

PROGRAMMING ASSIGNMENT 2 DOCUMENTATION

Submitted By:- Amal Majeed Mucheth Abdulmajeed
200415928

This program was written in **Python** programming language to be executed with python interpreter version **2.7**. The aim of the program is to implement a sender and receiver interface that communicates a message that is encrypted with RC4 stream encryption and a common 128 bit key. Utilising the two functions PRGA and inverse PRGA(IPRGA) implemented in programming assignment 1 , the receiver should be able to navigate to the appropriate RC4 state for decryption regardless of the order of receiving the encrypted sequences from the sender. We will be testing for a message of length around 1000 bytes , so we test out the 4 packets transmission using the 3 cases below:-

- 1) 0,1,2,3
- 2) 1,0,3,2
- 3) 3,2,1,0

Implementation/ Input parameters

***Note** :- In python , an array is called a list and can add any data type of values to it even other lists .

The function **key_schedule** takes in 2 arguments :

Purpose :- To generate a random 256 encryption stream from a common 128 bit key that sender and receiver only knows

- 1) S (int list) : - the 256 bit random stream array used for encryption,
- 2) T (int list) - 8 bit index pointer for swapping procedure to further randomise the array S

The function **PRGA** takes in 4 arguments :

Purpose :- To shuffle the 256 random array forward to obtain next RC4 state for encryption

- 3) S (int list) : - the 256 bit random stream array used for encryption generated by the **key_schedule** function using a 128 bit key shared by sender and receiver.
- 4) i (int) - 8 bit index pointer for swapping procedure to further randomise the array S
- 5) j (int) - 8 bit index pointer for swapping procedure to further randomise the array S
- 6) n (int) - number of times the PRGA algorithm has to be applied on RC4 state

The function **IPRGA** takes in 4 arguments :

Purpose :- To undo the effect of PRGA on random 256 array to obtain previous RC4 state

- 7) S (int list): - the 256 bit random stream array used for encryption generated by the **key_schedule** function using a 128 bit key shared by sender and receiver.
- 8) i (int) - 8 bit index pointer value at the end of n steps of PRGA on S
- 9) j (int) - 8 bit index pointer value at the end of n steps of PRGA on S
- 10) n (int) - number of times the IPRGA algorithm has to be applied on RC4 state.

The function **hash_gen** takes in 1 argument :

Purpose :- To generate 16 byte hash value from the message data and sequence counter

- 11) S (string) :- the string (data + sequence no) being used to generate the hash value using python **hashlib** module's **md5** function.

The function **hash_prep** takes 2 arguments :

Purpose :- To convert the sequence counter to 4 byte string and attach with message to generate the hash

- 12) data (string) :- the message string used along with sequence no to generate the hash value
13) seq (int) :- the sequence counter value which is attached to the data string to generate the hash value.

The function **enc_dec** takes 2 arguments :

Purpose :- To XOR the plaintext/ciphertext ASCII value with corresponding S array value.

- 14) data (int) :- the ASCII value of the character/message byte being encrypted
15) key (int) :- the encryption key number from the random 256 byte array generated with the 128 bit key.

The function **message_split** takes 2 arguments :

Purpose :- To split the full message to chunks/packets of size 252 bytes and assign them a counter value and calculate the hash

- 16) m (string) :- the complete message the sender wants to send to the receiver
17) size (int) :- the length of the complete message in bytes

The function **sender_logic** takes 2 arguments :

Purpose :- To encrypt the message packets along with the hash and send the packets to receiver

- 18) m (string) :- the complete message the sender wants to send to the receiver
19) S_sen (int list) :- sender's copy of the random 256 byte encryption array generated from the secret 128 bit key.

The function **receiver_logic** takes 3 arguments :

Purpose :- To decrypt the packets of ciphertext from the sender and if packets are out of order , use PRGA and IPRGA to obtain the correct S state to decrypt the packets and verify the hash value

- 20) seq_list (int list) :- list containing the order in which the receiver receives the packets of ciphertext
21) enc_list (dictionary list) :- encrypted list of data packets as a python dictionary , where each dictionary element has a "sequence" counter value , "enc_arr" array of ciphertext ASCII values and "enc_result" the ciphertext string.
22) S_rec (int list) :- receiver's copy of the random 256 byte encryption array generated from the secret 128 bit key.

Working

The program initially prompts the user to enter a 128 bit random string as key(i.e 16 ASCII characters) . If the key entered is not long enough or longer than 128 bits/16 bytes the programs asks the user to re-enter a valid one as shown below

```
Programming Assignment 2

Enter a random 128 bit key:n8asn219end
Key length was not 128 bits ! try another key:nas8e621b90xu27f
Enter your message here:
```

Once a valid key has been entered , we can enter the message as shown below

```
Programming Assignment 2

Enter a random 128 bit key:nas8e621b90xu27f
Enter your message here:People often install a kitty door, only to discover that they have a problem. The p
roblem is their cat will not use the kitty door. There are several common reasons why cats won't use kitty
doors. First, they may not understand how a kitty door works. They may not understand that it is a little d
oorway just for them. Second, many kitty doors are dark, and cats cannot see to the other side. As such, th
ey can't be sure of what is on the other side of the door, so they won't take the risk. One last reason cat
s won't use kitty doors is because some cats don't like the feeling of pushing through the door and having
the door drag across their back. But don't worry--there is a solution for this kitty-door problem.The first
step in solving the problem is to prop the door open with tape. This means your cat will now be able to see
through to the other side; your cat will likely begin using the kitty door immediately. Once your cat has
gotten used to using the kitty door, remove the tape.
Message Length 1006
```

