PART 1
AES and Wi-Fi Authentication Crack

1. AES encryption
    - Steps (https://legacy.cryptool.org/en/cto/aes-step-by-step)
        1. Choose default AES-128 configuration, 10 rounds, none chaining
        2. Fill in 128 key

    - Observations:
        - input of round 1 is similar to the key, input of plaintext is completely different
        - Difference between last round and the rest- in round 10, there's no "after mult", meaning that it only has 3 steps in that round. The rest of the rounds have 4 steps to it

Initial Vector (CBC only)

Key

2b7e1516 28aed2a6 abf71588 09cf4f3c

Expanded Key

2b7e1516 28aed2a6 abf71588 09cf4f3c a0fafe17 88542cb1 23a33939 2a6c7605 f2c295f2 7a96b943
5935807a 7359f67f 3d80477d 4716fe3e 1e237e44 6d7a883b ef44a541 a8525b7f b671253b db0bad00
d4d1c6f8 7c839d87 caf2b8bc 11f915bc 6d88a37a 110b3efd dbf98641 ca0093fd 4e54f70e 5f5fc9f3
84a64fb2 4ea6dc4f ead27321 b58dbad2 312bf560 7f8d292f ac7766f3 19fadc21 28d12941 575c006e
d014f9a8 c9ee2589 e13f0cc8 b6630ca6

Input

00000101 03030707 0f0f1f1f 3f3f7f7f

Encoding Rounds

Round 1

input to Round 1

2b7e1417 2badd5a1 a4f80a97 36f03043

after S-Box: ON

f1f3faf0 f1950332 49416788 058c041a

after permutation: ON

f195671a f14104f0 498cfa32 05f30388

after mult: ON

207384ce ce8fb3b6 d56d7cc9 8f7573f4

used subkey:

a0fafe17 88542cb1 23a33939 2a6c7605

after mix with key: ON

80897ad9 46db9f07 f6ce45f0 a51905f1

Round 9

input to Round 9

`b7e887ec 5505110f c2a3fce1 c58fc869`

after S-Box: ON

`a99b17ce fc6b8276 250ab0f8 a673e8f9`

after permutation: ON

`a96bb0f9 fc0ae8ce 25731776 a69b82f8`

after mult: ON

`bd4da9d2 db05747a be8ce2e7 9bee3103`

used subkey:

`ac7766f3 19fadc21 28d12941 575c006e`

after mix with key: ON

`113acf21 c2ffa85b 965dcba6 ccb2316d`

Round 10

input to Round 10

`113acf21 c2ffa85b 965dcba6 ccb2316d`

after S-Box: ON

`82808afd 2516c239 904c1f24 4b37c73c`

after permutation: ON

`82161f3c 254cc7fd 90378a39 4b80c224`

used subkey:

`d014f9a8 c9ee2589 e13f0cc8 b6630ca6`

after mix with key: ON

`5202e694 eca2e274 710886f1 fde3ce82`

Encoded

`5202e694 eca2e274 710886f1 fde3ce82`

Decoding Rounds

Round 10

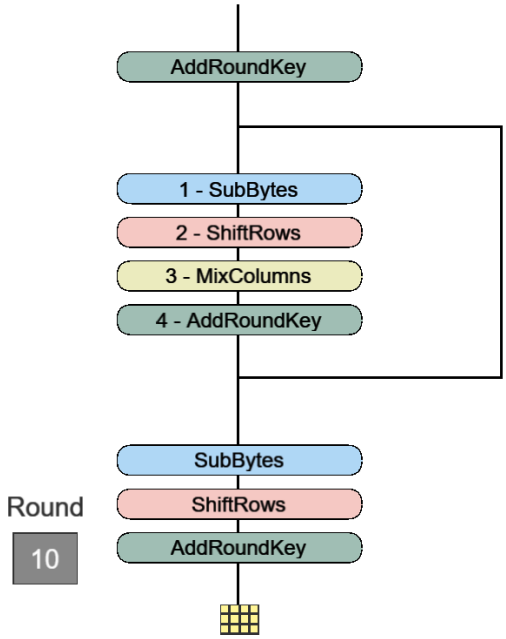
input to Round 10
82161f3c 254cc7fd 90378a39 4b80c224
after permutation: ON
82808afd 2516c239 904c1f24 4b37c73c
after S-Box: ON
113acf21 c2ffa85b 965dcba6 ccb2316d
used subkey:
ac7766f3 19fadc21 28d12941 575c006e
after mix with key: ON
bd4da9d2 db05747a be8ce2e7 9bee3103
after mult: ON
a96bb0f9 fc0ae8ce 25731776 a69b82f8

