4a) j2tham

Let E and D be a simple transposition cipher

If k is 2 bits long (i.e , 10)

E and D are the same as they would both swap every pair of symbols in the message

Hence, E'(k,m) = D' (k,m) = m = E(k,D(k,m))

4b)

5a) j2tham

Complexity = 2^{16}

5b) have each of the 16 bits have one bit be 1 and the rest 0, in order (i.e 0000 0000 0000 0001, 0000 0000 0000 0010, ect)

Use these to figure out the permuations and subtitiutions for any cipher text

5c) No. It would still be vulnerable to the chosen plaintext attack as the overall size of inputs is the same

5d) No. It would still be vulnerable to the chosen plaintext attack as the overall size of inputs is the same

5e) Yes, the size of the chosen plaintext attacks would increase to 128

5f) Low permutation size and repeated keys, use only 1 time keys which are larger

Tools used:

Excel

Python

https://planetcalc.com/8047/

https://www.cryptool.org/en/cto/

https://www.boxentriq.com/code-breaking/vigenere-cipher

https://www.dcode.fr/transposition-cipher

https://planetcalc.com/3324/

Discussed with:
Min Htet, Sean, Louis