Sean Poston
4/28/2020

Homework - Intro to Cryptography
Total = 40 points

1. **(15 points)** List the mathematical function for encryption and decryption for the following:
   a. Caesar Cipher
      - newChar = (char + k) % 26
      - char = (newChar – k) % 26

   b. Asymmetric Encryption
      - ?

   c. RSA encryption
      - $c = m^e \bmod n, m < n$
      - $m = c^d \bmod n$

   d. "One Time Pad" cipher
      - encrypt(key, text) = key XOR text
      - decrypt(key, text) = key XOR text

2. **(5 points)** What is the number of possible combinations of keys for brute force attack for the following key sizes?
    a. 1 bit
        - $2^1 = 2$
    b. 2 bits
        - $2^2 = 4$
    c. 1 byte
        - $2^8 = 256$
    d. 2 bytes
        - $2^{16} = 65536$

3. **(5 points)** What is the predicted encrypted output for the following?

Cipher type	Plaintext	Key
Caesar Cipher	Happy Birthday	k = 3
"One Time Pad" cipher	1011 1101	0101 1100

- **Caesar**: Kdssb Eluwkgd (or Kdssb#Eluwkgd if you count the space)
- **One Time Pad**: 1110 0001

4. **(5 points)** Draw the block diagram and explain symmetric and asymmetric encryption.
   - Symmetric encryption requires both the sender and receiver to know the secret key.
   - Asymmetric encryption does not require sender and receiver to share the key. There is a public encryption key that is known to all, but also a private decryption key that's known only to the receiver.

     PK = public key, R = Receiver, S = Sender, txt = plaintext, xtt = ciphertext

Asym.

1 R $\xrightarrow[\text{PK}]{}$ S

2 txt → PK → xtt

3 S $\xrightarrow[\text{xtt}]{}$ R

4 xtt $\xrightarrow[\text{priv. Key}]{}$ txt

Sym.

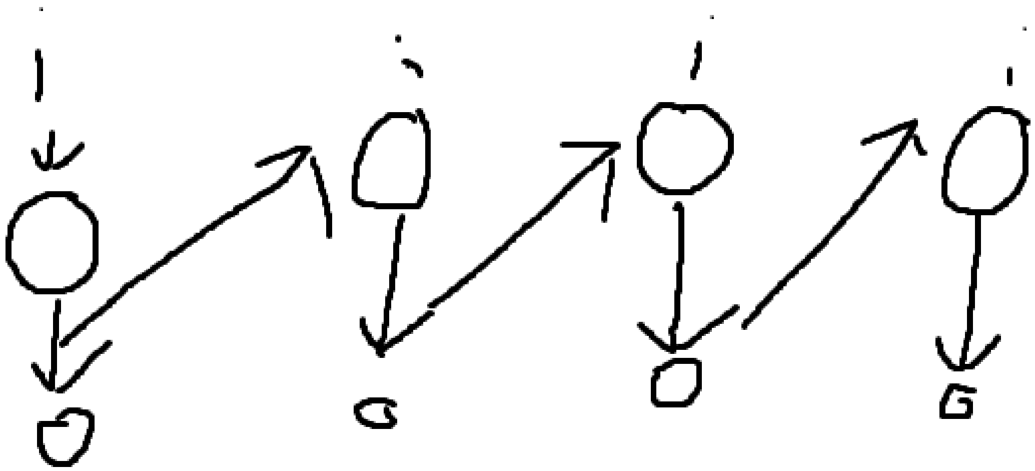
1 txt → xtt

2 S $\xrightarrow{\text{key}}$ R

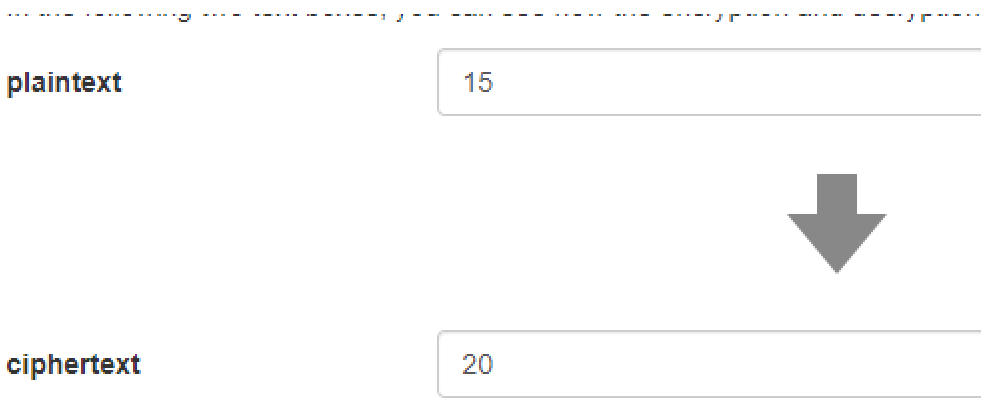
S $\xrightarrow{\text{xtt}}$ R

3 xtt $\xrightarrow{\text{key}}$ txt

5. **(5 points)** Explain the motivation for block chaining in encryption. Draw the block diagram and explain the different components in Cipher Block Chaining.
    - Block chaining keeps the same text from being encrypted as the as the same thing multiple times. This keeps the encryption harder to crack. The final block's output will be influenced by the entire input of the whole chain.



6. **(5 points)** Using RSA with the two given prime numbers (p = 5, q = 11) and public key = 13, find out the ciphertext for the plaintext as 15 and 25
Use the following link to solve this question: https://www.cryptool.org/en/cto-highlights/rsa-step-by-step
Also, enclose the screenshots for your output for plaintext = 15.



plaintext 15

ciphertext 20