ComS 431
Homework 2

Sean Gordon

Sep 6, 2020

1. The algorithm itself is sound, and you would be able to verify that your friend has the same key. However, if anybody happened to intercept both yours and your friend's transmission, they would simply need to XOR the two strings to obtain the secret key.

2.

Key Length (bits)	Number of Keys	Attack Time (Years) (Worst case scenario)
56	2^{56}	Avg = 761, Corp = .0076
128	2^{128}	Avg = 3.6e24, Corp = 3.6e19
256	2^{256}	Avg = 1.2e63, Corp = 1.2e58
512	2^{512}	Avg = 1.4e140, Corp = 1.4e135

   (a) See table.

   (b)

      i. NewTime = OldTime / 1000

      ii. NewTime = OldTime / (keySize / 2)

   Comparing these two outcomes, the second option would eclipse the first once the keysize/2 reached 1000, or when the keysize became 2^{11}. This is the case with just the first key length, and thus we should choose the second option.