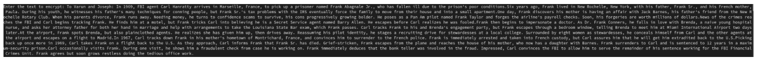
Computer Network Security (F20CN) CW 2

Joseph Emmanuel (H00375744) and Varun Senthil Kumar (H00384753)

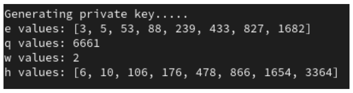
Group 30

Task 1

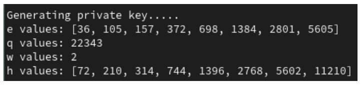


```
Enter the text to encrypt: To Varun and Joseph: In 1969, FBI agent Carl Hanratty arrives in Marseille, France, to pick up a prisoner named Frank Abagnale Jr., who has fallen ill due to the prison's poor conditions.Six years ago, Frank lived in New Rochelle, New York, with his father, Frank Sr., and his French mother,
 Paula. During his youth, he witnesses his father's many techniques for conning people, but Frank Sr.'s tax problems with the IRS eventually force the family to move from their house and into a small apartment.One day, Frank discovers his mother is having an affair with Jack Barnes, his father's friend from the New R
ochelle Rotary Club. When his parents divorce, Frank runs away. Needing money, he turns to confidence scams to survive, his cons progressively growing bolder. He poses as a Pan Am pilot named Frank Taylor and forges the airline's payroll checks. Soon, his forgeries are worth millions of dollars.News of the crimes rea
ches the FBI and Carl begins tracking Frank. He finds him at a motel, but Frank tricks Carl into believing he is a Secret Service agent named Barry Allen. He escapes before Carl realizes he was fooled.Frank then begins to impersonate a doctor. As Dr. Frank Conners, he falls in love with Brenda, a naive young hospital
 nurse, and asks her attorney father for both her hand in marriage and help with arrangements to take the Louisiana State Bar exam, which Frank passes. Carl tracks Frank to his and Brenda's engagement party, but Frank escapes through a bedroom window, telling Brenda to meet him at Miami International Airport two days
 later.At the airport, Frank spots Brenda, but also plainclothed agents. He realizes she has given him up, then drives away. Reassuming his pilot identity, he stages a recruiting drive for stewardesses at a local college. Surrounded by eight women as stewardesses, he conceals himself from Carl and the other agents at
 the airport and escapes on a flight to Madrid.In 1967, Carl tracks down Frank in his mother's hometown of Montrichard, France, and convinces him to surrender to the French police. Frank is immediately arrested and taken into French custody, but Carl assures him that he will get him extradited back to the U.S.Picking
 back up once more in 1969, Carl takes Frank on a flight back to the U.S. As they approach, Carl informs Frank that Frank Sr. has died. Grief-stricken, Frank escapes from the plane and reaches the house of his mother, who now has a daughter with Barnes. Frank surrenders to Carl and is sentenced to 12 years in a maxim
um-security prison.Carl occasionally visits Frank. During one visit, he shows him a fraudulent check from case he is working on. Frank immediately deduces that the bank teller was involved in the fraud. Impressed, Carl convinces the FBI to allow him to serve the remainder of his sentence working for the FBI Financial
 Crimes Unit. Frank agrees but soon grows restless doing the tedious office work.
```

- This is the input the user gives into the program first.
- The program then turns the ASCII values into binary format to process the data for encryption and decryption.

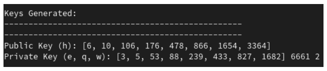


```
Generating private key.....
e values: [3, 5, 53, 88, 239, 433, 827, 1682]
q values: 6661
w values: 2
h values: [6, 10, 106, 176, 478, 866, 1654, 3364]
```

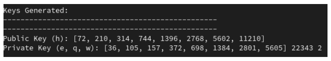


```
Generating private key.....
e values: [36, 105, 157, 372, 698, 1384, 2801, 5605]
q values: 22343
w values: 2
h values: [72, 210, 314, 744, 1396, 2768, 5602, 11210]
```

- A private key is then generated first by generating random e values, these are random numbers where the next random number is greater than the previous sum of random numbers. After this, we generate a q value, just a random prime number that should be greater than the sum of all $max\ (e\ values)\ \times\ 2$. Then finally we generate a number w which should have a GCD value of 1 with q. All of this makes up our private key.

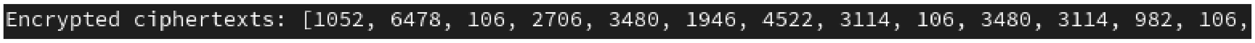


```
Keys Generated:
--------------------------------------------------
--------------------------------------------------
Public Key (h): [6, 10, 106, 176, 478, 866, 1654, 3364]
Private Key (e, q, w): [3, 5, 53, 88, 239, 433, 827, 1682] 6661 2
```



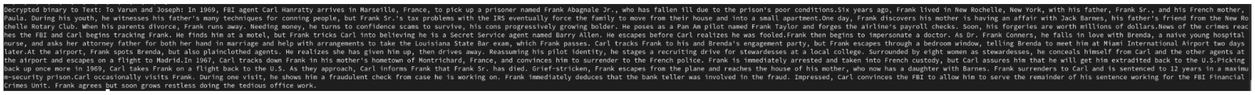
```
Keys Generated:
--------------------------------------------------
--------------------------------------------------
Public Key (h): [72, 210, 314, 744, 1396, 2768, 5602, 11210]
Private Key (e, q, w): [36, 105, 157, 372, 698, 1384, 2801, 5605] 22343 2
```

