach is to do a frequency analysis of given ciphertext and apply knowledge of English language where letters 'e' or 'a' appear lot more often in any English text and letter 'z' and 'x' appear much less.

## Example

### Ciphertext

```
Rp@ye@fmq@zmipyfg@jmz@wieyfgeege@pm@hzmuycg@x@uxzygpk@mj@hzmpg
opymfe@yforicyfa@gfozkhpymf@jmz@yfjmzbxpymf@pnxp@ye@pzxfebyppg
c@xozmee@fgpqmzse@uyx@png@Rfpgzfgp@mz@uyx@qyzgrgee@cguyoge_@@X
fog@cxpx@xzg@epmzgc@rmoxrrk@qnyon@ye@zgjgzzgc@pm@xe@cxpx@xp@zg
ep@pngf@pngzg@ye@mjpgf@rypprg@hzmpgopymf@wgkmfc@cmbxyf@xipngfp
yoxpymf@xfc@mhgzxpyfa@ekepgb@xoogee@omfpzmre_@Gxpx@xp@zgep@xzg
@mjpgf@zmipyfgrk@wxosgc@ih@pm@egomfcxzk@epmzxag@eion@xe@mhpyox
r@bgcyx@pxhg@mz@zgbmuxwrg@cyes@xzonyugc@jmz@yfcgjyfypg@hgzymce
```

```
_@Oizpngz@gugf@qngf@cxpx@xzg@gzxegc@jzmb@x@nxzc@cyes@ifpyr@png
@zgrguxfp@cyes@egopmze@xzg@zgiegc@png@cxpx@xzg@zgomugzxwrg_
```

Key mapping (ciphertext->plaintext) for max occurring character in cipher text

```
g -> e
```

### Plaintext

The above ciphertext corresponds to below plaintext

```
     It is now routine for businesses to provide a variety of
protections including encryption for information that is
transmitted across networks via the Internet or via wireless
devices.  Once data are stored locally which is referred to as
data at rest then there is often little protection beyond
domain authentication and operating system access controls.
Data at rest are often routinely backed up to secondary
storage such as optical media tape or removable disk archived
for indefinite periods. Further even when data are erased from
a hard disk until the relevant disk sectors are reused the
data are recoverable.
```

### Substitution keys

```
     ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz .
     PVUGZOTQRHFICBXDNLMWEYSJAKxwocgjanylsrbfmhvzepiuqtkd@_
```

### Explanation and Hints

In this substitution cipher, SPACE is substituted by '@' and DOT('.') is substituted by '_'. The letter 'I' is substituted by 'R', 't' is substituted by 'p' and so on. Doing a frequency analysis in ciphertext, three most common character occurrences are

'g': more than 60 times

'x': more than 45 times.

'y': more than 35 times

Thus, these letters are likely to be substituted from 'e', 'a', 'i etc. Based on these trial and error, replace other letters similarly, arrive at the word that makes sense.

Hint: First replace '_' and '@' appropriately to help define the word boundaries.

## Assessment

Please do submit the following

1. Cipher text and Plain text (4 marks)
2. Substitution keys used (2 marks)
3. Steps taken to identify the plain text (2 marks)
4. Challenges faced and how did you address these (2 marks)

## Note

Any plagiarism activity will result in penalties of being awarded 0 marks.

<end of Exercise 01>