AES Encryption Visualisation

- Steps (https://www.cryptool.org/en/cto/aes-animation)
    1. Fill in same 128 bit key

- Observations:
    - Extra roundkey added before first round
    - 1-9 rounds have 4 steps
    - Round 10 only has 3 steps

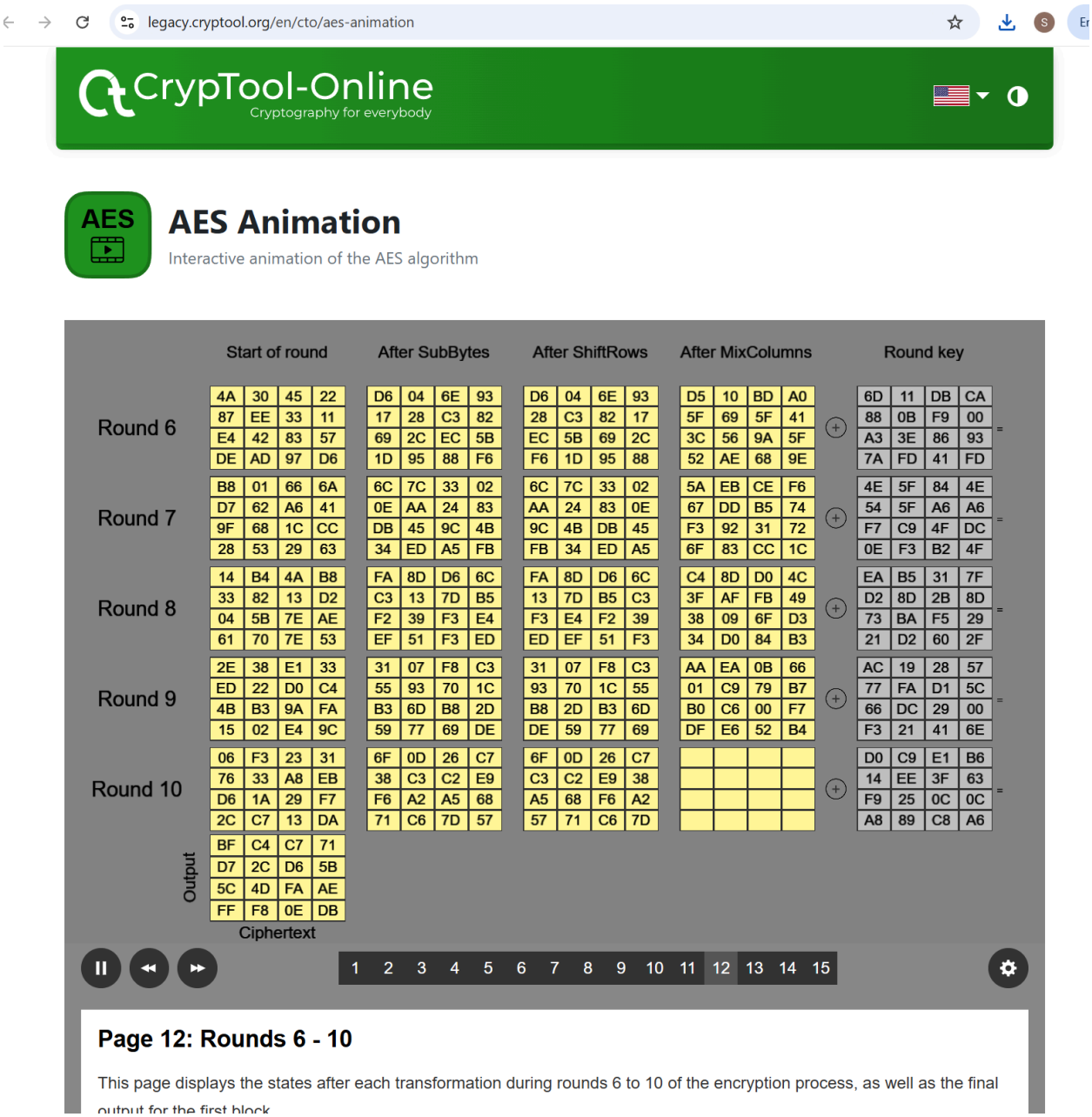
Encryption Process



initial round

9 main rounds

final round



PART 2
WIFI Authentication Crack

- Uses multiple parts of the IEEE 802 protocol family, designed to interwork with Ethernet