- We then calculate the h values which are our public key, h values are computed by $(w\ \times\ ei)\ \%\ q$ where ei are the elements of e.
- The message is then broken down into 8 bits each to then be encrypted via the public key values $h1\ \times\ m1\ +\ h2\ \times\ m2$ where mi is the broken message bit chunks



```
Encrypted ciphertexts: [1052, 6478, 106, 2706, 3480, 1946, 4522, 3114, 106, 3480, 3114, 982, 106,
```

- We then get the final encrypted text which is just the weight of each 8 bits within the message encrypted
- To decrypt the text we need our private key and to do that we need to find the w_{inv}using extended Euclid's algorithm. We then use this to get the adjusted c'value by calculating $c'\ =\ (c\ \times\ q)\ \%\ q$ which will give us the adjusted c'value for each 8 bits.
- We can then use the adjusted c' values to compare it with the largest ei values and keep going down the list to recreate the bits of the message. If c' is larger then ei the bit is 1 then subtract $c'\ -\ ei$ to get the updated c'value else 0 bit.
- We get the decrypted binary of the message which we will then transform it back into ASCII values



```
Decrypted binary to Text: To Varun and Joseph: In 1969, FBI agent Carl Hanratty arrives in Marseille, France, to pick up a prisoner named Frank Abagnale Jr., who has fallen ill due to the prison's poor conditions.Six years ago, Frank lived in New Rochelle, New York, with his father, Frank Sr., and his French mother,
Paula. During his youth, he witnesses his father's many techniques for conning people, but Frank Sr.'s tax problems with the IRS eventually force the family to move from their house and into a small apartment.One day, Frank discovers his mother is having an affair with Jack Barnes, his father's friend from the New Ro
chelle Rotary Club. When his parents divorce, Frank runs away. Needing money, he turns to confidence scams to survive, his cons progressively growing bolder. He poses as a Pan Am pilot named Frank Taylor and forges the airline's payroll checks. Soon, his forgeries are worth millions of dollars.News of the crimes reac
hes the FBI and Carl begins tracking Frank. He finds him at a motel, but Frank tricks Carl into believing he is a Secret Service agent named Barry Allen. He escapes before Carl realizes he was fooled.Frank then begins to impersonate a doctor. As Dr. Frank Conners, he falls in love with Brenda, a naive young hospital
nurse, and asks her attorney father for both her hand in marriage and help with arrangements to take the Louisiana State Bar exam, which Frank passes. Carl tracks Frank to his and Brenda's engagement party, but Frank escapes through a bedroom window, telling Brenda to meet him at Miami International Airport two days
later.At the airport, Frank spots Brenda, but also plainclothed agents. He realizes she has given him up, then drives away. Reassuming his pilot identity, he stages a recruiting drive for stewardesses at a local college. Surrounded by eight women as stewardesses, he conceals himself from Carl and the other agents at
the airport and escapes on a flight to Madrid.In 1967, Carl tracks down Frank in his mother's hometown of Montrichard, France, and convinces him to surrender to the French police. Frank is immediately arrested and taken into French custody, but Carl assures him that he will get him extradited back to the U.S.Picking
back up once more in 1969, Carl takes Frank on a flight back to the U.S. As they approach, Carl informs Frank that Frank Sr. has died. Grief-stricken, Frank escapes from the plane and reaches the house of his mother, who now has a daughter with Barnes. Frank surrenders to Carl and is sentenced to 12 years in a maximu
m-security prison.Carl occasionally visits Frank. During one visit, he shows him a fraudulent check from case he is working on. Frank immediately deduces that the bank teller was involved in the fraud. Impressed, Carl convinces the FBI to allow him to serve the remainder of his sentence working for the FBI Financial
Crimes Unit. Frank agrees but soon grows restless doing the tedious office work.
```

- Final decrypted text!!.

Please do note due to the size of the text we were not able to screenshot everything but it still does prove the math and decryption work well. Please check the appendix for more information.

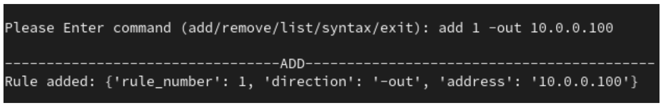
(Please also note the key length we had chosen for the task is 8 bits. Of course,e in a real-world scenario this would be a security nightmare but for computational and educational purposes we had chosen a small number, just to understand and demonstrate the task well)

```
FUNCTION is_prime(n):
    RETURN True if n > 1 and has no divisors up to sqrt(n)

FUNCTION find_next_prime(start):
    INCREMENT start until prime number found; RETURN start

FUNCTION modular_inverse(a, b):
    USE Extended Euclidean Algorithm to find the mod_inverse; RETURN inverse mod b

FUNCTION generate_private_key(length, max_value):
    CREATE list e with random values where each value is higher than the sum of previous values; RETURN e

FUNCTION generate_public_key(e):
    CALCULATE q = next prime > (2 * sum(e))
    FIND w such that gcd(w, q) = 1
    CALCULATE h = [(w * ei) % q for each ei in e]; RETURN h, q, w

FUNCTION text_to_binary(text):
    CONVERT each character to 8-bit binary; RETURN binary list

FUNCTION encrypt_message(binary_message, h):
    DIVIDE binary_message into 8-bit chunks
    CALCULATE ciphertext as sum(chunk[i] * h[i]); RETURN ciphertext list

FUNCTION decrypt_message(ciphertexts, e, q, w):
    CALCULATE w_inverse
    FOR each ciphertext:
        COMPUTE c' = (ciphertext * w_inverse) MOD q
        REVERSE private key to reconstruct binary
    RETURN full decrypted binary

FUNCTION binary_to_text(binary_message):
    CONVERT 8-bit chunks to characters; RETURN text
```

The hard part of the task was to find the modular inverse correctly as previous implementations did not work. Finding the next prime number was also a bit of a challenge as we kept having issues where the prime numbers were taking too long to calculate as the numbers were bigger.

