# Gaining Access

## WEP Cracking

- Wired Equivalent Privacy
- Old encryption.
- Uses an algorithm called RC4.
- Still used in some networks.
- Can be cracked easily.

WEP

# WEP Cracking

- Client encrypts data using a key.
- Encrypted packet sent in the air.
- Router decrypts packet using the key.

# WEP Cracking

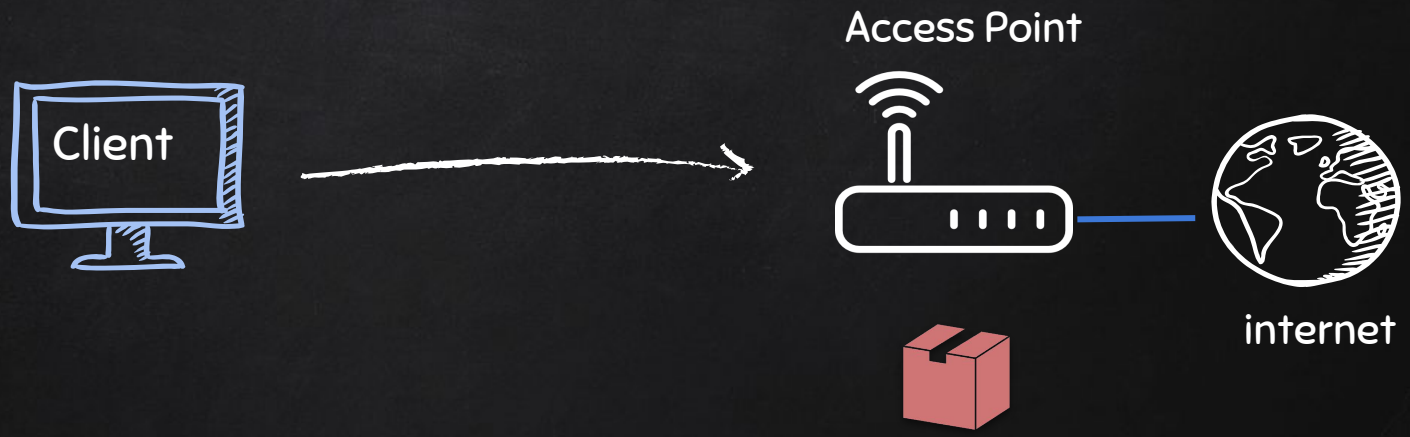
- Client encrypts data using a key.
- Encrypted packet sent in the air.
- Router decrypts packet using the key.

# WEP Cracking

- Client encrypts data using a key.
- Encrypted packet sent in the air.
- Router decrypts packet using the key.

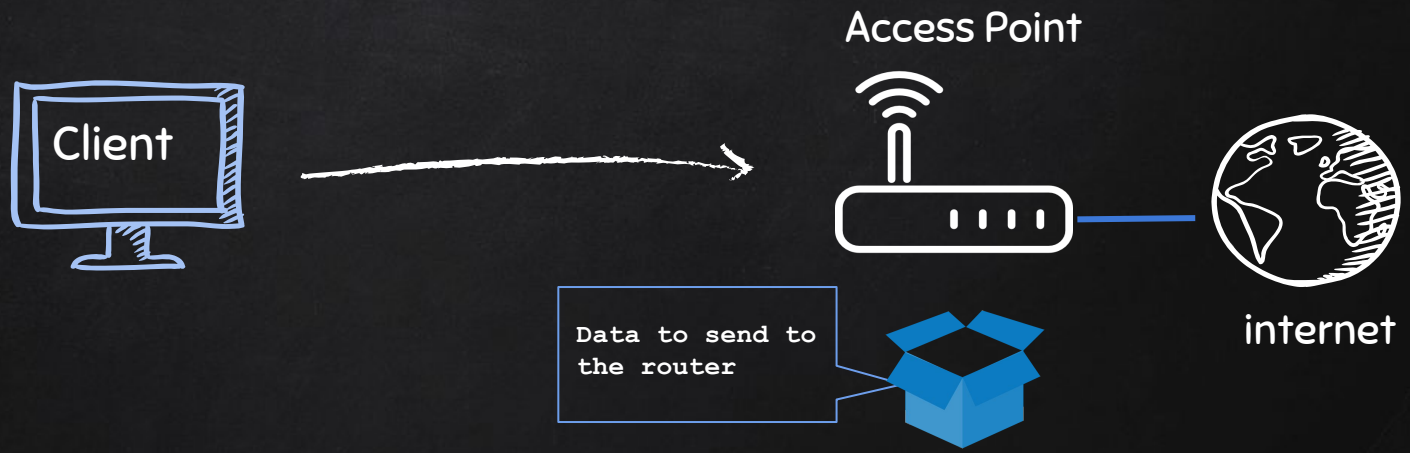
# WEP Cracking

- Client encrypts data using a key.
- Encrypted packet sent in the air.
- Router decrypts packet using the key.