The message length will be shown . The message is to be divided to packets of length 252 bytes, if the last byte is shorter , then padding is done with a '1' followed by trailing '0's till the packet is 252 bytes long.After the split , the list of data packets along with generated hash values and sequence counter values will be encapsulated as a python dictionary with key-value mappings .

```

The last block contains : 250

After padding the message block :
The problem is to prop the door open with tape. This means your cat will now be able to see through to the other side; your cat will likely begin using the kitty door immediately. Once your cat has gotten used to using the kitty door, remove the tape.10

The list of data packets :
[{'hash': 'e400bbbed6056c43e', 'data': 'People often install a kitty door, only to discover that they have a problem. The problem is their cat will not use the kitty door. There are several common reasons why cats won\'t use kitty doors. First, they may not understand how a kitty door works', 'sequence': 0}, {'hash': '8097950e27095f3b', 'data': '. They may not understand that it is a little doorway just for them. Second, many kitty doors are dark, and cats cannot see to the other side. As such, they can\'t be sure of what is on the other side of the door, so they won\'t take the risk. One la', 'sequence': 1}, {'hash': '352fb6a071f8235d', 'data': 'st reason cats won\'t use kitty doors is because some cats don\'t like the feeling of pushing through the door and having the door drag across their back. But don\'t worry there is a solution for this kitty-door problem.The first step in solving t', 'sequence': 2}, {'hash': '706f6df4cdbf0db1', 'data': 'he problem is to prop the door open with tape. This means your cat will now be able to see through to the other side; your cat will likely begin using the kitty door immediately. Once your cat has gotten used to using the kitty door, remove the tape.10', 'sequence': 3}]

```

Then the encryption portion of the code in the sender_logic function starts to work, each dictionary element or data packet in the above list will be looped over one by one in sequence order and for each character/byte of the data(252 bytes) + hash (16 bytes) , the PRGA algorithm shuffles the random 256 bit array 'S' and encrypts the entire packet byte by byte with corresponding 'S' array element and the PRGA keeps shuffling it after each character or byte. The string being encrypted is **data + hash value** .

```

Encryption Begins Here

Plaintext being encrypted (data + hash (last 16 bytes)) :
People often install a kitty door, only to discover that they have a problem. The problem is their cat will not use the kitty door. There are several common reasons why cats won't use kitty doors. First, they may not understand how a kitty door works400bb6d6056c43e

Corresponding input ASCII array :
[80, 101, 111, 112, 108, 101, 32, 111, 102, 116, 101, 110, 32, 105, 110, 115, 116, 97, 108, 108, 32, 97, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 44, 32, 111, 110, 108, 121, 32, 116, 111, 32, 100, 105, 115, 99, 111, 118, 101, 114, 32, 116, 104, 97, 116, 32, 116, 104, 101, 121, 32, 104, 97, 118, 101, 32, 97, 32, 112, 114, 111, 98, 108, 101, 109, 46, 32, 84, 104, 101, 32, 112, 114, 111, 98, 108, 101, 109, 32, 105, 115, 32, 116, 104, 101, 105, 114, 32, 99, 97, 116, 32, 119, 105, 108, 108, 32, 110, 111, 116, 32, 117, 115, 101, 32, 116, 104, 101, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 46, 32, 84, 104, 101, 114, 101, 32, 97, 114, 101, 32, 115, 101, 118, 101, 114, 97, 108, 32, 99, 111, 109, 109, 111, 110, 32, 114, 101, 97, 115, 111, 110, 115, 32, 119, 104, 121, 32, 99, 97, 116, 115, 32, 119, 111, 110, 226, 128, 153, 116, 32, 117, 115, 101, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 115, 46, 32, 70, 105, 114, 115, 116, 44, 32, 116, 104, 101, 121, 32, 109, 97, 121, 32, 110, 111, 116, 32, 117, 110, 100, 101, 114, 115, 116, 97, 110, 100, 32, 104, 111, 119, 32, 97, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 32, 119, 111, 114, 107, 115, 101, 52, 48, 48, 98, 98, 101, 100, 54, 48, 53, 54, 99, 52, 51, 101]

Plaintext being encrypted (data + hash (last 16 bytes)) :
. They may not understand that it is a little doorway just for them. Second, many kitty doors are dark, and cats cannot see to the other side. As such, they can't be sure of what is on the other side of the door, so they won't take the risk. One 1a8097950e27095f3b

Corresponding input ASCII array :
[46, 32, 84, 104, 101, 121, 32, 109, 97, 121, 32, 110, 111, 116, 32, 117, 110, 100, 101, 114, 115, 116, 97, 110, 100, 32, 116, 104, 97, 116, 32, 105, 116, 32, 105, 115, 32, 97, 32, 108, 105, 116, 116, 108, 101, 32, 100, 111, 111, 114, 119, 97, 121, 32, 106, 117, 115, 116, 32, 102, 111, 114, 32, 116, 104, 101, 109, 46, 32, 83, 101, 99, 111, 110, 100, 44, 32, 109, 97, 110, 121, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 115, 32, 97, 114, 101, 32, 100, 97, 114, 107, 44, 32, 97, 110, 100, 32, 99, 97, 116, 115, 32, 99, 97, 110, 110, 111, 116, 32, 115, 101, 101, 32, 116, 111, 32, 116, 104, 101, 32, 111, 116, 104, 101, 114, 32, 115, 105, 100, 101, 46, 32, 65, 115, 32, 115, 117, 99, 104, 44, 32, 116, 104, 101, 121, 32, 99, 97, 110, 226, 128, 153, 116, 32, 98, 101, 32, 115, 117, 114, 101, 32, 111, 102, 32, 119, 104, 97, 116, 32, 105, 115, 32, 111, 110, 32, 116, 104, 101, 32, 111, 116, 104, 101, 114, 32, 115, 105, 100, 101, 32, 111, 102, 32, 116, 104, 101, 32, 100, 111, 111, 114, 44, 32, 115, 111, 32, 116, 104, 101, 121, 32, 119, 111, 110, 226, 128, 153, 116, 32, 116, 97, 107, 101, 32, 116, 104, 101, 32, 114, 105, 115, 107, 46, 32, 79, 110, 101, 32, 108, 97, 56, 48, 57, 55, 57, 53, 48, 101, 50, 55, 48, 57, 53, 102, 51, 98]

