Section 1 Lecture 6 – Substitution ciphers - Solutions

Q1)

ON TWO OCCASIONS I HAVE BEEN ASKED, “PRAY MR BABBAGE, IF YOU PUT INTO THE MACHINE WRONG FIGURES, WILL THE RIGHT ANSWERS COME OUT?” I AM NOT ABLE RIGHTLY TO APPREHEND THE KIND OF CONFUSION OF IDEAS THAT COULD PROVOKE SUCH A QUESTION.

Q2) The apostrophes give you a good starting point: ‘A must almost certainly be ‘S and ‘XX must almost certainly be ‘LL

"History has taught us: never underestimate the amount of money, time, and effort someone will expend to thwart a security system. It's always better to assume the worst. Assume your adversaries are better than they are. Assume science and technology will soon be able to do things they cannot yet. Give yourself a margin for error. Give yourself more security than you need today. When the unexpected happens, you'll be glad you did."

Q3)

(i) \/~ @|<$> %:=-(#=© !|&)Δ =O~: \/~ *+∞◊ £=?
(ii) CRYPTOGRAPHY IS INTERESTING SOMETIMES

Q4) See attached solution in the Resources

Q5)

(i) I am aware of “BOOKKEEPER” (and if you ignore the hyphen you could have “SWEET-TOOTHED”) – can you think of any others?

(ii) I know “UNCOPYRIGHTABLE” – can you make anything better?

(iii) Over to you – what is the shortest you can create?