# WEP Cracking

- Client encrypts data using a key.
- Encrypted packet sent in the air.
- Router decrypts packet using the key.



# WEP Cracking

- Each packet is encrypted using a unique key stream.
- Random initialization vector (IV) is used to generate the keys streams.
- The initialization vector is only 24 bits!
- IV + Key (password) = Key stream.

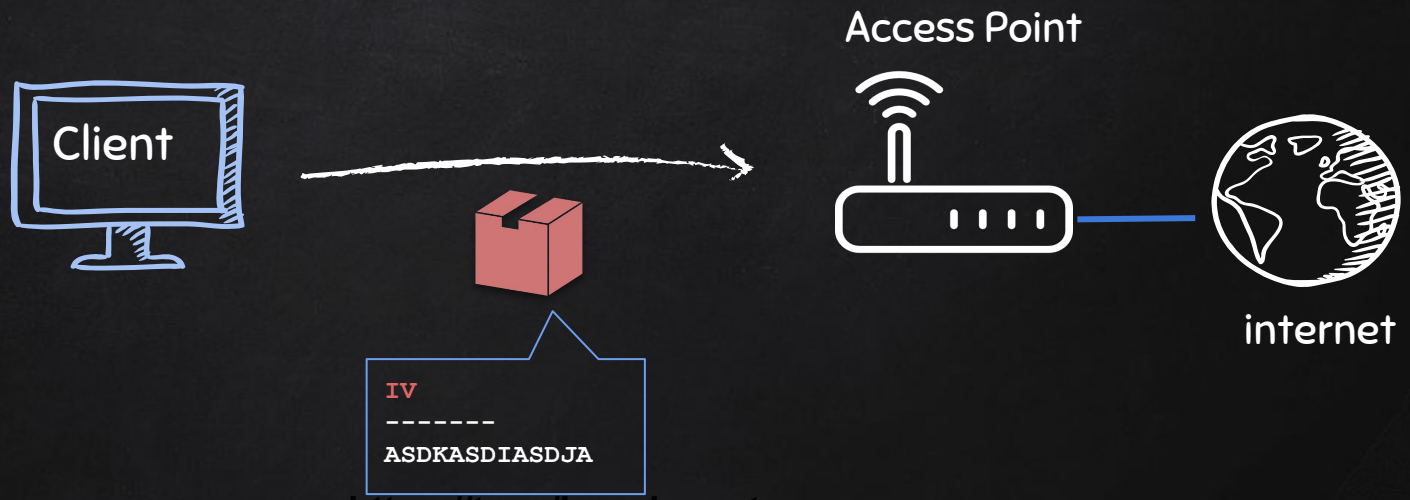
# WEP Cracking

- Each packet is encrypted using a unique key stream.
- Random initialization vector (IV) is used to generate the keys streams.
- The initialization vector is only 24 bits!
- IV + Key (password) = Key stream.