- Connecting to a WIFI network, user needs network name (SSID) and password
    - Password encrypts WIFI packets

- Wired Equivalent Privacy (WEP)
    - Security algorithm for IEEE 802.11 wireless networks
    - Provides data confidentiality
    - Replaced by WIFI protected access (WPA)

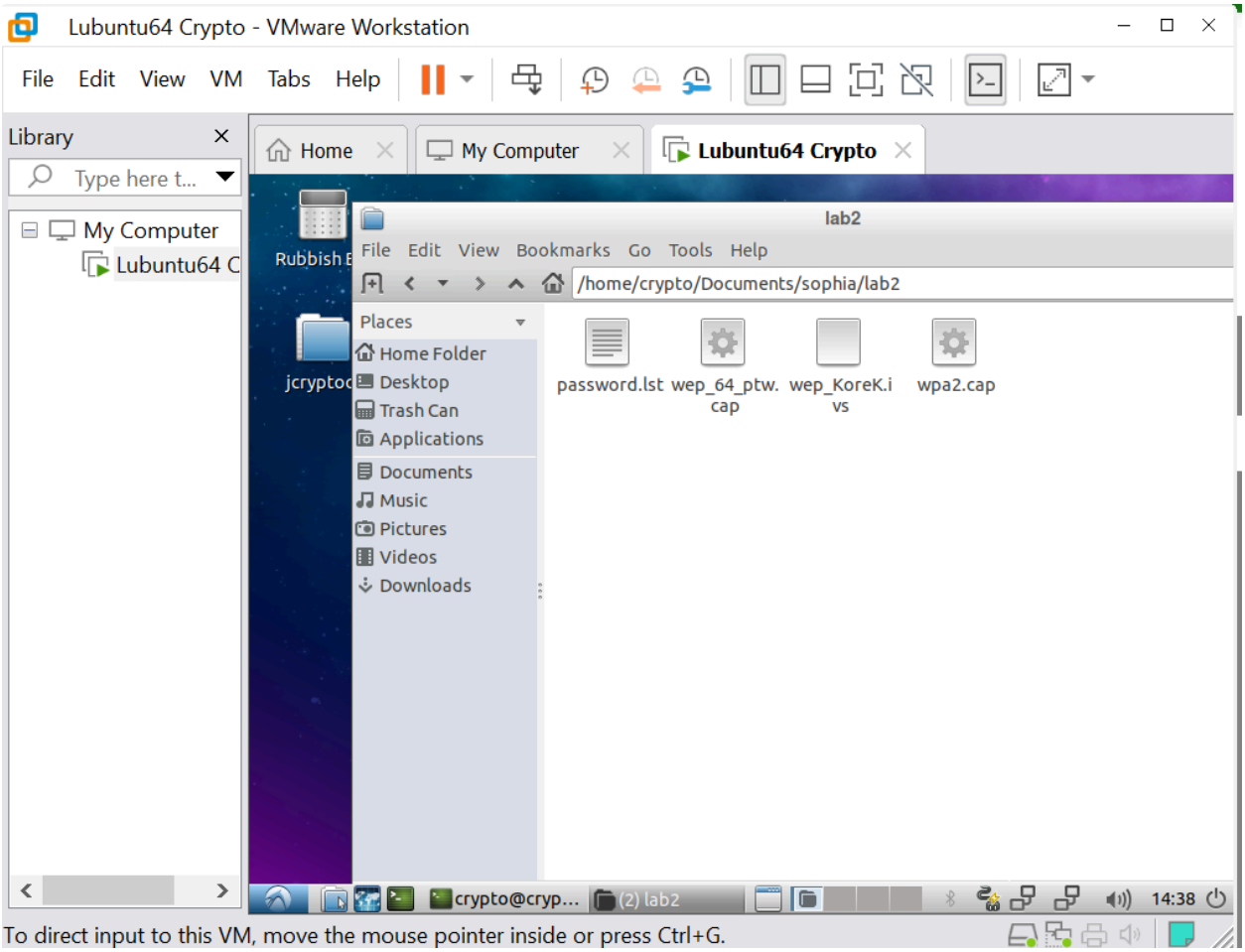
- WPA
    - Security certification program to secure wireless networks
    - WPA3 most recent