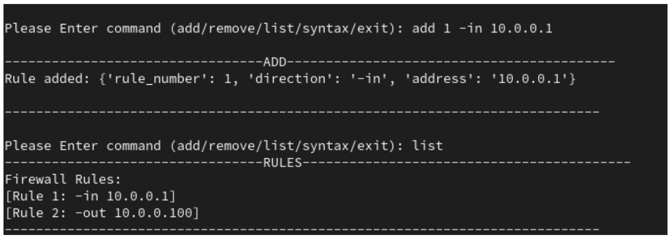
The rest of the implementation was fairly fine and with the help of Gemini, and other online resources we were able to understand the math quite well. Overall a great task for sure!!

Task 2



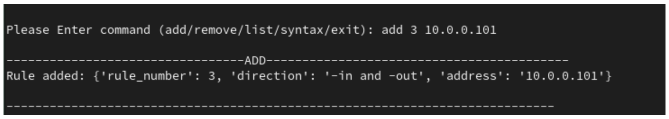
```
Please Enter command (add/remove/list/syntax/exit): add 1 -out 10.0.0.100

---------------------------------ADD------------------------------------------
Rule added: {'rule_number': 1, 'direction': '-out', 'address': '10.0.0.100'}
```

- Rule adding



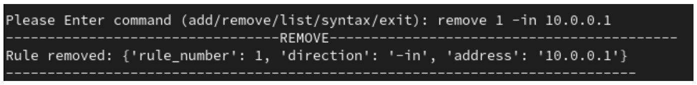
```
Please Enter command (add/remove/list/syntax/exit): add 1 -in 10.0.0.1

--------------------------------ADD-----------------------------------------
Rule added: {'rule_number': 1, 'direction': '-in', 'address': '10.0.0.1'}

--------------------------------------------------------------------------


Please Enter command (add/remove/list/syntax/exit): list
--------------------------------RULES-----------------------------------------
Firewall Rules:
[Rule 1: -in 10.0.0.1]
[Rule 2: -out 10.0.0.100]
--------------------------------------------------------------------------
```

- New rule 1 overwrites previous rule 1



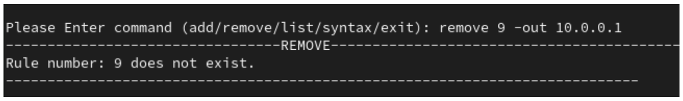
```
Please Enter command (add/remove/list/syntax/exit): add 3 10.0.0.101

-------------------------------ADD----------------------------------------
Rule added: {'rule_number': 3, 'direction': '-in and -out', 'address': '10.0.0.101'}

------------------------------------------------------------------------
```

- Direction not mentioned means both -in and -out are set



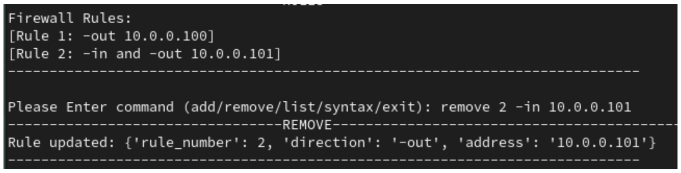
```
Please Enter command (add/remove/list/syntax/exit): remove 1 -in 10.0.0.1
---------------------------------REMOVE------------------------------------------
Rule removed: {'rule_number': 1, 'direction': '-in', 'address': '10.0.0.1'}
--------------------------------------------------------------------------
```

- Remove mentioned rule



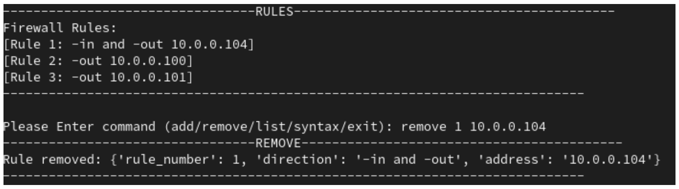
```
Please Enter command (add/remove/list/syntax/exit): remove 9 -out 10.0.0.1
---------------------------------REMOVE-------------------------------------------
Rule number: 9 does not exist.
--------------------------------------------------------------------------
```

- Remove rule not listed (error)



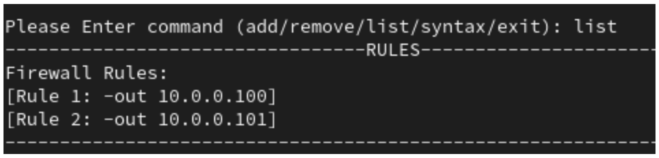
```
Firewall Rules:
[Rule 1: -out 10.0.0.100]
[Rule 2: -in and -out 10.0.0.101]
--------------------------------------------------------------------------


Please Enter command (add/remove/list/syntax/exit): remove 2 -in 10.0.0.101
---------------------------------REMOVE-------------------------------------------
Rule updated: {'rule_number': 2, 'direction': '-out', 'address': '10.0.0.101'}
--------------------------------------------------------------------------
```