Keystream + "Data to send to the router" = ASDKASDIASDJA

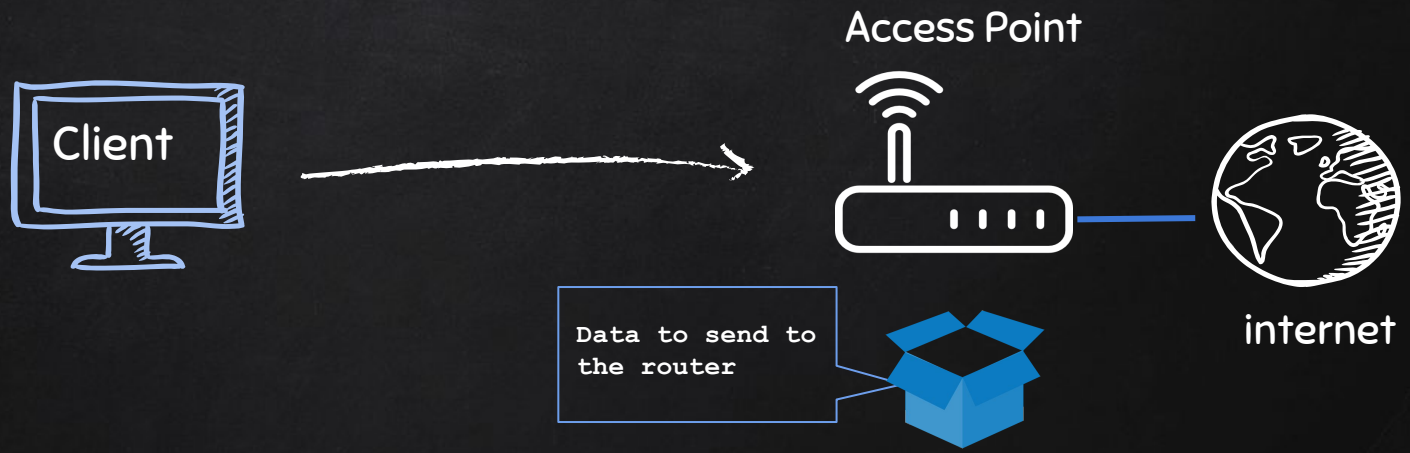
# WEP Cracking

- Each packet is encrypted using a unique key stream.
- Random initialization vector (IV) is used to generate the keys streams.
- The initialization vector is only 24 bits!
- IV + Key (password) = Key stream.



# WEP Cracking

- Client encrypts data using a key.
- Encrypted packet sent in the air.
- Router decrypts packet using the key.



# WEP Cracking

- IV is too small (only 24 bits).
- IV is sent in plain text.

Result:

- IV's will repeat on busy networks.
- This makes WEP vulnerable to statistical attacks.
- Repeated IVs can be used to determine the key stream;
- And break the encryption

WEP

# WEP Cracking

Conclusion:

To crack WEP we need to:

1. Capture a large number of packets/IVs.
2. Analyse the captured IVs and crack the key.

WEP

# WEP Cracking

Conclusion:

To crack WEP we need to:

1. Capture a large number of packets/IVs. → using airodump-ng
2. Analyse the captured IVs and crack the key. → using aircrack-ng

WEP

# WEP Cracking

Problem:

- If network is not busy.
- It would take some time to capture enough IVs.

Solution:

→ Force the AP to generate new IVs.

WEP

# WEP Cracking

## Fake Authentication

Problem:

- APs only communicate with connected clients.

→ We can't communicate with it.

→ We can't even start the attack.

Solution:

→ Associate with the AP before launching the attack.

WEP

# WEP Cracking

## ARP Request Replay

- Wait for an ARP packet.
- Capture it, and replay it (retransmit it).
- This causes the AP to produce another packet with a new IV.
- Keep doing this till we have enough IVs to crack the key.

WEP

# WPA / WPA2 Cracking

- Both can be cracked using the same methods
- Made to address the issues in WEP.
- Much more secure.
- Each packet is encrypted using a unique temporary key.

→ Packets contain no useful information.

WPA/WPA2

# WPA / WPA2 Cracking

## Exploiting WPS

- WPS is a feature that can be used with WPA & WPA2.
- Allows clients to connect without the password.
- Authentication is done using an 8 digit pin.
  - 8 Digits is very small.
  - We can try all possible pins in relatively short time.
  - Then the WPS pin can be used to compute the actual password.

PS: This only works if the router is configured not to use PBC (Push Button Authentication).

WPA/WPA2

# WPA / WPA2 Cracking

- Fixed all weaknesses in WEP.
- Packets contain no useful data.
- Only packets that can aid with the cracking process are the handshake packets.
  - These are 4 packets sent when a client connects to the network.

WPA/WPA2

# WPA / WPA2 Cracking

- The handshake does not contain data the helps recover the key.
- It contains data that can be used to check weather a key is valid or not.

Handshake

# Creating a Wordlist

Crunch can be used to create a wordlist.

