

**COMP3260/COMP6360 Data Security**  
**Week 5 Workshop – 22<sup>nd</sup> and 24<sup>th</sup> March 2021**

1. For polyalphabetic substitution cipher with period  $d$  estimate the unicity distance, assuming that all keys are equally likely.
2. Decipher the following ciphertext, which was enciphered using a Vigenere cipher with key ART: YFN GFM IKK IXA T.
3. Decipher the following ciphertext, which was enciphered using a Beaufort cipher with key ART: CDZ ORQ WRH SZA AHP
4. Consider a linear substitution cipher that uses the transformation  $f(a) = ak \bmod 26$ . Suppose you know with certainty that the plaintext letter J(9) corresponds to the ciphertext letter P(15), that is,  $9k \bmod 26 = 15$ . Break the cipher by solving for  $k$ .
5. Consider again a linear substitution cipher that uses the transformation  $f(a) = ak \bmod 26$ . Suppose you know with certainty that the plaintext letter N(13) corresponds to the ciphertext letter N(13), that is,  $13k \bmod 26 = 13$ . Can you break the cipher by solving for  $k$ ? What about if you also know that the plaintext letter C(2) corresponds to the ciphertext G(6)?
6. Consider again a linear substitution cipher that uses the transformation  $f(a) = ak \bmod 26$ . Suppose that you suspect that the plaintext letter N(13) corresponds to the ciphertext letter P(15), that is,  $13k \bmod 26 = 15$ . Can you break the cipher by solving for  $k$ ?
7. Consider the Measure of Roughness  $M = \sum_{i=0}^{n-1} (p_i - \frac{1}{n})^2$  and consider the alternative versions  $M_1 = \sum_{i=0}^{n-1} (p_i - \frac{1}{n})$  and  $M_2 = \sum_{i=0}^{n-1} |p_i - \frac{1}{n}|$ . Could each of  $M_1$  and  $M_2$  be used in place of  $M$ ? If yes, which one is a better?