- Remove direction within a rule that has -in and -out



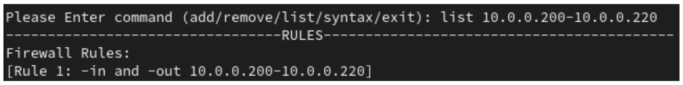
```
-------------------------------RULES----------------------------------------
Firewall Rules:
[Rule 1: -in and -out 10.0.0.104]
[Rule 2: -out 10.0.0.100]
[Rule 3: -out 10.0.0.101]
--------------------------------------------------------------------------


Please Enter command (add/remove/list/syntax/exit): remove 1 10.0.0.104
--------------------------------REMOVE-----------------------------------------
Rule removed: {'rule_number': 1, 'direction': '-in and -out', 'address': '10.0.0.104'}
--------------------------------------------------------------------------
```

- Remove full rule without mentioning direction (for both -in and -out)



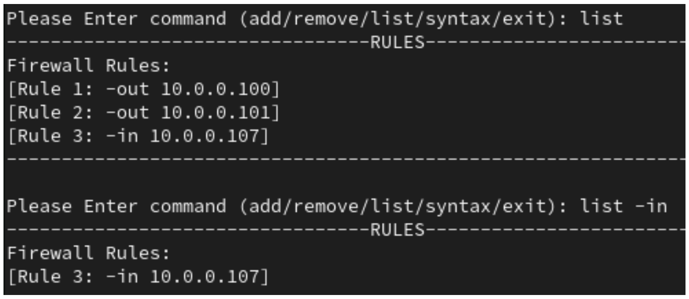
```
Please Enter command (add/remove/list/syntax/exit): list
---------------------------------RULES----------------------
Firewall Rules:
[Rule 1: -out 10.0.0.100]
[Rule 2: -out 10.0.0.101]
------------------------------------------------------------
```

- List all the rules



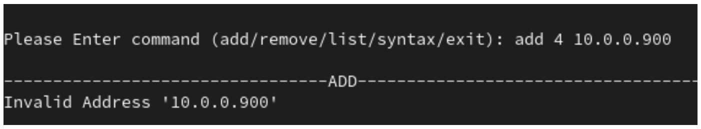
```
Please Enter command (add/remove/list/syntax/exit): list 10.0.0.200-10.0.0.220
-------------------------------RULES----------------------------------------
Firewall Rules:
[Rule 1: -in and -out 10.0.0.200-10.0.0.220]
```

- List a rule based on range or single IP address

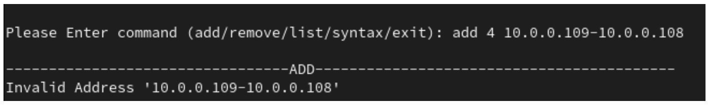


```
Please Enter command (add/remove/list/syntax/exit): list
---------------------------------RULES------------------------
Firewall Rules:
[Rule 1: -out 10.0.0.100]
[Rule 2: -out 10.0.0.101]
[Rule 3: -in 10.0.0.107]
--------------------------------------------------------------

Please Enter command (add/remove/list/syntax/exit): list -in
---------------------------------RULES------------------------
Firewall Rules:
[Rule 3: -in 10.0.0.107]
```

- List all rules based on a certain direction

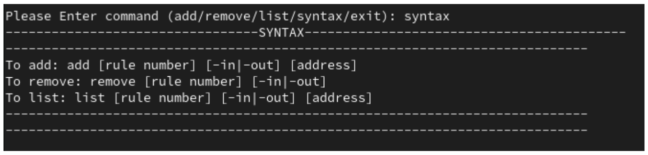


```
Please Enter command (add/remove/list/syntax/exit): add 4 10.0.0.900

--------------------------------ADD----------------------------------
Invalid Address '10.0.0.900'
```



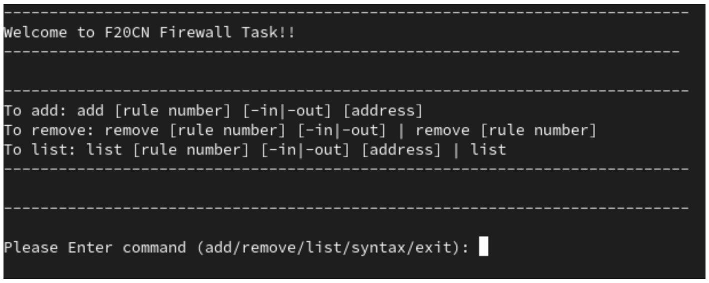
```
Please Enter command (add/remove/list/syntax/exit): add 4 10.0.0.109-10.0.0.108

--------------------------------ADD-----------------------------------------
Invalid Address '10.0.0.109-10.0.0.108'
```

- Error handling for incorrect IP address format or range



```
Please Enter command (add/remove/list/syntax/exit): syntax
-------------------------------SYNTAX----------------------------------------
------------------------------------------------------------------------
To add: add [rule number] [-in|-out] [address]
To remove: remove [rule number] [-in|-out]
To list: list [rule number] [-in|-out] [address]
------------------------------------------------------------------------
------------------------------------------------------------------------
```

