

UE20CS411SE-EH-Assignment-2

NAME	SRN	CLASS & SECTION
Vijay J	PES2UG20CS815	7 - J

PROBLEM STATEMENT:

Fencing On Rails_1

I forgot to buy a ticket! I asked the train conductor to let me off this time and he said he would, but only if I helped him decipher this message sent by his 5 fencing instructors. Help me solve it so i don't have to pay a fine

Encrypted Message: *ilis_i4nfikr5c{3t}r_*

CODE:

```
nvim ~/P/7/E/A/PES2UG20CS815
1 def rail_fence_decrypt(ciphertext, rails):
2     fence = [[' ' for _ in range(len(ciphertext))] for _ in range(rails)]
3     direction = -1
4     row, col = 0, 0
5
6     for char in ciphertext:      • "char" is not accessed
7         fence[row][col] = '*'
8         if row == 0 or row == rails - 1:
9             direction *= -1
10        row += direction
11        col += 1
12
13    index = 0
14    for i in range(rails):
15        for j in range(len(ciphertext)):
16            if fence[i][j] == '*' and index < len(ciphertext):
17                fence[i][j] = ciphertext[index]
18                index += 1
19
20    plaintext = ''.join(fence[i][j] for j in range(len(ciphertext)) for i in range(rails) if fence[i][j] != ' ')
21    return plaintext
22
23 def main():
24     print("Rail Fence Cipher Decryption")
25     rails = int(input("Enter the number of rails: "))
26     ciphertext = input("Enter the encrypted message: ")
27
28     decrypted_message = rail_fence_decrypt(ciphertext, rails)
29     print("Decrypted Message:", decrypted_message)
30
31 if __name__ == "__main__":
32     main()
NORMAL pes2ug20cs815_rail_fence.py 1 LSP ~ pyright PES2UG20CS815 Top
```

OUTPUT:

```
~/P/7/E/A/PES2UG20CS815
the@vengeance in ~/PESU/7th Sem/EH/Assignment/PES2UG20CS815 via v3.11.5 (venv) took 2ms
python pes2ug20cs815_rail_fence.py
Rail Fence Cipher Decryption
Enter the number of rails: 5
Enter the encrypted message: i1is_i4nfikr5c{3t}r_
Decrypted Message: isfcr{i_1ik3_tr4in5}

the@vengeance in ~/PESU/7th Sem/EH/Assignment/PES2UG20CS815 via v3.11.5 (venv) took 47s
```

PROBLEM STATEMENT:

Desu Yo_1

My friend sent me this hex string and said "**weak desu yo**". What did he mean by this?

Encrypted Message: `\xc8\xd7\xdb\x02\x25\xa0\x6b\xcb\xa4\xb7\x86\xa0\x42\x71\x06\x13\x6e\xdc\x11\xfe\xfb\x9e\xfc\x61\x3b\x28\x35\x80\x17\x4c\x65\x87`

CODE:

```
nvim ~/P/7/E/A/PES2UG20CS815
pes2ug20cs815... x
1 from Crypto.Cipher import DES      • Import "Crypto.Cipher" could not be resolved
2 flag = b"\xc8\xd7\xdb\x02\x25\xa0\x6b\xcb\xa4\xb7\x86\xa0\x42\x71\x06\x13\x6e\xdc\x11\xfe\xfb\x9e\xfc\x61\x3b\x28\x35\x80\x17\x4c\x65\x87"
3 keys = []
4 keys.append(bytes.fromhex("0101010101010101"))
5 keys.append(bytes.fromhex("FEFEFEFEFEFEFEFEFE"))
6 keys.append(bytes.fromhex("E0E0E0E0F1F1F1F1"))
7 keys.append(bytes.fromhex("1F1F1F1F0E0E0E0E"))
8
9 for key in keys:
10     cipher = DES.new(key, DES.MODE_ECB)
11     decrypted_flag = cipher.decrypt(flag)
12     print(decrypted_flag)
```

OUTPUT:

```
~/P/7/E/A/PES2UG20CS815
the@vengeance in ~/PESU/7th Sem/EH/Assignment/PES2UG20CS815 via v3.11.5 (venv) took 2ms
python pes2ug20cs815_desu_vo.py
b'\xb5h_\x99\xf0\x12\x08\xa2\xd0\xa5m\xea\t\xce7J\x7f\x1f\x12\x9a\xaa\x16<\xbe\xe3\xfdy\xbd\xe5\x9f'
b'isfcr{d4ta_3ncrypt10n_standard}\x01'
b'\xd138\x8dt\xed\x13?\x9f\xcd\x8b^b\x8a\x85\xd95\xee\xa1\x8e1\xc1c\x98 \xfah\xd2'
b'\xa2+\xfaDM\x9e\x04\xfe\x82\x9eM\x102\x8d97\xe6\x00\xf3\x1b\tM\x96\xa80\xea\x13\xe5=\xc9d\xee'
the@vengeance in ~/PESU/7th Sem/EH/Assignment/PES2UG20CS815 via v3.11.5 (venv) took 95ms
```

PROBLEM STATEMENT:

RSA Starter

Can you crack this revolutionary asymmetric encryption system?

VALUE:

RSA DECODER

Indicate known numbers, leave remaining cells empty.

★ VALUE OF THE CIPHER MESSAGE (INTEGER) C=

55194046403951580740074039693319065969881451755210...

★ PUBLIC KEY E (USUALLY E=65537) E=

65537

★ PUBLIC KEY VALUE (INTEGER) N=

10847901175976939372717630845745705118586820202822...

OUTPUT:

```
isfcr{rivest_shamir_adleman}
```