ITS64304: Theory of Computation
Tutorial – 7: Classical Cryptography

Aim

The aim of this tutorial is to understand the relationship between Complexity and Cryptography. You will understand how cryptography can be made secure by making use of problems with high complexity. By the end of this tutorial you should be able to estimate how long it will take to break certain crypto systems and hence determine how long they remain secure. (Aligns to Module Learning Outcome 4)

Taylor's Graduate Capabilities (TGCs) developed

7.1 Ciphers

i) Consider the following message, encoded in a cipher.

JXIXVPFX FP X CLLA EBXSBK

Break the code; describe briefly the method used, and how long it took to break. What is the message?

ii) What is the maximum number of possible attempts needed to break the code? How is the number related to the size of the alphabet?

iii) If the message was encoded as an arbitrary mapping of letters to letters, such that for e.g., 'a' becomes 'x', 'b' becomes 'g', and 'c' becomes 'l', how does this change the maximum?

iv) How long in terms of time would it take to break such a message encoded as above, if we could perform 1000 attempts per second?

7.2 More Ciphers

More ciphers for you to break.

i) CD EPXC CD VPXC

ii) OVGH SZEV HLNV UFM DRGS XRKSVIH

iii) WNR DKT DEE KNT MRRAPTU?

iv) TEETEIAEOEOA HWAHRSWSMTDY

v) VM VH GV FG RV RE MG CW FS NP FD LF QN GL DB OQ NO UM OP BR UP VF TM TN TD

7.3 Scenario

A large financial institution, for example ABS Bank, uses the RSA technique for encrypting its data. One day it hears that an algorithm has been published on the web, claiming to be a linear-time factorization algorithm. Assume yourself as a Security Consultant and ABS Bank has asked you to investigate this claim, and to recommend an appropriate course of action. How would you go about investigating this claim? Assuming that your analysis shows the claim to be valid, what course of action would you recommend?

7.4 Reflection

Why or how intractable problems are useful in cryptography? What could be the possible risk in this approach? Record you observations in the tutorial summary sheet.

-oo0oo-