Section 3 Lecture 18 – One-time pad implementation Exercises

Q1) Encrypt the message “HELLOEVERYBODY” using the one-time pad keyword “FSADPMZAHEKDUG”.

Q2) In the example we did in the lecture, Alice sent the message “MEETMEATTHECAFETONIGHT”. That used Page 1 of our pad. Now, Bob wants to reply with “MEETTOMORROWINSTEAD”. Encrypt this using Page 2 of your pad, and then check that decrypting it works.

Q3) Decrypt the message “KPKNXNDFFDPICKJ” using the one-time pad keyword “RHYJSCVBNLBDCSQ”

Q4) Remember that the strength of the one-time pad is that an interceptor has no idea what the keyword is and guessing is no help because every combination of letters is equally likely. For example, if you try to crack the same message “NHYYSLWXBBJIWJMNTOEKQG” as we did before (the decryption of “MEETMEATTHECAFETONIGHT”), but guessing the keyword “FAYDOLJXMKBGIQYAHQXGQD”, you also get an English sentence. What is it? Create another keyword that also gives an English sentence.

Q5) Suppose you have intercepted the message “WDJJDLDDI”. Show that the keywords “SGHFSAZQP” and “DPQJSGDVX” both give rise to a sensible phrase. Create another keyword that also gives a sensible phrase.