The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security
Week 4 Workshop – 21st and 22nd March 2019

1) Consider the following ciphertexts:

- XXXXX
- VWXYZ
- RKTIC
- JZQAT

Which of the these ciphertexts could result from enciphering five-letter words of English using:

a) A substitution cipher, where each letter is replaced with some other letter, but the letters are not necessarily shifted as in the Caesar cipher (thus A could be replaced with K, B with W, etc).
b) Any transposition cipher.

2) Intercepted ciphertext is C=TEHAOEHIETURRNBTNIETOWDT. Single letter frequency analysis indicates that this is a transposition cipher. Find the matching plaintext.

3) Consider a homophonic cipher that uses 26h ciphertext symbols, assigning h homophones to each letter of the English alphabet. Determine the number of possible keys (i.e., assignments of homophones), and use your result to calculate unicity distance of the cipher.

4) A generalization of the shift cipher, known as the affine cipher, is as follows: f(p)=(ap+b) mod 26. A requirement that any encryption function needs to satisfy is to be *one-to-one*, that is, if p≠q then f(p) ≠ f(q), otherwise the encryption would be impossible, as more than one plaintext character maps into the same ciphertext character. The affine cipher is not necessarily one-to-one; for example, for a=2 and b=3, f(0)=f(13)=3.

a) Are there any limitations on the value of b? If yes, determine which values are not allowed.
b) Are there any limitations on the value of a? If yes, determine which values are not allowed.
c) Provide a general statement of which values of a and b are not allowed.

5) How many one-to-one affine ciphers are there?

6) A ciphertext has been generated with an affine cipher. The most frequent letter of the ciphertext is "B", and the second most is "U". Based on this information, try to break the cipher.

7) In one of his cases, Sherlock Holmes was confronted with the following message:

534 C2 13 127 36 31 4 17 21 41 douglas 109 293 5 37 birlstone 26 birlstone 9 127 171

Although Watson was puzzled, Holmes was able immediately to deduce the type of cipher. Can you?

8) For each one of the following ciphers estimate the unicity distance, assuming that all keys are equally likely:

a) Transposition cipher with period d

b) Shift cipher $c = (p + k) \bmod 26$

c) Affine cipher $c = (k_1 p + k_0) \bmod 26$, where $\gcd(k_1, n)=1$

d) General monoalphabetic substitution cipher