```

Two examples of the data strings being encrypted (data+hash) along with their corresponding ASCII array used for encryption is shown above. These ASCII input array values are XOR'ed with corresponding random values from the 'S' array which is shuffled after every XOR operation/encryption to ensure maximum randomness. After encryption the ciphertext packets are formed as dictionary elements with "enc_arr" which is the resultant ciphertext ASCII after the XOR, "enc_result" which is the ciphertext string obtained from the ciphertext ASCII array and "sequence" which is the sequence number of the data packet being encrypted using the 'S' array to get the "enc_result".

The final encrypted packet list will be displayed as shown in the next page :

Encryption Ends Here

When the decryption begins, the receiver displays the counter value the sender gave and the ciphertext. The receiver next checks it with its own counter value and if the received packet is ahead of its counter value, then the receiver uses **PRGA** algorithm for the necessary number of steps to advance its array state 'S' to match with the one for that received packet, else if the received packet is behind its counter value, then the receiver uses **IPRGA** algorithm for the necessary number of steps to trace back its array state 'S' to match with the one for that received packet. After decryption receiver increments its counter by one.

```

CASE 1 : Sequence order 0 -> 1 -> 2 -> 3

Decryption Begins Here

Counter value of next piece of ciphertext sent by sender : 0

Ciphertext being decrypted :
=??T?>fg?]]??k???7/V&a}??uQ?90??p??A\<????{?M?x? ?v/????2?????]?#g0%=%m??pTGm??|5?XK4]?h?A???dB?xo2?:^? [??d???????;????6?$
?? ??0???E?δ?@?6riu/?..??3???Y???l?zk??j3N?4V#i?/Ba\?
pd??S>/wHY?^2?S?-?I*
}??f

Decryption array after XOR with corresponding key value :
[80, 101, 111, 112, 108, 101, 32, 111, 102, 116, 101, 110, 32, 105, 110, 115, 116, 97, 108, 108, 32, 97, 32, 107, 105, 116, 11
6, 121, 32, 100, 111, 111, 114, 44, 32, 111, 110, 108, 121, 32, 116, 111, 32, 100, 105, 115, 99, 111, 118, 101, 114, 32, 116,
104, 97, 116, 32, 116, 104, 101, 121, 32, 104, 97, 118, 101, 32, 97, 32, 112, 114, 111, 98, 108, 101, 109, 46, 32, 84, 104, 10
1, 32, 112, 114, 111, 98, 108, 101, 109, 32, 105, 115, 32, 116, 104, 101, 105, 114, 32, 99, 97, 116, 32, 119, 105, 108, 108, 3
2, 110, 111, 116, 32, 117, 115, 101, 32, 116, 104, 101, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 46, 32, 84, 104,
101, 114, 101, 32, 97, 114, 101, 32, 115, 101, 118, 101, 114, 97, 108, 32, 99, 111, 109, 109, 111, 110, 32, 114, 101, 97, 115,
111, 110, 115, 32, 119, 104, 121, 32, 99, 97, 116, 115, 32, 119, 111, 110, 226, 128, 153, 116, 32, 117, 115, 101, 32, 107, 10
5, 116, 116, 121, 32, 100, 111, 111, 114, 115, 46, 32, 70, 105, 114, 115, 116, 44, 32, 116, 104, 101, 121, 32, 109, 97, 121, 3
2, 110, 111, 116, 32, 117, 110, 100, 101, 114, 115, 116, 97, 110, 100, 32, 104, 111, 119, 32, 97, 32, 107, 105, 116, 116, 121,
32, 100, 111, 111, 114, 32, 119, 111, 114, 107, 115, 101, 52, 48, 48, 98, 98, 101, 100, 54, 48, 53, 54, 99, 52, 51, 101]

Plaintext obtained (without the hash) after decryption from the XOR'd decryption array :
People often install a kitty door, only to discover that they have a problem. The problem is their cat will not use the kitty
door. There are several common reasons why cats won't use kitty doors. First, they may not understand how a kitty door works

Receiver manually generating hash value of decrypted plaintext obtained : e400bbbed6056c43e

Receiver Comparing generated hash with hash attached inside ciphertext given by sender !

The hash values match !

Expected next value of counter : 1

```

After the receiver receives a packet it decrypts it obtains the plaintext from the ciphertext after applying the necessary number of PRGA or IPRGA iterations. Then the receiver again generates the hash of the decrypted data string and compares it with the hash sent by the sender embedded in the ciphertext to verify that data has not been tampered with. If hashes match , it means data has not been modified as shown above..

```

Decryption Ends Here

THE FINAL PLAINTEXT RECEIVED BY RECEIVER AFTER RE-ORDERING (Along with padding of last block)
:

People often install a kitty door, only to discover that they have a problem. The problem is their cat will not use the kitty
door. There are several common reasons why cats won't use kitty doors. First, they may not understand how a kitty door works.
They may not understand that it is a little doorway just for them. Second, many kitty doors are dark, and cats cannot see to t
he other side. As such, they can't be sure of what is on the other side of the door, so they won't take the risk. One last rea
son cats won't use kitty doors is because some cats don't like the feeling of pushing through the door and having the door dra
g across their back. But don't worry-there is a solution for this kitty-door problem.The first step in solving the problem is
to prop the door open with tape. This means your cat will now be able to see through to the other side; your cat will likely b
egin using the kitty door immediately. Once your cat has gotten used to using the kitty door, remove the tape.10