Syntax:

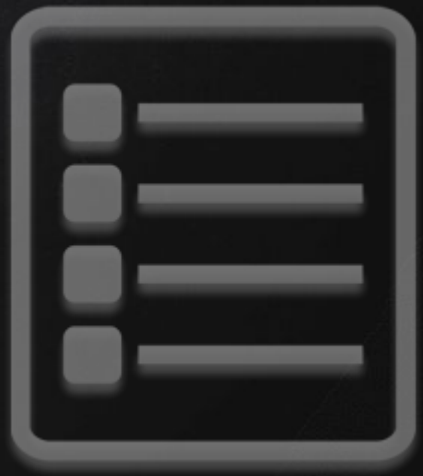
> crunch [min] [max] [characters] -t [pattern] -o [FileName]

Example:

> crunch 6 8 123abc$ -i wordlist -t a@@@@b

Generated passes:

aaaaab
aabbbb
aan$$b
.....



# WPA / WPA2 Cracking

Two things needed to crack WPA/WPA2 :

1. 4-way handshake.
2. Wordlist.

| 123456789 |
| --- |
| qwertyqwerty |
| football |
| iloveyou |
| abc123abc |

Wordlist

Handshake

# WPA / WPA2 Cracking

| 123456789 |
| --- |
| qwertyqwerty |
| football |
