CPRE 431

Module 2 HW

Assignments will be submitted in PDF format via Canvas.

Please submit your homework online through Canvas. Late homework will not be accepted.
Important: Your submission must be in .pdf format ONLY!

1. Suppose that your friend suggests the following way to confirm that both of you have the same secret key. You create a random bit string which is having the length of the key, then, XOR it with the key, and send the result over the channel. Your partner XORs the incoming block with the key (which should be the same key) and sends the result back. If what you receive is your original string, you have verified that your partner has the same secret key, yet neither of you has ever transmitted the key on the channel. Is there a flaw in this scheme?

2. Fill in the table below, according to the following assumptions:

   Modern computers run approximately 3 billion compute cycles per second and with cloud computing, it is easily imaginable that a well-funded private organization can rent 100,000 such systems in the cloud. To test whether a given ciphertext decrypted with a key matches a known plaintext, takes approximately 1000 compute cycles.

Key Length (bits)	Number of Keys	Attack Time (Years) (Worst case scenario)
56		
128		
256		
512		

   a. Assuming that we have a block of ciphertext with known plaintext, indicate the time in years needed to test every possible key for each key length, in the case of:
      i. One modern computer.
      ii. A well-funded private organization as described above.
   b. Assume you were working on a research lab, and you were asked to find a solution to improve the cracking performance and time. Your team came up with two promising solutions.
      i. Use specialized hardware to increase the speed of such an attack by 1000 times.
      ii. Make cryptanalysis of the cipher to be able to guess half of the key bits at little cost.

      Explain with calculations which solution do you think would give better results?