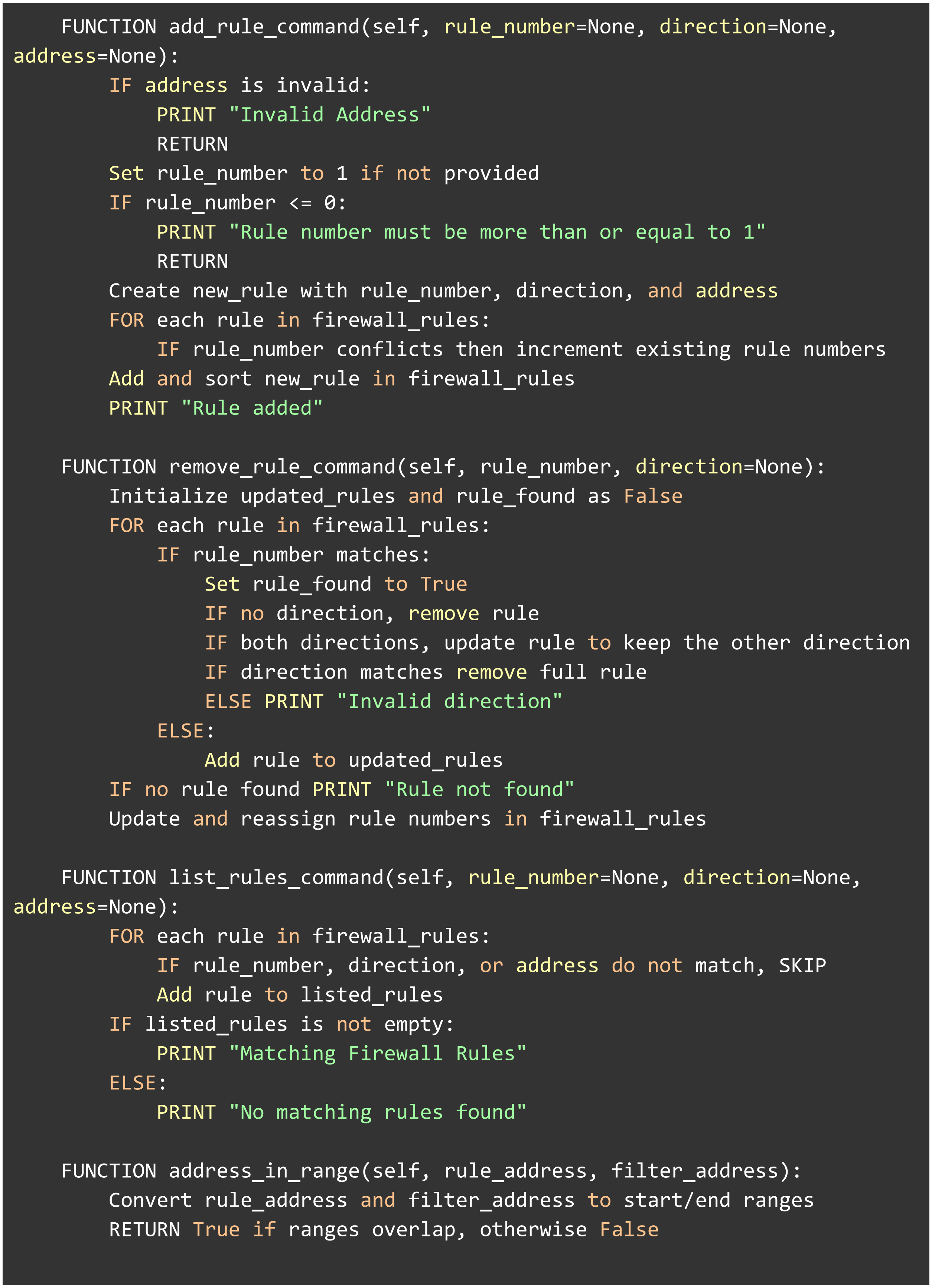
- Syntax option for the user when using the program



```
--------------------------------------------------------------------------
Welcome to F20CN Firewall Task!!
-------------------------------------------------------------------------


--------------------------------------------------------------------------
To add: add [rule number] [-in|-out] [address]
To remove: remove [rule number] [-in|-out] | remove [rule number]
To list: list [rule number] [-in|-out] [address] | list
--------------------------------------------------------------------------

--------------------------------------------------------------------------

Please Enter command (add/remove/list/syntax/exit): 
```

- Start screen when you run the program

```
CLASS Firewall:
    METHOD _init_():
        Initialize firewall_rules as an empty list
```



```
    FUNCTION add_rule_command(self, rule_number=None, direction=None,
address=None):
        IF address is invalid:
            PRINT "Invalid Address"
            RETURN
        Set rule_number to 1 if not provided
        IF rule_number <= 0:
            PRINT "Rule number must be more than or equal to 1"
            RETURN
        Create new_rule with rule_number, direction, and address
        FOR each rule in firewall_rules:
            IF rule_number conflicts then increment existing rule numbers
        Add and sort new_rule in firewall_rules
        PRINT "Rule added"

    FUNCTION remove_rule_command(self, rule_number, direction=None):
        Initialize updated_rules and rule_found as False
        FOR each rule in firewall_rules:
            IF rule_number matches:
                Set rule_found to True
                IF no direction, remove rule
                IF both directions, update rule to keep the other direction
                IF direction matches remove full rule
                ELSE PRINT "Invalid direction"
            ELSE:
                Add rule to updated_rules
        IF no rule found PRINT "Rule not found"
        Update and reassign rule numbers in firewall_rules

    FUNCTION list_rules_command(self, rule_number=None, direction=None,
address=None):
        FOR each rule in firewall_rules:
            IF rule_number, direction, or address do not match, SKIP
            Add rule to listed_rules
        IF listed_rules is not empty:
            PRINT "Matching Firewall Rules"
        ELSE:
            PRINT "No matching rules found"

    FUNCTION address_in_range(self, rule_address, filter_address):
        Convert rule_address and filter_address to start/end ranges
        RETURN True if ranges overlap, otherwise False
    FUNCTION validate_address(self, address):
        TRY to validate address as single or range
        RETURN True if valid, otherwise False

FUNCTION parse_input(input_str):
    Split input into command, rule_number, direction, address
    RETURN parsed values as dictionary
```