| iloveyou |
| abc123abc |

Wordlist

SP Address
STA Address
AP Nonce
STA Nonce
EAPOL
Payload

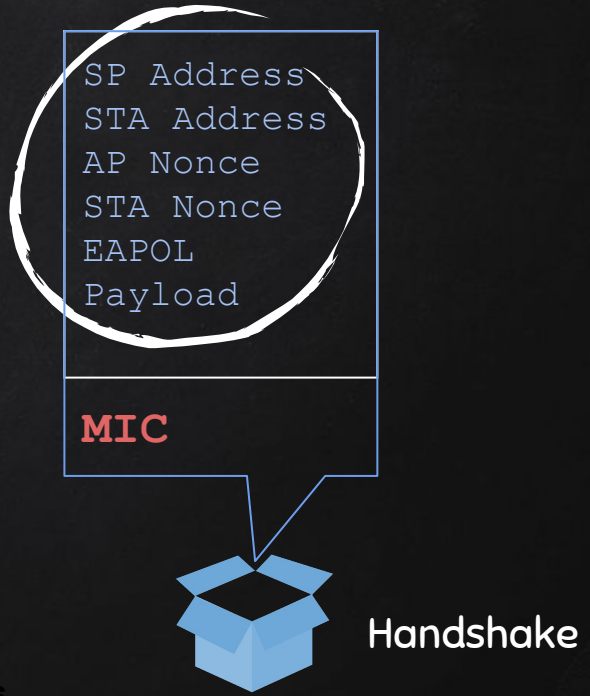
**MIC**

Handshake

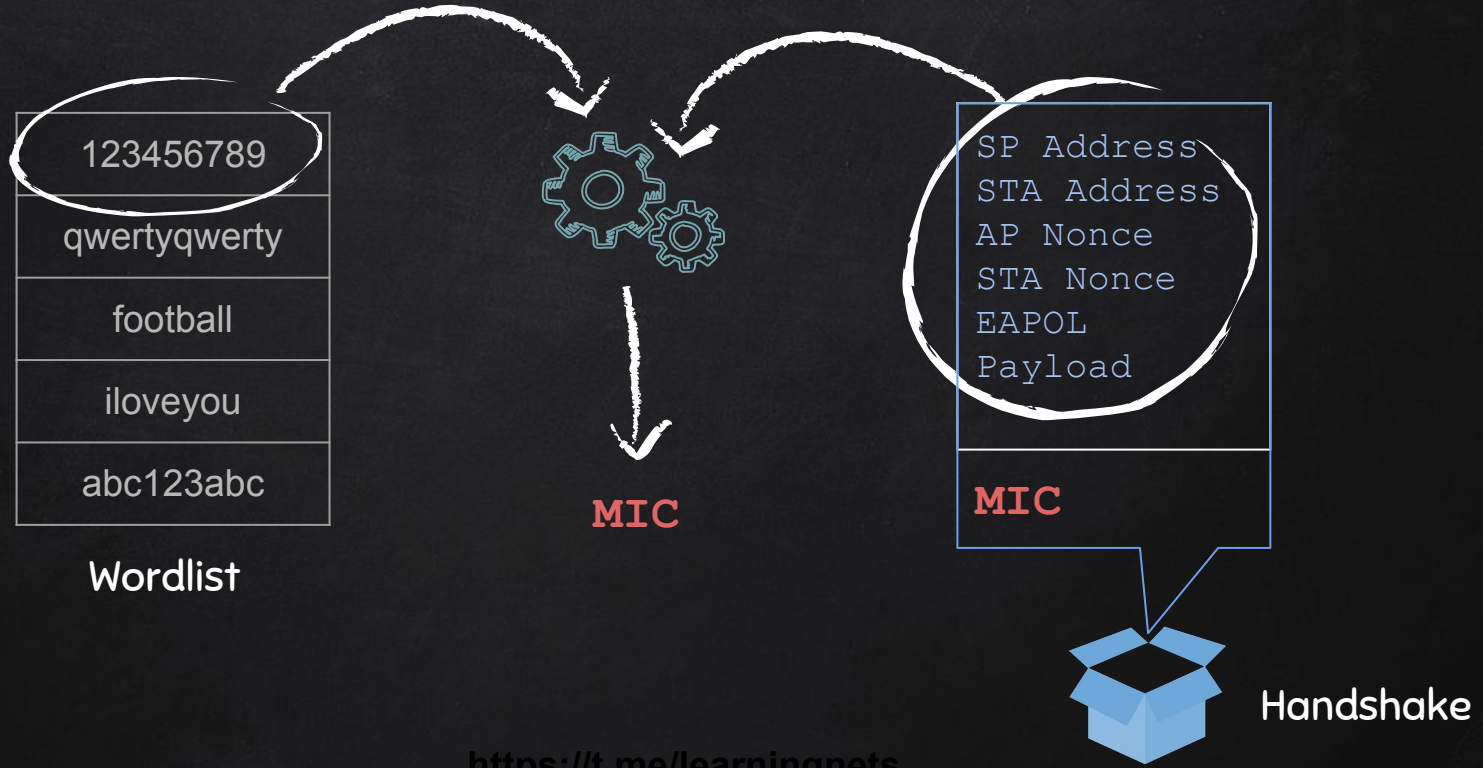
# WPA / WPA2 Cracking

| 123456789 |
| --- |