- Aircrack-NG
    - Tools to assess WIFI network security
        - Monitoring- packet capture, export of data
        - Attacking- replaying attacks, deauthentication, fake access points
        - Testing- checking WIFI cards and driver capabilities (Capture and injection)
        - Cracking- WEP and WPA PSK(WPA 1 and 2)

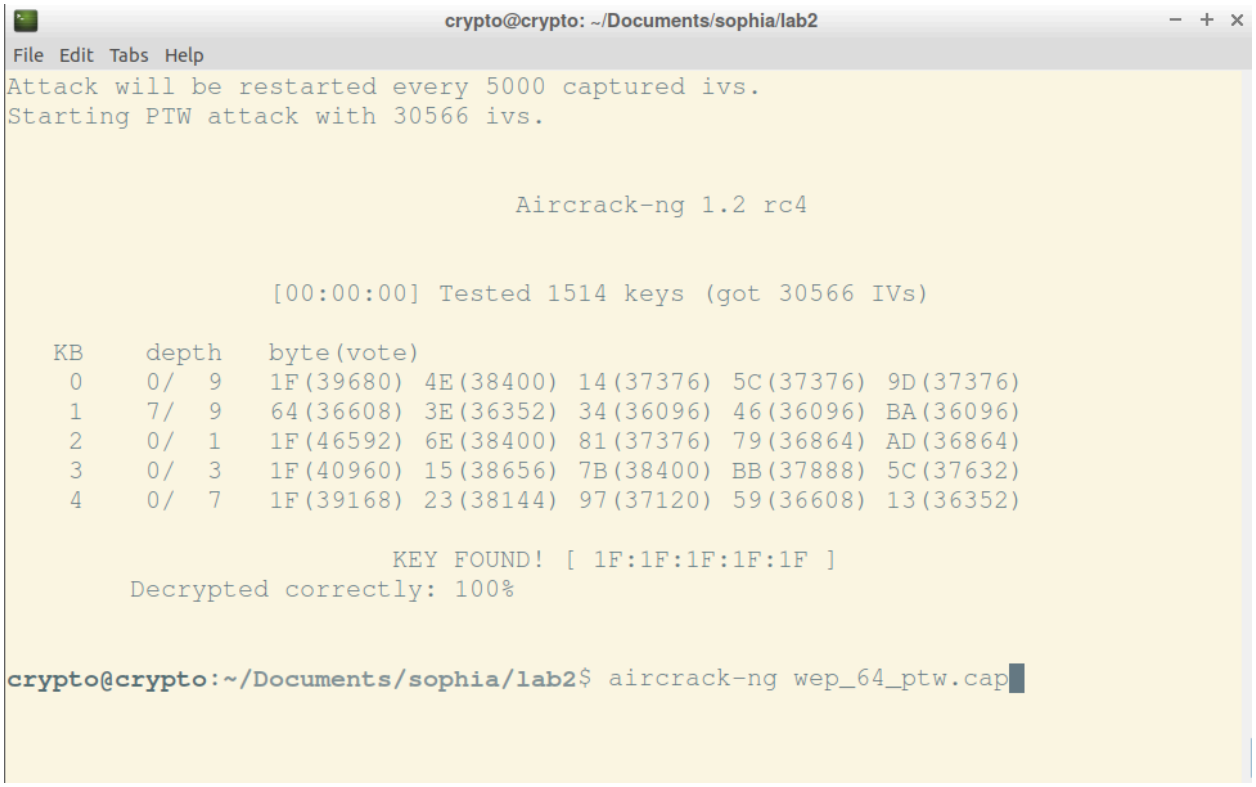
WEP Crack

- Aircrack-ng recovers WEP key once enough encrypted packets have been captured
    - First method:
        - PTW (Pyshkin, Tews, Weinmann)
    - Second method:
        - FMS/KoreK- incorporates statistical attacks to discover the WEP key, uses these in combination instead of brute forcing (requires more packets, but can recover the passphrase instead of failing)