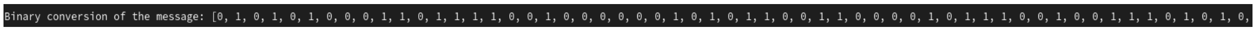
The way the firewall task was done was through simple logic. It was mainly a if else if tree spanning across based on what we needed to do and how it was supposed to be done, based on the CW. We essentially divided up what functionality was necessary and based on that we had done the task. Once the functionality was done it was just a matter of customization, how we wanted the terminal start screen to look like, help options and so on. The only external libraries used were the IP address library to convert the addresses given within the terminal to IPV4 objects, this just made things much easier and overall smooth.

Abstract

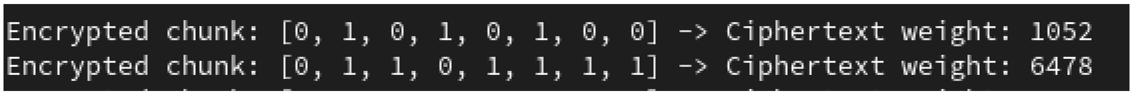
500+ word text for Task 1

To Varun and Joseph: In 1969, FBI agent Carl Hanratty arrives in Marseille, France, to pick up a prisoner named Frank Abagnale Jr., who has fallen ill due to the prison's poor conditions.Six years ago, Frank lived in New Rochelle, New York, with his father, Frank Sr., and his French mother, Paula. During his youth, he witnesses his father's many techniques for conning people, but Frank Sr.'s tax problems with the IRS eventually force the family to move from their house and into a small apartment.One day, Frank discovers his mother is having an affair with Jack Barnes, his father's friend from the New Rochelle Rotary Club. When his parents divorce, Frank runs away. Needing money, he turns to confidence scams to survive, his cons progressively growing bolder. He poses as a Pan Am pilot named Frank Taylor and forges the airline's payroll checks. Soon, his forgeries are worth millions of dollars.News of the crimes reaches the FBI and Carl begins tracking Frank. He finds him at a motel, but Frank tricks Carl into believing he is a Secret Service agent named Barry Allen. He escapes before Carl realizes he was fooled.Frank then begins to impersonate a doctor. As Dr. Frank Conners, he falls in love with Brenda, a naive young hospital nurse, and asks her attorney father for both her hand in marriage and help with arrangements to take the Louisiana State Bar exam, which Frank passes. Carl tracks Frank to his and Brenda's engagement party, but Frank escapes through a bedroom window, telling Brenda to meet him at Miami International Airport two days later.At the airport, Frank spots Brenda, but also plainclothed agents. He realizes she has given him up, then drives away. Reassuming his pilot identity, he stages a recruiting drive for stewardesses at a local college. Surrounded by eight women as stewardesses, he conceals himself from Carl and the other agents at the airport and escapes on a flight to Madrid.In 1967, Carl tracks down Frank in his mother's hometown of Montrichard, France, and convinces him to surrender to the French police. Frank is immediately arrested and taken into French custody, but Carl assures him that he will get him extradited back to the U.S.Picking back up once more in 1969, Carl takes Frank on a flight back to the U.S. As they approach, Carl informs Frank that Frank Sr. has died. Grief-stricken, Frank escapes from the plane and reaches the house of his mother, who now has a daughter with Barnes. Frank surrenders to Carl and is sentenced to 12 years in a maximum-security prison.Carl occasionally visits Frank. During one visit, he shows him a fraudulent check from case he is working on. Frank immediately deduces that the bank teller was involved in the fraud. Impressed, Carl convinces the FBI to allow him to serve the remainder of his sentence working for the FBI Financial Crimes Unit. Frank agrees but soon grows restless doing the tedious office work.

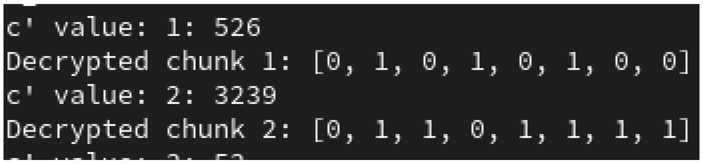
Screenshots from Task 1



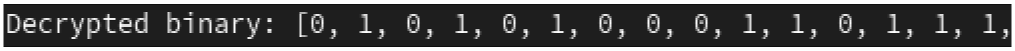
```
Binary conversion of the message: [0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0,
```