```

Finally after the last packet in the sequence has been decrypted , the receiver puts together the entire plaintext pieces back in order to get back the original plaintext message the sender wanted to send the

receiver. The above snapshots show for case 1 , where the packets are sent in order 0,1,2,3. Similar are the cases for the other 2 cases

CASE 2 : 1,0,3,2

Snapshots

```
CASE 2 : Sequence order 1 -> 0 -> 3 -> 2

Decryption Begins Here

Counter value of next piece of ciphertext sent by sender : 1

Ciphertext being decrypted :
'?c???d?/gtjQ\???#?m?+I??W????xE?KXMH   u???=?ôd??n?2JU
                                           ? :Ek?Hjn?
                                           ?za?2Pp/I????_=
                                           o)??

???B???
    Jzx????
??59?=[?N?e??2?Wl??h?>??p?o??<aC????vChu?A$?/V????y?h?M\??Z0??z?Gs?QwL??A?)?N??C?G???9y?R8

Decryption array after XOR with corresponding key value :
[46, 32, 84, 104, 101, 121, 32, 109, 97, 121, 32, 110, 111, 116, 32, 117, 110, 100, 101, 114, 115, 116, 97, 110, 100, 32, 116, 104
, 97, 116, 32, 105, 116, 32, 105, 115, 32, 97, 32, 108, 105, 116, 116, 108, 101, 32, 100, 111, 111, 114, 119, 97, 121, 32, 106, 11
7, 115, 116, 32, 102, 111, 114, 32, 116, 104, 101, 109, 46, 32, 83, 101, 99, 111, 110, 100, 44, 32, 109, 97, 110, 121, 32, 107, 10
5, 116, 116, 121, 32, 100, 111, 111, 114, 115, 32, 97, 114, 101, 32, 100, 97, 114, 107, 44, 32, 97, 110, 100, 32, 99, 97, 116, 115
, 32, 99, 97, 110, 110, 111, 116, 32, 115, 101, 101, 32, 116, 111, 32, 116, 104, 101, 32, 111, 116, 104, 101, 114, 32, 115, 105, 1
00, 101, 46, 32, 65, 115, 32, 115, 117, 99, 104, 44, 32, 116, 104, 101, 121, 32, 99, 97, 110, 226, 128, 153, 116, 32, 98, 101, 32,
115, 117, 114, 101, 32, 111, 102, 32, 119, 104, 97, 116, 32, 105, 115, 32, 111, 110, 32, 116, 104, 101, 32, 111, 116, 104, 101, 1
14, 32, 115, 105, 100, 101, 32, 111, 102, 32, 116, 104, 101, 32, 100, 111, 111, 114, 44, 32, 115, 111, 32, 116, 104, 101, 121, 32,
119, 111, 110, 226, 128, 153, 116, 32, 116, 97, 107, 101, 32, 116, 104, 101, 32, 114, 105, 115, 107, 46, 32, 79, 110, 101, 32, 10
8, 97, 56, 48, 57, 55, 57, 53, 48, 101, 50, 55, 48, 57, 53, 102, 51, 98]

Plaintext obtained (without the hash) after decryption from the XOR'd decryption array :
. They may not understand that it is a little doorway just for them. Second, many kitty doors are dark, and cats cannot see to the
other side. As such, they can't be sure of what is on the other side of the door, so they won't take the risk. One la

Receiver manually generating hash value of decrypted plaintext obtained : 8097950e27095f3b

Receiver Comparing generated hash with hash attached inside ciphertext given by sender !

The hash values match !

Expected next value of counter : 2

Counter value of next piece of ciphertext sent by sender : 0

Ciphertext being decrypted :
=???T?>fg?]????k???7/V&a)??uQ?90??p??A\<????{?M?x? ?v/????2??????}#g0%=%?m??pTGm??|5?XK4]?h?A???dB?xo2???^?[[?d???????;????6?$$$?
??0???E?d?@?6riu/?..??3???Y???L?zk??j3N?4V#l?/Ba\?
pd??S>/wHY?^2?S?-?I*                                }?f
```



```
Decryption array after XOR with corresponding key value :
[80, 101, 111, 112, 108, 101, 32, 111, 102, 116, 101, 110, 32, 105, 110, 115, 116, 97, 108, 108, 32, 97, 32, 107, 105, 116, 116, 1
21, 32, 100, 111, 111, 114, 44, 32, 111, 110, 108, 121, 32, 116, 111, 32, 100, 105, 115, 99, 111, 118, 101, 114, 32, 116, 104, 97,
116, 32, 116, 104, 101, 121, 32, 104, 97, 118, 101, 32, 97, 32, 112, 114, 111, 98, 108, 101, 109, 46, 32, 84, 104, 101, 32, 112,
114, 111, 98, 108, 101, 109, 32, 105, 115, 32, 116, 104, 101, 105, 114, 32, 99, 97, 116, 32, 119, 105, 108, 108, 32, 110, 111, 116
, 32, 117, 115, 101, 32, 116, 104, 101, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 46, 32, 84, 104, 101, 114, 101, 32, 9
7, 114, 101, 32, 115, 101, 118, 101, 114, 97, 108, 32, 99, 111, 109, 109, 111, 110, 32, 114, 101, 97, 115, 111, 110, 115, 32, 119,
104, 121, 32, 99, 97, 116, 115, 32, 119, 111, 110, 226, 128, 153, 116, 32, 117, 115, 101, 32, 107, 105, 116, 116, 121, 32, 100, 1
1, 111, 114, 115, 46, 32, 70, 105, 114, 115, 116, 44, 32, 116, 104, 101, 121, 32, 109, 97, 121, 32, 110, 111, 116, 32, 117, 110,
100, 101, 114, 115, 116, 97, 110, 100, 32, 104, 111, 119, 32, 97, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 32, 119, 11
1, 114, 107, 115, 101, 52, 48, 48, 98, 98, 101, 100, 54, 48, 53, 54, 99, 52, 51, 101]
```