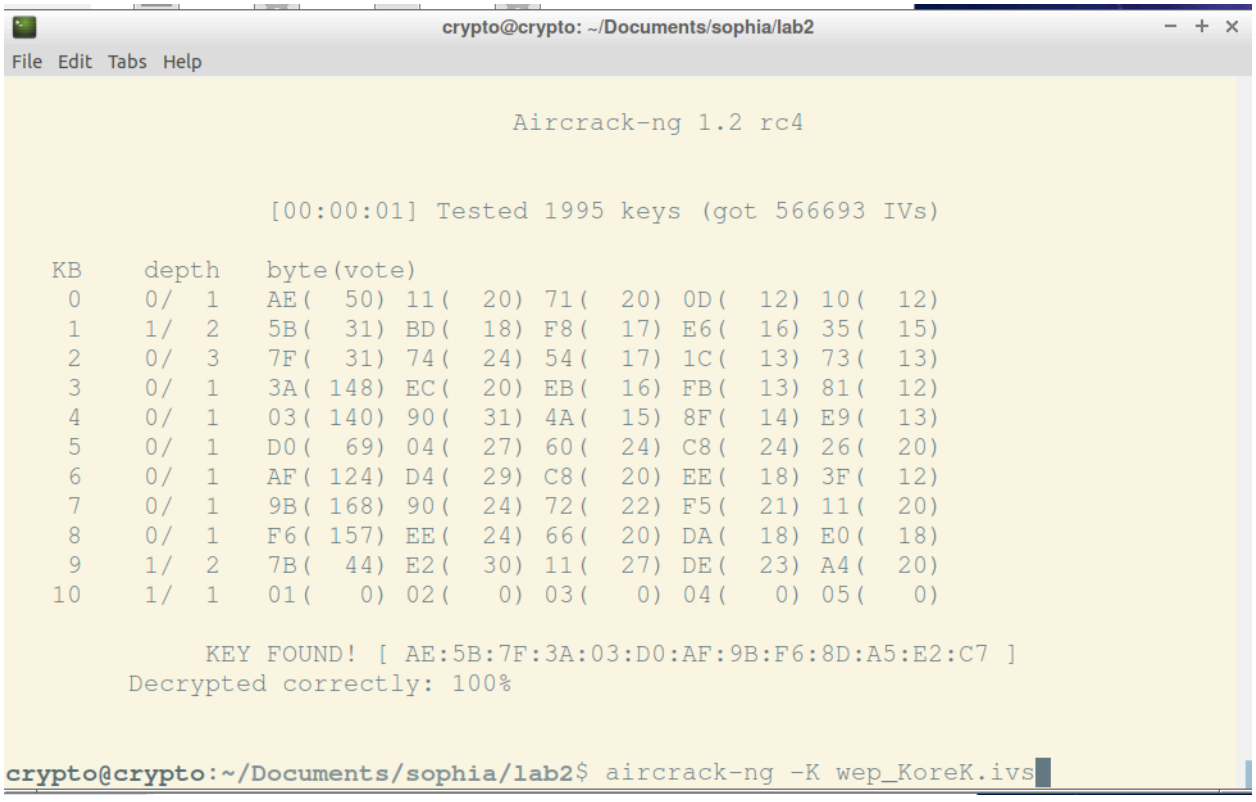
- Copying and pasting files



- Cracking WEP password using PTW mode



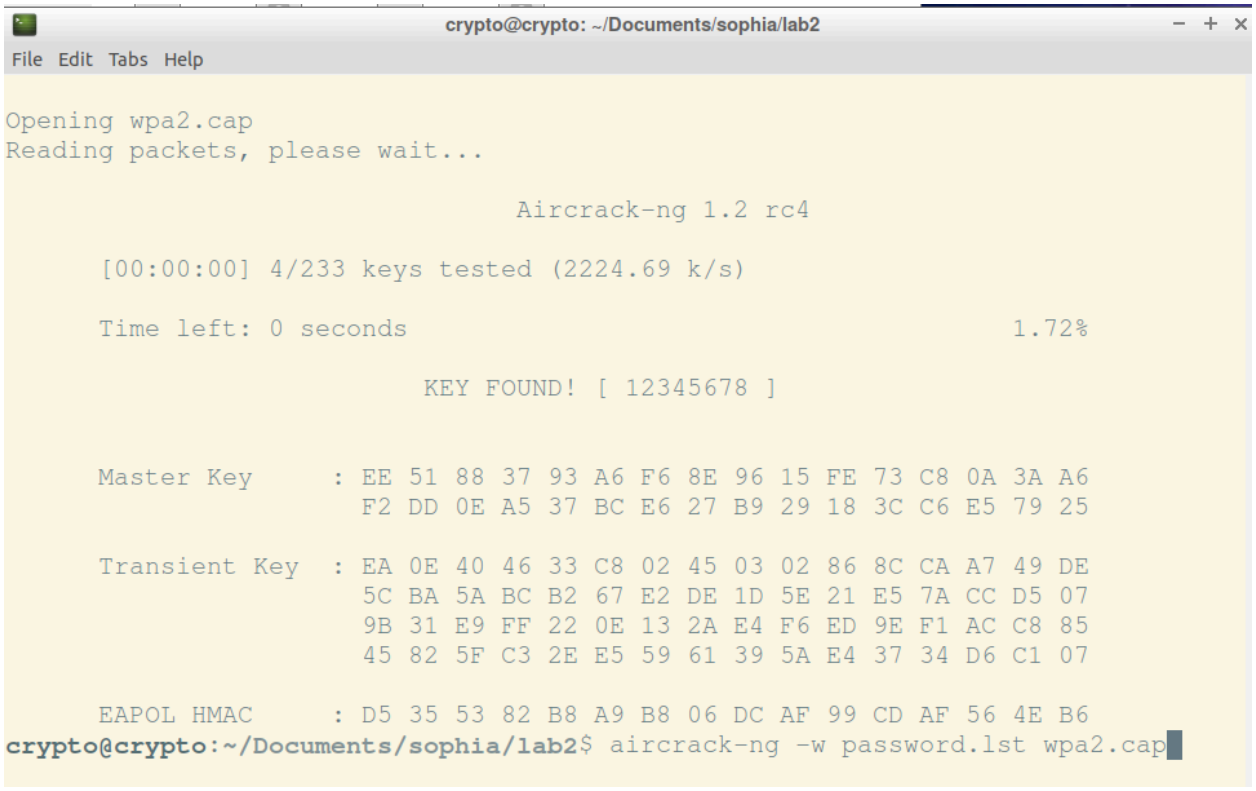
- Cracking WEP password using Korek



WPA2 crack

- WPA handshake composed of four packets

- Cracking WPA2 password using bruteforce



WPA3

- Released 2018

- Q1: What is the vulnerability of WPA2 Personal?
    - Weak passwords- relies on pre-shared key (PSK) to authenticate, passwords can be easily brute forced if it's weak
    - Doesn't provide forward secrecy- if attacker can access the network they can can analyse the traffic and decrypt it to obtain PSK

- Q2: How does WPA3 solve WPA2 shortcomings?
    - Simultaneous authentication of equals (SAE)
        - Instead of using PSK, SAE is a secure key exchange protocol that makes WPA3 resistant to offline dictionary attacks (attacker can't brute force password)
        - Uses 4-way handshake, ensures that key installation can't be exploited by attackers
        - Has forward secrecy- attackers can't decrypt traffic network (session keys unique for each session)
        - OWE- enhanced open, encrypts open networks

        - 128- bit minimum security- more bits, more security

- Q3: Are there any possible attacks against WPA3?
    - Devices being forced to be downgraded into WPA2
    - Side channel attacks- attackers extracting info through power consumption analysis