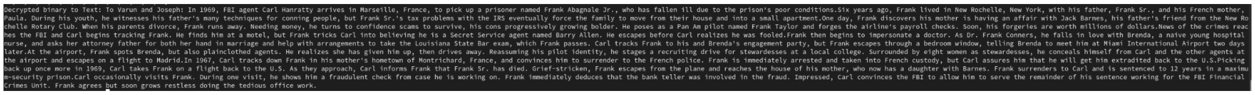
```
Encrypted chunk: [0, 1, 0, 1, 0, 1, 0, 0] -> Ciphertext weight: 1052
Encrypted chunk: [0, 1, 1, 0, 1, 1, 1, 1] -> Ciphertext weight: 6478
```



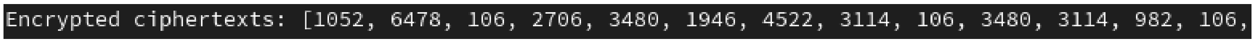
```
c' value: 1: 526
Decrypted chunk 1: [0, 1, 0, 1, 0, 1, 0, 0]
c' value: 2: 3239
Decrypted chunk 2: [0, 1, 1, 0, 1, 1, 1, 1]
```



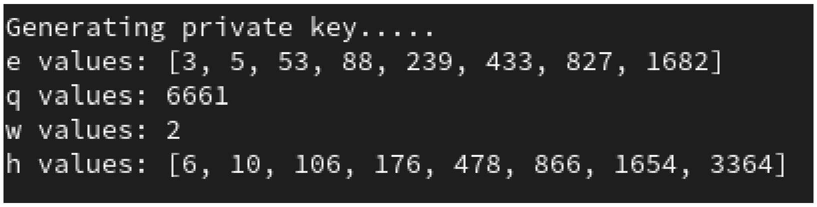
```
Decrypted binary: [0, 1, 0, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1,
```



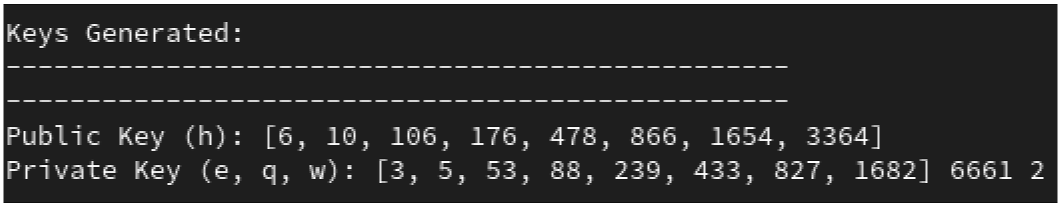
```
Decrypted binary to Text: To Varun and Joseph: In 1969, FBI agent Carl Hanratty arrives in Marseille, France, to pick up a prisoner named Frank Abagnale Jr., who has fallen ill due to the prison's poor conditions.Six years ago, Frank lived in New Rochelle, New York, with his father, Frank Sr., and his French mother,
Paula. During his youth, he witnesses his father's many techniques for conning people, but Frank Sr.'s tax problems with the IRS eventually force the family to move from their house and into a small apartment.One day, Frank discovers his mother is having an affair with Jack Barnes, his father's friend from the New Ro
chelle Rotary Club. When his parents divorce, Frank runs away. Needing money, he turns to confidence scams to survive, his cons progressively growing bolder. He poses as a Pan Am pilot named Frank Taylor and forges the airline's payroll checks. Soon, his forgeries are worth millions of dollars.News of the crimes reac
hes the FBI and Carl begins tracking Frank. He finds him at a motel, but Frank tricks Carl into believing he is a Secret Service agent named Barry Allen. He escapes before Carl realizes he was fooled.Frank then begins to impersonate a doctor. As Dr. Frank Conners, he falls in love with Brenda, a naive young hospital
nurse, and asks her attorney father for both her hand in marriage and help with arrangements to take the Louisiana State Bar exam, which Frank passes. Carl tracks Frank to his and Brenda's engagement party, but Frank escapes through a bedroom window, telling Brenda to meet him at Miami International Airport two days
later.At the airport, Frank spots Brenda, but also plainclothed agents. He realizes she has given him up, then drives away. Reassuming his pilot identity, he stages a recruiting drive for stewardesses at a local college. Surrounded by eight women as stewardesses, he conceals himself from Carl and the other agents at
the airport and escapes on a flight to Madrid.In 1967, Carl tracks down Frank in his mother's hometown of Montrichard, France, and convinces him to surrender to the French police. Frank is immediately arrested and taken into French custody, but Carl assures him that he will get him extradited back to the U.S.Picking
back up once more in 1969, Carl takes Frank on a flight back to the U.S. As they approach, Carl informs Frank that Frank Sr. has died. Grief-stricken, Frank escapes from the plane and reaches the house of his mother, who now has a daughter with Barnes. Frank surrenders to Carl and is sentenced to 12 years in a maximu
m-security prison.Carl occasionally visits Frank. During one visit, he shows him a fraudulent check from case he is working on. Frank immediately deduces that the bank teller was involved in the fraud. Impressed, Carl convinces the FBI to allow him to serve the remainder of his sentence working for the FBI Financial
Crimes Unit. Frank agrees but soon grows restless doing the tedious office work.
```



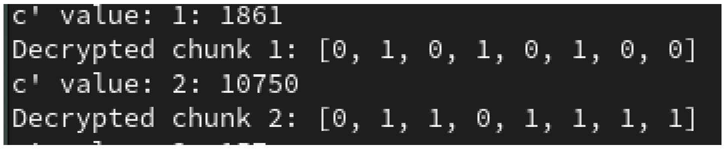
```
Encrypted ciphertexts: [1052, 6478, 106, 2706, 3480, 1946, 4522, 3114, 106, 3480, 3114, 982, 106,
```