Plaintext obtained (without the hash) after decryption from the XOR'ed decryption array :
People often install a kitty door, only to discover that they have a problem. The problem is their cat will not use the kitty door
. There are several common reasons why cats won't use kitty doors. First, they may not understand how a kitty door works

Receiver manually generating hash value of decrypted plaintext obtained : e400bbcd6056c43e

Receiver Comparing generated hash with hash attached inside ciphertext given by sender !

The hash values match !

Expected next value of counter : 1

Counter value of next piece of ciphertext sent by sender : 3

Ciphertext being decrypted :
p?z??9Pú.???Rx3?+eW??Q??^???K?9?s????-y&^?E?AiAo?+e?d????,?0=k???달?S?9?3??B??K0H?Y????E
?SQ?? ??T?
?M?=? ???H??b??b????NM"b??k??rn??M?? ?L????W??LBa??D?<?::???Bf`*?.?f?¿(k?2???n??J???X?C??l?M?&Q\$~???'h? [?v;?
?Y????%?

```
Decryption array after XOR with corresponding key value :
[104, 101, 32, 112, 114, 111, 98, 108, 101, 109, 32, 105, 115, 32, 116, 111, 32, 112, 114, 111, 112, 32, 116, 104, 101, 32, 100, 1
11, 111, 114, 32, 111, 112, 101, 110, 32, 119, 105, 116, 104, 32, 116, 97, 112, 101, 46, 32, 84, 104, 105, 115, 32, 109, 101, 97,
110, 115, 32, 121, 111, 117, 114, 32, 99, 97, 116, 32, 119, 105, 108, 108, 32, 110, 111, 119, 32, 98, 101, 32, 97, 98, 108, 101, 3
2, 116, 111, 32, 115, 101, 101, 32, 116, 104, 114, 111, 117, 103, 104, 32, 116, 111, 32, 116, 104, 101, 32, 111, 116, 104, 101, 11
4, 32, 115, 105, 100, 101, 59, 32, 121, 111, 117, 114, 32, 99, 97, 116, 32, 119, 105, 108, 108, 32, 108, 105, 107, 101, 108, 121,
32, 98, 101, 103, 105, 110, 32, 117, 115, 105, 110, 103, 32, 116, 104, 101, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 3
2, 105, 109, 109, 101, 100, 105, 97, 116, 101, 108, 121, 46, 32, 79, 110, 99, 101, 32, 121, 111, 117, 114, 32, 99, 97, 116, 32, 10
4, 97, 115, 32, 103, 111, 116, 116, 101, 110, 32, 117, 115, 101, 100, 32, 116, 111, 32, 117, 115, 105, 110, 103, 32, 116, 104, 101
, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 44, 32, 114, 101, 109, 111, 118, 101, 32, 116, 104, 101, 32, 116, 97, 112,
101, 46, 49, 48, 55, 48, 54, 102, 54, 100, 102, 52, 99, 100, 98, 102, 48, 100, 98, 49]
```

Plaintext obtained (without the hash) after decryption from the XOR'ed decryption array :
he problem is to prop the door open with tape. This means your cat will now be able to see through to the other side; your cat wil
l likely begin using the kitty door immediately. Once your cat has gotten used to using the kitty door, remove the tape.10

Receiver manually generating hash value of decrypted plaintext obtained : 706f6df4cdbf0db1

Receiver Comparing generated hash with hash attached inside ciphertext given by sender !

The hash values match !

Counter value of next piece of ciphertext sent by sender : 2

Ciphertext being decrypted :

????s?Lh?i????xVQ???G%??LC?;??U?? ȳ????YQ(???X.??8???/I?Taf???e?? J?f(r??o?

?s?n???A???oX?,??(#x?J????1S?nHjv1?tMb?"I4?1V'??E??.??@M?U??1?d??)}zh???8??0W?][??_9??????#????*|J???W/?9?
^i?.0??C?.

v???n5??

p??[A?\??0

Decryption array after XOR with corresponding key value :

[115, 116, 32, 114, 101, 97, 115, 111, 110, 32, 99, 97, 116, 115, 32, 119, 111, 110, 226, 128, 153, 116, 32, 117, 115, 101, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 115, 32, 105, 115, 32, 98, 101, 99, 97, 117, 115, 101, 32, 115, 111, 109, 101, 32, 99, 97, 116, 115, 32, 100, 111, 110, 226, 128, 153, 116, 32, 108, 105, 107, 101, 32, 116, 104, 101, 32, 102, 101, 101, 108, 105, 110, 103, 32, 111, 102, 32, 112, 117, 115, 104, 105, 110, 103, 32, 116, 104, 114, 111, 117, 103, 104, 32, 116, 104, 101, 32, 100, 111, 111, 114, 32, 97, 110, 100, 32, 104, 97, 118, 105, 110, 103, 32, 116, 104, 101, 32, 100, 111, 111, 114, 32, 100, 114, 97, 103, 32, 97, 99, 114, 111, 115, 115, 32, 116, 104, 101, 105, 114, 32, 98, 97, 99, 107, 46, 32, 66, 117, 116, 32, 100, 111, 110, 226, 128, 153, 116, 32, 119, 111, 114, 114, 121, 226, 128, 148, 116, 104, 101, 114, 101, 32, 105, 115, 32, 97, 32, 115, 111, 108, 117, 116, 105, 111, 110, 32, 102, 111, 114, 32, 116, 104, 105, 115, 32, 107, 105, 116, 116, 121, 45, 100, 111, 111, 114, 32, 112, 114, 111, 98, 108, 101, 109, 46, 84, 104, 101, 32, 102, 105, 114, 115, 116, 32, 115, 116, 101, 112, 32, 105, 110, 32, 115, 111, 108, 118, 105, 110, 103, 32, 116, 51, 53, 50, 102, 98, 54, 97, 48, 55, 49, 102, 56, 50, 51, 53, 100]

