Gauge Hartwell

5 January, 2021

CS427

Homework 1

1. C1 = 00110100 00111100 01100001 10110001 01100100
   C2 = 00110111 00111000 01100000 10101000 01100100

   Both ciphertexts end in the same character (01100100), which gives me a clue as to which pair of plaintexts (alpha & bravo or delta & gamma) C1 and C2 correspond to.

   delta as binary: 01100100 01100101 01101100 01110100 01100001
   gamma as binary: 01100111 01100001 01101101 01101101 01100001

   Delta and gamma end in the same character. I can find the key by performing an XOR operation on C1 and "Delta."

   00110100 00111100 01100001 10110001 01100100
   ⊕ 01100100 01100101 01101100 01110100 01100001
   = 01010000 01011001 00001101 11000101 00000101 == k

2. The flaw in the argument:
   "Consider the following attack against one-time pad: upon seeing a ciphertext c, the eavesdropper tries every candidate key $k \in \{0,1\}^{\lambda}$ until she has found the one that was used, at which point she outputs the plaintext m. This contradicts the argument in the book that the eavesdropper can obtain no information about m by seeing the ciphertext."

   Is that the eavesdropper does not know what the value of the plaintext is, and OTP does not impart any information about the plaintext to the eavesdropper. Thus, the eavesdropper has no way of knowing what the actual plaintext is that they are after (if their goal is to decrypt the correct message). If the eavesdropper simply tries every candidate key on the ciphertext, all they will accomplish is producing every possible plaintext that can be obtained with that ciphertext.

3. B = 011

M	M&B = C
000	000
001	001
010	010
011	011
100	000
101	001
110	010
111	011

With the bitwise AND operation, the only way for there to be a uniform distribution is for B to be 111. Otherwise, there is not a uniform distribution.