Natnael Kebede

1. What are the disadvantages of symmetric cryptography?

The disadvantages of symmetric cryptography are problems associated with key exchange (the challenge of securely distributing keys across unsecured medium), and It is impossible to guarantee that no one will be able to tap communication channels. Origin and authenticity of messages can’t also be guaranteed since messages can’t be verified whom they came from. Furthermore, communication with multiple entities requires establishing distinct keys with each entity, which results in an increased total amount of keys needed for communication.

1. Explain how you were able to run a brute force attack and break the Caesar cipher. (Review Caesar5.py if needed)

I was able to run a brute force attack and break the Caesar cipher by using a python script (Caesar5.py) to try all the shift values from 0 to 25 to decipher the ciphertext that was input and then examining the output of the program for a readable plain text.

1. Discuss one of the problems that Whit Diffie was trying to solve.

Whitfield Diffie was trying to solve the problem with key distribution/exchange that was displayed by the existing methods of cryptography. He devised a way to implement modular arithmetic and one-way function which is easy to compute one way but very hard to reverse in order to develop a shared secret key agreement solution which allows securely distributing keys in an open (public) and vulnerable environment.

1. Examine the session keys you created this week's lab. What keys should be known, and which ones should be kept secret.

The sender’s and receiver’s secret key (Alice’s and Bob’s secret key) and the shared secret key they each compute should be kept private and secret by them. On the other hand, their public keys (Alice’s and Bob’s public key) should be known by each other and can be transmitted across the open communication medium that might be vulnerable to someone else listening.

1. Explain how Asymmetric Cryptography could make the use of Caesar cipher stronger.

Asymmetric Cryptography could make the use of Caesar cipher stronger in the following way. First, the receiver sends its public key to the sender. Second, using the receiver’s public key, the sender encrypts the ciphertext that is produced and the shift value that was input to create the ciphertext using Caesar cipher and sends both to the receiver. Then, the receiver can decrypt the message to get the original ciphertext and shift value used by the sender to encrypt. The receiver then uses that shift value to reverse the ciphertext (decrypt) and obtain the plain text message.