telnet is a terminal execution program 🡪 used to access remote servers

**Teletype Network**

Developed in 1969 and were used without encryption

ssh is an good alternative

**wep**

if device and the roueter have the key

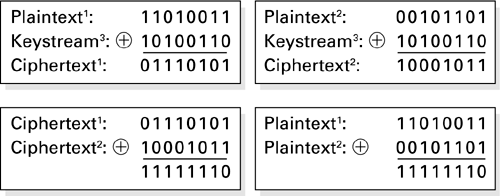
device side

* Initializing vector (random 24bit number) is produce
  + This is done so that every packet has unique key (password) to decrypt it
* Now **IV + KEY (password) ->** using **RC4** -> converted to as key called **keystream**
  + Iv + key is also known as seed
  + Iv + key = seed (64/128 bit)
  + Seed is converted to keystream using rc4 algo
* Keystream + “data to send to the router” = encrypted data
  + Data is encryoted using simple xor function
  + Keystream X **xor** X data = encryptedData
* Now packet is send to the router
* The packet contains
  + IV (initialization vector)
    - **IV** is added to the packet because AP only have the preshared key (password)
    - Ap cannot simply decrypt the package using only the key because the packet’s encryption key (keystream) is based on a random number (**IV**)
    - So router gets this random number from the packet, generate the **keystream** (encryption key)
      * **IV + key 🡪 using RC4 🡪 keystream**
      * **Use key stream to decrypt data**
      * **Keystream . XOR . encrypteddata = decrypteddata**
  + Ecrypted data

CONS

As the IV can be repeated , so when the iv rpeated we will get two cipher text with the same iV

We know xoring two cypher text with the same iv = xoring two plain text



So if we know

1 plain text ->(manually sent by us)

And 2 cypher text

We can extract the keystream and decrypt the message

* Now we have
  + Iv
  + Keystream
  + Encryptedtext
  + Decryptedtext
* We know iv + key (**seed**) 🡪 rc4 🡪 keystream