

Explanation of the

So firstly, I look at all the file and did cat on all the files. One of the files read it as a pdf extension. So, I changed it to the pdf extension. It was locked and asked for the password. Then I went to the third file and after a while I tried everything and ran it through

<https://www.dcode.fr/scytale-cipher>

and got of the first hit as = the.password.to.the.pdf.is.J6LNj65UjWJSjoDPjwBpigBQHgx=_

Then I realized that the password and tried using it. Seems like it was not it. Then I went to the second file def6a1d8dd8f0f79a36bae077b2ed568b863d5b806914925bce839a285b1ed97 file and as soon as I saw = I realized it was base64 file and cat it to name it differently and decoded the base64 file. I then changed it to a pdf. I ran into an issue when converting it to pdf, so I cat it to a file as soon as I decode it. I used

(base) Prashant Challenge1 \$ base64 -D -i

def6a1d8dd8f0f79a36bae077b2ed568b863d5b806914925bce839a285b1ed97 -o challenge.pdf

Then the challenge.pdf gave me a Table with Value Char pair. After consulting with my teammates I tried decrypting the J6LNj65UjWJSjoDPjwBpigBQHgx=_ file.

And referenced to the table for char value and used the value of char,

J → 29

6 → 6

L → 33

N → 37

j → 28

6 → 6

5 → 5

U → 51

j → 28

W → 55

J → 29

S → 47

j → 28

o → 38

D → 17

P → 41

j → 28

w → 54

B → 13

p → 40

i → 26

g → 22

B → 13

Q → 43

H → 25

g → 22

x → 56

= → padding

_ → invalid / not in this table

And then I converted it to the binary

011101 000110 100001 100101 011100 000110 000101 110011

011100 110111 011101 101111 011100 100110 010001 101001

011100 110110 001101 101000 011010 010110 001101 101011

011001 010110 111000

and then I consulted with chatgpt for converting it to the text and I got the answer

“thepasswordischicken” which is then used to unlock the pdf. After that point I used the text in the PDF and used the hint given at bottom to convert it to atbash. After converting it to atbash I

got the string of “myxqbkdevkdsyxc. iye qyd dy dro oxn yp drsc fobi cswzvo mrkvvoxqo.” which I then used the Caesar cipher algorithm, which I got from the hint of salad.

<https://www.dcode.fr/caesar-cipher>

I used this website to brute force it.

After brute forcing after 16 rotations I got like a readable string of “congratulations. you got to the end of this very simple challenge.” and I completed the challenge.