Plaintext obtained (without the hash) after decryption from the XOR'ed decryption array :

st reason cats won't use kitty doors is because some cats don't like the feeling of pushing through the door and having the door drag across their back. But don't worry--there is a solution for this kitty-door problem.The first step in solving t

Receiver manually generating hash value of decrypted plaintext obtained : 352fb6a071f8235d

Receiver Comparing generated hash with hash attached inside ciphertext given by sender !

The hash values match !

Expected next value of counter : 3

Decryption Ends Here

THE FINAL PLAINTEXT RECEIVED BY RECEIVER AFTER RE-ORDERING (Along with padding of last block) :

People often install a kitty door, only to discover that they have a problem. The problem is their cat will not use the kitty door . There are several common reasons why cats won't use kitty doors. First, they may not understand how a kitty door works. They may not understand that it is a little doorway just for them. Second, many kitty doors are dark, and cats cannot see to the other side. As such, they can't be sure of what is on the other side of the door, so they won't take the risk. One last reason cats won't use kitty doors is because some cats don't like the feeling of pushing through the door and having the door drag across their back. But don't worry--there is a solution for this kitty-door problem.The first step in solving the problem is to prop the door open with tape. This means your cat will now be able to see through to the other side; your cat will likely begin using the kitty door immediately. Once your cat has gotten used to using the kitty door, remove the tape.10

