Refo Yudhanto

CS350

HW 4

1. Get the baby ascii table and translate the cipher text;
   C = 47391112828 4663943684 5483262135
   Since we know what n is, we should find the private key which is d
   We could brute force to find p and q, and p = 242399 and q= 43481.
   Now we can find the d which is d*e = 1 mod phi thus we found is 3226366849
   Then lets find the phi which is 10539…
   Now we encode the C by taking C^D mod phi,
   C1 = GREAT!
   C2 = !XIXG
   C3 = OTIXT
   The secret word is found if you considered X as space which is GREAT! I GOT IT
2. We can do the Huffman algorithm using digits. And it works as follows:
   a. Create 10 nodes using first 10 data
   b. Attach as children of a new node that contains the sum of its children's frequencies.
   c. Add the node to a second list
   d. Do this until run out of nodes.
3. There is no perfect cryptographic protocol. It will just take time to crack a cryptographic protocol and understanding it. This has been done to any cracked cryptographic protocol ever created. This all based on the use of mathematics, since most cryptographic protocol is basically a mix of mathematics to make the code complex. Like how RSA was cracked. It was cracked by prime factorization and use Euclidean algorithm to crack the cipher text and expose the plain text. This shows that most encryption schemes rely on some sort of mathematical expression. Although using mathematics was not the only way to crack a cryptography protocol.

   There are also smarter way to crack a private key. One way is to make the private key obsolete and by just overflowing memory, which is usually found on a flawed systems. This happens with the PlayStation 3 security system. PS3 was called the most secure console until the deleted linux usage in their console. Hackers started to mess with the console to let them create homebrew code into the console. The whole process can be seen in https://www.youtube.com/watch?v=LuIlbmn-4A4. The video shows how they can crack the private key from privilege escalation.