School of Electrical and Information Engineering
University of the Witwatersrand, Johannesburg
ELEN3015 – Data and Information Management

Classical Cryptography - Extra problems

1 Polyalphabetic cipher

Consider the two ciphers:

1. Cipher 1: $P_1(\lambda) = (4\lambda + 11)\mathbf{mod}26$
2. Cipher 2: $P_2(\lambda) = (C_1\lambda + C_0)\mathbf{mod}26$

Questions:

1. Why doesn't the translation table work?
2. What values of C_1 and C_2 will work? What are the properties of those values?
3. What is the keyspace of this cipher?

2 Method of Kasiski

Use the method of Kasiski to determine the most likely key length that was used in the following polyalphabetic encryption. Explain how you would recover the plaintext after finding the key length.

```
aiekw   lwmji  kiwpx  abmcm  llicx  zteyv  kiwpx
abmcm   llicx  ztiqi  guesw  vdtsx  opadl  wpoos
xuwyp   ahpxi  khqda  shbri  wewml  gujop  atnsx
opadl   wtxyg  zdnsr
```