CASE 3 : 3,2,1,0

Snapshots

```
CASE 3 : Sequence order 3 -> 2 -> 1 -> 0

Decryption Begins Here

Counter value of next piece of ciphertext sent by sender : 3

Ciphertext being decrypted :
p?z???lPú.???Rx3?+e?W??Q???^???K?9?s????-y&^?E?ÅiAo?+e?d=???,?0=k???달?S?9?3???b???KôH?Y????E
?SQ?? ??T?
?M?=? ???H?b?>????NM"b??k?rn???M?? ?l?????W??lB,??D?<?:???l???Bf`*?.?f,?(k?2???n??J???X?C??l?M?&Q$~???'h?[?v;?
?Y?????%?

Decryption array after XOR with corresponding key value :
[104, 101, 32, 112, 114, 111, 98, 108, 101, 109, 32, 105, 115, 32, 116, 111, 32, 112, 114, 111, 112, 32, 116, 104, 101, 32, 100, 1
11, 111, 114, 32, 111, 112, 101, 110, 32, 119, 105, 116, 104, 32, 116, 97, 112, 101, 46, 32, 84, 104, 105, 115, 32, 109, 101, 97,
110, 115, 32, 121, 111, 117, 114, 32, 99, 97, 116, 32, 119, 105, 108, 108, 32, 110, 111, 119, 32, 98, 101, 32, 97, 98, 108, 101, 3
2, 116, 111, 32, 115, 101, 101, 32, 116, 104, 114, 111, 117, 103, 104, 32, 116, 111, 32, 116, 104, 101, 32, 111, 116, 104, 101, 11
4, 32, 115, 105, 100, 101, 59, 32, 121, 111, 117, 114, 32, 99, 97, 116, 32, 119, 105, 108, 108, 32, 108, 105, 107, 101, 108, 121,
32, 98, 101, 103, 105, 110, 32, 117, 115, 105, 110, 103, 32, 116, 104, 101, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 3
2, 105, 109, 109, 101, 100, 105, 97, 116, 101, 108, 121, 46, 32, 79, 110, 99, 101, 32, 121, 111, 117, 114, 32, 99, 97, 116, 32, 10
4, 97, 115, 32, 103, 111, 116, 116, 101, 110, 32, 117, 115, 101, 100, 32, 116, 111, 32, 117, 115, 105, 110, 103, 32, 116, 104, 101
, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 44, 32, 114, 101, 109, 111, 118, 101, 32, 116, 104, 101, 32, 116, 97, 112,
101, 46, 49, 48, 55, 48, 54, 102, 54, 100, 102, 52, 99, 100, 98, 102, 48, 100, 98, 49]

Plaintext obtained (without the hash) after decryption from the XOR'ed decryption array :
he problem is to prop the door open with tape. This means your cat will now be able to see through to the other side; your cat wil
l likely begin using the kitty door immediately. Once your cat has gotten used to using the kitty door, remove the tape.10

Receiver manually generating hash value of decrypted plaintext obtained : 706f6df4cdbf0db1

Receiver Comparing generated hash with hash attached inside ciphertext given by sender !

The hash values match !

Counter value of next piece of ciphertext sent by sender : 2

Ciphertext being decrypted :
????s?Lh?i????xY0????Gx??LC?;?U?? w????Y0(???X.???8????/I?Taf???e?? J?f(r???o?

?s?n???A????oX?,??(#x?J????LS?nJvL?tMb?"I4?1V'??E??..??@M?U??1?d??))zh????8??0W?]??_9???????#????*|J???W/?9?
^i?.0??C?.
v???n5??
p??[A?\\??0
```



```

Decryption array after XOR with corresponding key value :
[115, 116, 32, 114, 101, 97, 115, 111, 110, 32, 99, 97, 116, 115, 32, 119, 111, 110, 226, 128, 153, 116, 32, 117, 115, 101, 32, 10
7, 105, 116, 116, 121, 32, 100, 111, 111, 114, 115, 32, 105, 115, 32, 98, 101, 99, 97, 117, 115, 101, 32, 115, 111, 109, 101, 32,
99, 97, 116, 115, 32, 100, 111, 110, 226, 128, 153, 116, 32, 108, 105, 107, 101, 32, 116, 104, 101, 32, 102, 101, 101, 108, 105, 1
10, 103, 32, 111, 102, 32, 112, 117, 115, 104, 105, 110, 103, 32, 116, 104, 114, 111, 117, 103, 104, 32, 116, 104, 101, 32, 100, 1
11, 111, 114, 32, 97, 110, 100, 32, 104, 97, 118, 105, 110, 103, 32, 116, 104, 101, 32, 100, 111, 111, 114, 32, 100, 114, 97, 103,
32, 97, 99, 114, 111, 115, 115, 32, 116, 104, 101, 105, 114, 32, 98, 97, 99, 107, 46, 32, 66, 117, 116, 32, 100, 111, 110, 226, 1
28, 153, 116, 32, 119, 111, 114, 114, 121, 226, 128, 148, 116, 104, 101, 114, 101, 32, 105, 115, 32, 97, 32, 115, 111, 108, 117, 1
16, 105, 111, 110, 32, 102, 111, 114, 32, 116, 104, 105, 115, 32, 107, 105, 116, 116, 121, 45, 100, 111, 111, 114, 32, 112, 114, 1
11, 98, 108, 101, 109, 46, 84, 104, 101, 32, 102, 105, 114, 115, 116, 32, 115, 116, 101, 112, 32, 105, 110, 32, 115, 111, 108, 118
, 105, 110, 103, 32, 116, 51, 53, 50, 102, 98, 54, 97, 48, 55, 49, 102, 56, 50, 51, 53, 100]

Plaintext obtained (without the hash) after decryption from the XOR'ed decryption array :
st reason cats won't use kitty doors is because some cats don't like the feeling of pushing through the door and having the door d
rag across their back. But don't worry--there is a solution for this kitty-door problem.The first step in solving t

Receiver manually generating hash value of decrypted plaintext obtained : 352fb6a071f8235d

Receiver Comparing generated hash with hash attached inside ciphertext given by sender !

The hash values match !

Expected next value of counter : 3

Counter value of next piece of ciphertext sent by sender : 1

Ciphertext being decrypted :
'?c????d?/gtjQ\????#m?+I??W????xE?KXMH   u???=?ôd??n?2JU
                                     ? :Ek?Njn?
                                     ?za?2Pp/I????L=
                                     o)??

????B????
      Jzx????
??59?=?N?e???2?Wl???h?>??p?o??<aC????vChu?A$/V????y?h?M\???Z0???z?Gs?Q*L??A?)?N???C?G???9y?R8

Decryption array after XOR with corresponding key value :
[46, 32, 84, 104, 101, 121, 32, 109, 97, 121, 32, 110, 111, 116, 32, 117, 110, 100, 101, 114, 115, 116, 97, 110, 100, 32, 116, 104
, 97, 116, 32, 105, 116, 32, 105, 115, 32, 97, 32, 108, 105, 116, 116, 108, 101, 32, 100, 111, 111, 114, 119, 97, 121, 32, 106, 11
7, 115, 116, 32, 102, 111, 114, 32, 116, 104, 101, 109, 46, 32, 83, 101, 99, 111, 110, 100, 44, 32, 109, 97, 110, 121, 32, 107, 10
5, 116, 116, 121, 32, 100, 111, 111, 114, 115, 32, 97, 114, 101, 32, 100, 97, 114, 107, 44, 32, 97, 110, 100, 32, 99, 97, 116, 115
, 32, 99, 97, 110, 110, 111, 116, 32, 115, 101, 101, 32, 116, 111, 32, 116, 104, 101, 32, 111, 116, 104, 101, 114, 32, 115, 105, 1
00, 101, 46, 32, 65, 115, 32, 115, 117, 99, 104, 44, 32, 116, 104, 101, 121, 32, 99, 97, 110, 226, 128, 153, 116, 32, 98, 101, 32,
115, 117, 114, 101, 32, 111, 102, 32, 119, 104, 97, 116, 32, 105, 115, 32, 111, 110, 32, 116, 104, 101, 32, 111, 116, 104, 101, 1
14, 32, 115, 105, 100, 101, 32, 111, 102, 32, 116, 104, 101, 32, 100, 111, 111, 114, 44, 32, 115, 111, 32, 116, 104, 101, 121, 32,
119, 111, 110, 226, 128, 153, 116, 32, 116, 97, 107, 101, 32, 116, 104, 101, 32, 114, 105, 115, 107, 46, 32, 79, 110, 101, 32, 10
8, 97, 56, 48, 57, 55, 57, 53, 48, 101, 50, 55, 48, 57, 53, 102, 51, 98]

Plaintext obtained (without the hash) after decryption from the XOR'ed decryption array :
. They may not understand that it is a little doorway just for them. Second, many kitty doors are dark, and cats cannot see to the
other side. As such, they can't be sure of what is on the other side of the door, so they won't take the risk. One la

Receiver manually generating hash value of decrypted plaintext obtained : 8097950e27095f3b

Receiver Comparing generated hash with hash attached inside ciphertext given by sender !

```

The hash values match !

