

Cryptography Challenges

Table of Contents:

Fencing On Rails_1	2
Challenge	2
Hints	2
Desu Yo_1	2
Challenge	2
Hints	2
RSA Starter	3
Challenge	3
Hints	

Fencing On Rails_1

Difficulty: Easy

Challenge

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: `i1is_i4nfikr5c{3t}r_`

Hints

- Encryption Script - Present in the challenge folder
- [Rail Fence Cipher](#)
- Surely one Rail conductor doesn't need so many instructors.

Desu Yo_1

Difficulty: Medium

Challenge

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\xf8\x9e\xfc\x61\x3b\x28\x35\x80\x17\x4c\x65\x87
```

Hints

- [DES](#)
- [Encryption Script](#)
- [Weak Keys](#)

RSA Starter

Difficulty: Medium

Challenge

Can you crack this revolutionary asymmetric encryption system?

cipher.txt:

```
n =
108479011759769393727176308457457051185868202028229648190
667018102389154815514421272511788818630907941383004277918
921724359698326811100798212287777156373854025160462416970
207713010402684330377900249272920821196418994434689542195
444008546643909734553918562196237000260811736016995830450
094506601223180883688118367193617732939585810720318219660
211710733808215174048484794731011578459721161876052257146
687991978315725043744813520691467819521825409725421924282
740640715767718923851036438509804069110541415248000720606
907056103122751808376882405235966768597369796819161915929
329975604623470108492326664937
```

e = 65537

```
c =
551940464039515807400740396933190659698814517552103157901
302208116485553487364559020139846605613149677875893049327
855581027728335881582761046428020476566023624654782900712
169848486370004204828767889948118481368286540519002718573
820758931364175489610814327584860219679731591039865372364
938280683799713345159073364944139930644621928548202326427
313765214415870574993875784555928599639790323118534133481
181510897922279319456483547168066234333710914250446053028
136246154089708758959859848480779884155548880428742408536
741330376562260935284789773921284976881026919766133271053
1585774180052484876172501963
```

Hints

- [RSA cryptosystem](#).
- Convert the digits to alphabets.