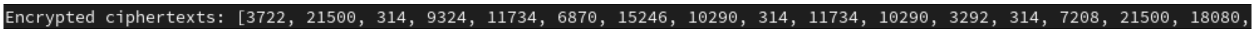
```
Generating private key.....
e values: [3, 5, 53, 88, 239, 433, 827, 1682]
q values: 6661
w values: 2
h values: [6, 10, 106, 176, 478, 866, 1654, 3364]
```



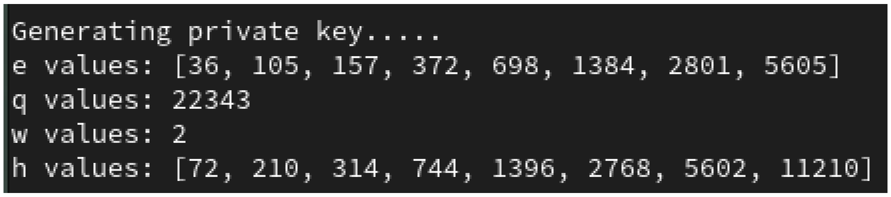
```
Keys Generated:
--------------------------------------------------
--------------------------------------------------
Public Key (h): [6, 10, 106, 176, 478, 866, 1654, 3364]
Private Key (e, q, w): [3, 5, 53, 88, 239, 433, 827, 1682] 6661 2
```



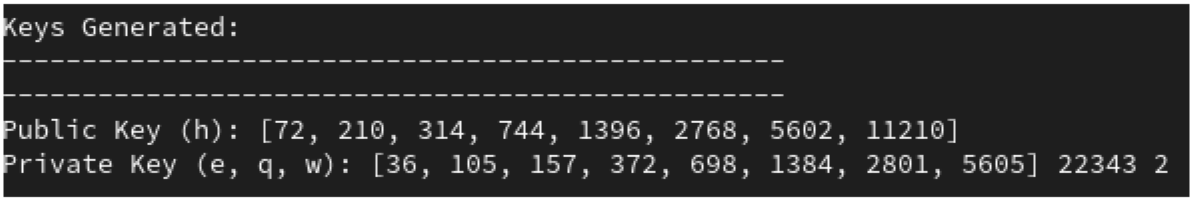
```
c' value: 1: 1861
Decrypted chunk 1: [0, 1, 0, 1, 0, 1, 0, 0]
c' value: 2: 10750
Decrypted chunk 2: [0, 1, 1, 0, 1, 1, 1, 1]
```



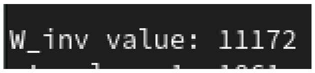
```
Encrypted ciphertexts: [3722, 21500, 314, 9324, 11734, 6870, 15246, 10290, 314, 11734, 10290, 3292, 314, 7208, 21500, 18080,
```



```
Generating private key.....
e values: [36, 105, 157, 372, 698, 1384, 2801, 5605]
q values: 22343
w values: 2
h values: [72, 210, 314, 744, 1396, 2768, 5602, 11210]
```



```
Keys Generated:
--------------------------------------------------
--------------------------------------------------
Public Key (h): [72, 210, 314, 744, 1396, 2768, 5602, 11210]
Private Key (e, q, w): [36, 105, 157, 372, 698, 1384, 2801, 5605] 22343 2
```



```
W_inv value: 11172
```

Math To Task 1
(PLEASE CHECK BELOW)

PUBLIC KEY (h)

$e = [e_1, e_2, e_3 \ldots]$

↓

$e = [3, 4, 8, 17 \ldots]$

↗

(1) each e_i is greater than the Sum of all Previous elements

(2) $q > 2 \times \max(e)$

↓

Random Prime number

2x max [3, 4, 8, 17]

2x max[~~6~~ 32]

64

q any prime after 64

q = 67, 71, 73 ...

③ gcd(w, q) = 1

should = 1

w = random number that shares no common factor with q (1)

$\gcd(2, 71) = \underline{\underline{1}}$

④ $h = [h1, h2 \ldots]$

Where $hi = (W \times ei) \% q$

$h_1 = (2 \times 3) \% 71$

$h_2 = (2 \times 4) \% 71$

$h_3 = (2 \times 8) \% 71$

ENCRYPTION

M -> message

$M = [m_1, m_2, m_3 .....]$

(1) array of BITS
0 or 1

each mi is a Bit (0 or 1)

(2) C -> ciphertext

$C = h_1 \times m_1 + h_2 \times m_2 ....$

hi is the Computed
Public key

Decryption

TO DECRYPT USE

(e, q, w) TO find

W_inv !

$$w \times w\_inv \equiv 1 \ (\mathrm{mod}\ q)$$

① $2 \times \underset{\uparrow}{W\_inv} \equiv 1 \ (\mathrm{mod}\ 71)$

To find this use
euclids extended Algorithm

2 $1 = a \times w + b \times q$

$\downarrow$

~~$71 = 2 \times 35 + 1$~~

$\frac{71}{2} = 35.5$

$71 = 2 \times 35 + 1$

$1 = 71 - 2 \times 35$

$\boxed{1 = a \times w + b \times q}$

$\uparrow$

Rearange to this

$1 = (-35) \times 2 + 1 \times 71$

If negative do

3 $-35 + q$

$-35 + 71 = \underline{\underline{36}}$

~~W_inv~~ W_inv = 36

$\underline{\underline{\text{2 mod inverse } 71 = 36}}$