Expected next value of counter : 2

Counter value of next piece of ciphertext sent by sender : 0

Ciphertext being decrypted :

```
=??T?>fg?]]??k??7/V&a}??uQ?90??p??A\<????{?M?x? ?v/????2?????]?#g0%=%m??pTGm??[5?XK4]?h?A???dB?xo2??:^?[??d???????;????6?$$$  
??0???E?d?@?6riu/?..??3????Y???l?zk??j3N?4V#i?/Ba?  
pd??S>/wHY?^2?S?-~I* }?f
```

Decryption array after XOR with corresponding key value :

```
[80, 101, 111, 112, 108, 101, 32, 111, 102, 116, 101, 110, 32, 105, 110, 115, 116, 97, 108, 108, 32, 97, 32, 107, 105, 116, 116, 1  
21, 32, 100, 111, 111, 114, 44, 32, 111, 110, 108, 121, 32, 116, 111, 32, 100, 105, 115, 99, 111, 118, 101, 114, 32, 116, 104, 97,  
116, 32, 116, 104, 101, 121, 32, 104, 97, 118, 101, 32, 97, 32, 112, 114, 111, 98, 108, 101, 109, 46, 32, 84, 104, 101, 32, 112,  
114, 111, 98, 108, 101, 109, 32, 105, 115, 32, 116, 104, 101, 105, 114, 32, 99, 97, 116, 32, 119, 105, 108, 108, 32, 110, 111, 116  
, 32, 117, 115, 101, 32, 116, 104, 101, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 46, 32, 84, 104, 101, 114, 101, 32, 9  
7, 114, 101, 32, 115, 101, 118, 101, 114, 97, 108, 32, 99, 111, 109, 109, 111, 110, 32, 114, 101, 97, 115, 111, 110, 115, 32, 119,  
104, 121, 32, 99, 97, 116, 115, 32, 119, 111, 110, 226, 128, 153, 116, 32, 117, 115, 101, 32, 107, 105, 116, 116, 121, 32, 100, 1  
11, 111, 114, 115, 46, 32, 70, 105, 114, 115, 116, 44, 32, 116, 104, 101, 121, 32, 109, 97, 121, 32, 110, 111, 116, 32, 117, 110,  
100, 101, 114, 115, 116, 97, 110, 100, 32, 104, 111, 119, 32, 97, 32, 107, 105, 116, 116, 121, 32, 100, 111, 111, 114, 32, 119, 11  
1, 114, 107, 115, 101, 52, 48, 48, 98, 98, 101, 100, 54, 48, 53, 54, 99, 52, 51, 101]
```

Plaintext obtained (without the hash) after decryption from the XOR'd decryption array :

People often install a kitty door, only to discover that they have a problem. The problem is their cat will not use the kitty door . There are several common reasons why cats won't use kitty doors. First, they may not understand how a kitty door works

Receiver manually generating hash value of decrypted plaintext obtained : e400bbbed6056c43e

Receiver Comparing generated hash with hash attached inside ciphertext given by sender !

The hash values match !

Expected next value of counter : 1

Decryption Ends Here

THE FINAL PLAINTEXT RECEIVED BY RECEIVER AFTER RE-ORDERING (Along with padding of last block) :

People often install a kitty door, only to discover that they have a problem. The problem is their cat will not use the kitty door . There are several common reasons why cats won't use kitty doors. First, they may not understand how a kitty door works. They may not understand that it is a little doorway just for them. Second, many kitty doors are dark, and cats cannot see to the other side. As such, they can't be sure of what is on the other side of the door, so they won't take the risk. One last reason cats won't use kitty doors is because some cats don't like the feeling of pushing through the door and having the door drag across their back. But don't worry—there is a solution for this kitty-door problem. The first step in solving the problem is to prop the door open with tape. This means your cat will now be able to see through to the other side; your cat will likely begin using the kitty door immediately. Once your cat has gotten used to using the kitty door, remove the tape.10

Amals-MacBook-Air:prog_assgmnt amalmajeed\$

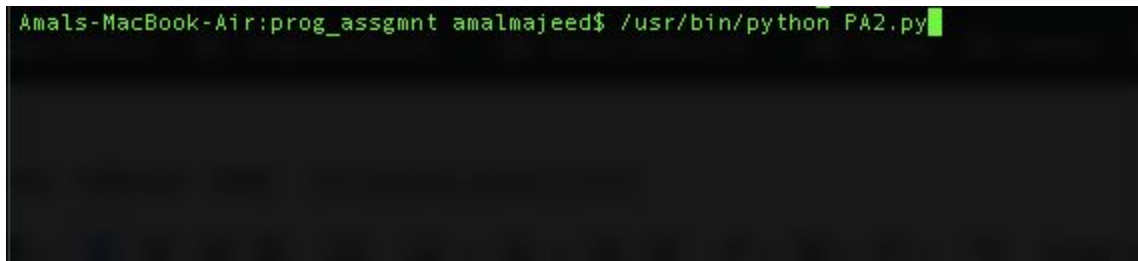
Dependencies / Software Requirements

- **Python 2.7** interpreter (On how to install if not already installed , visit : <https://www.python.org/downloads/>)
- **hashlib** module - ***comes pre-installed in all python interpreters above 2.6*** (in case an import error occurs - run 'pip install hashlib' from terminal)

Execution

The command environment varies from system to system , the below specifications are for linux based operating systems (Ubuntu , MacOS etc) and might be different for windows systems.

1. In the command prompt type in the path to the interpreter followed by the name of the program file as follows : -

A screenshot of a terminal window with a black background and green text. The prompt shows the user is on a Mac (Amals-MacBook-Air) in a directory named 'prog_assgmt'. The user has entered the command '/usr/bin/python PA2.py' and the cursor is at the end of the line.

```
Amals-MacBook-Air:prog_assgmt amalmajeed$ /usr/bin/python PA2.py
```

Where **PA2.py** is the name of the program and **/usr/bin/python** is the full system path for the python2.7 interpreter (this varies from system to system).