| qwertyqwerty |
| football |
| iloveyou |
| abc123abc |

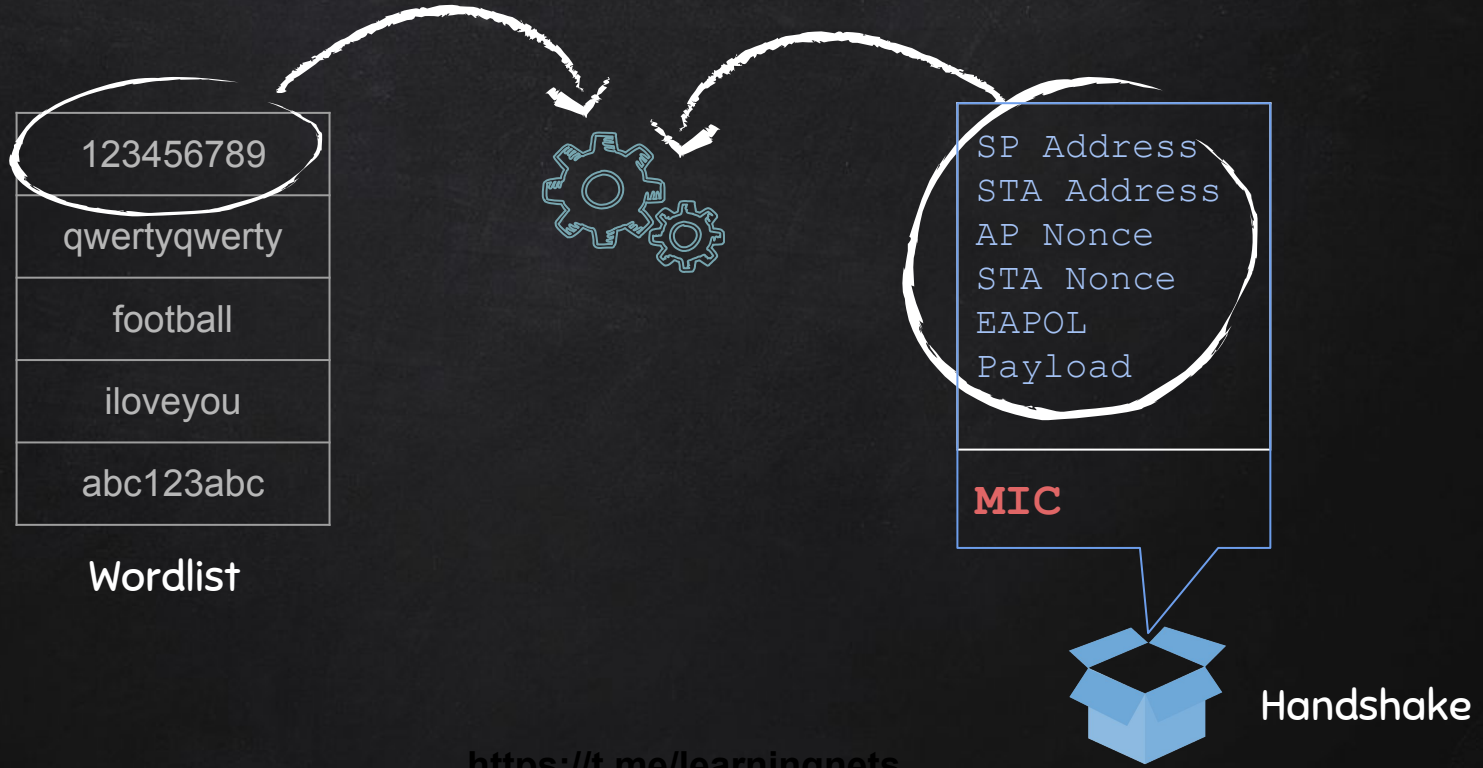
Wordlist



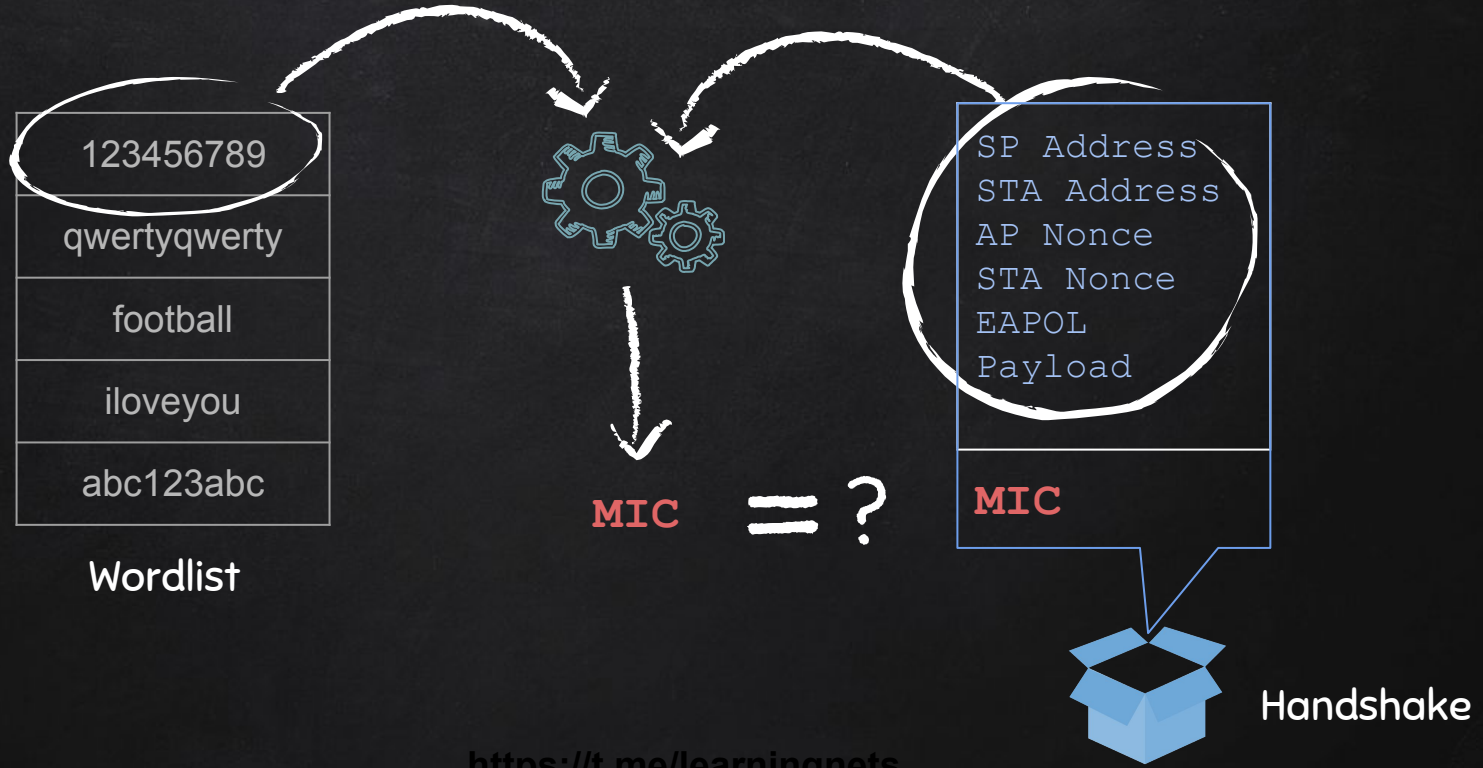
# WPA / WPA2 Cracking



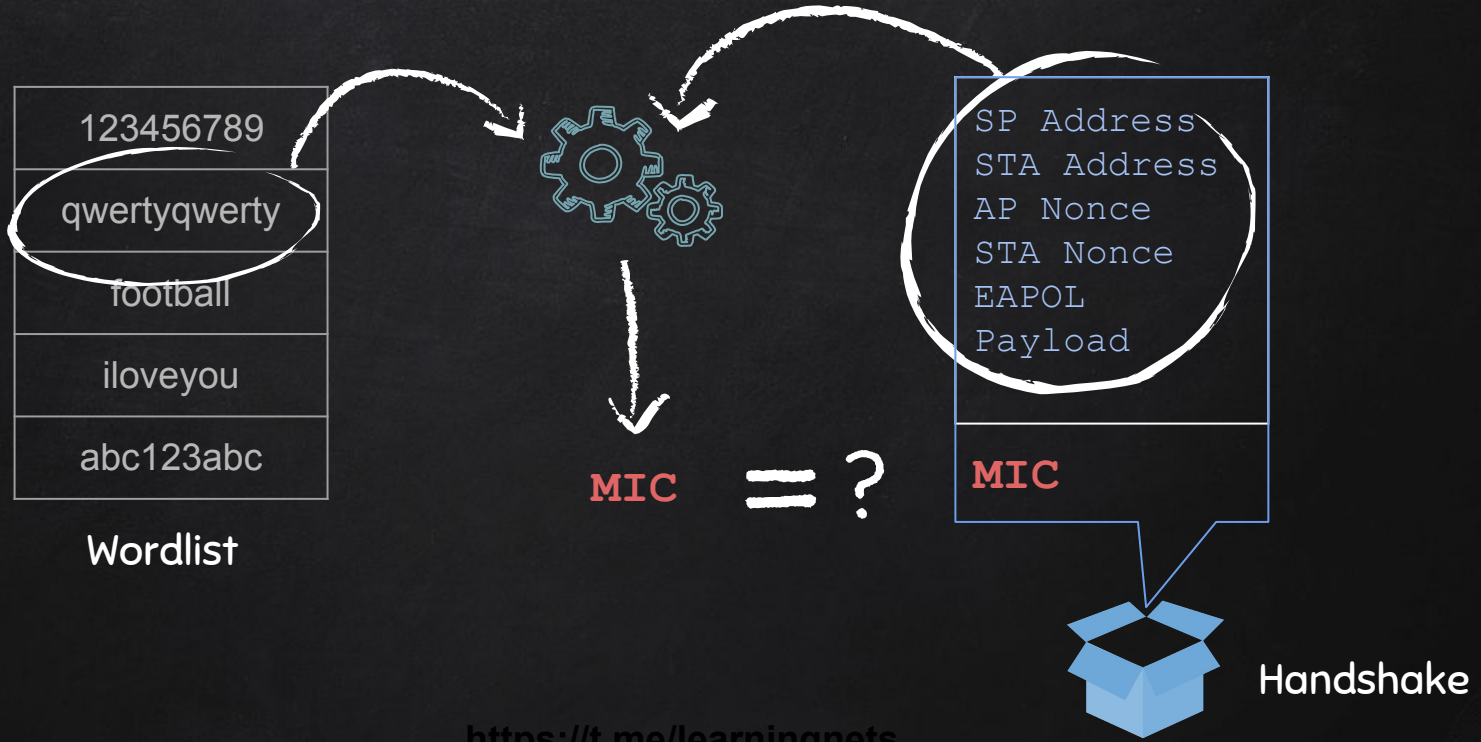
# WPA / WPA2 Cracking



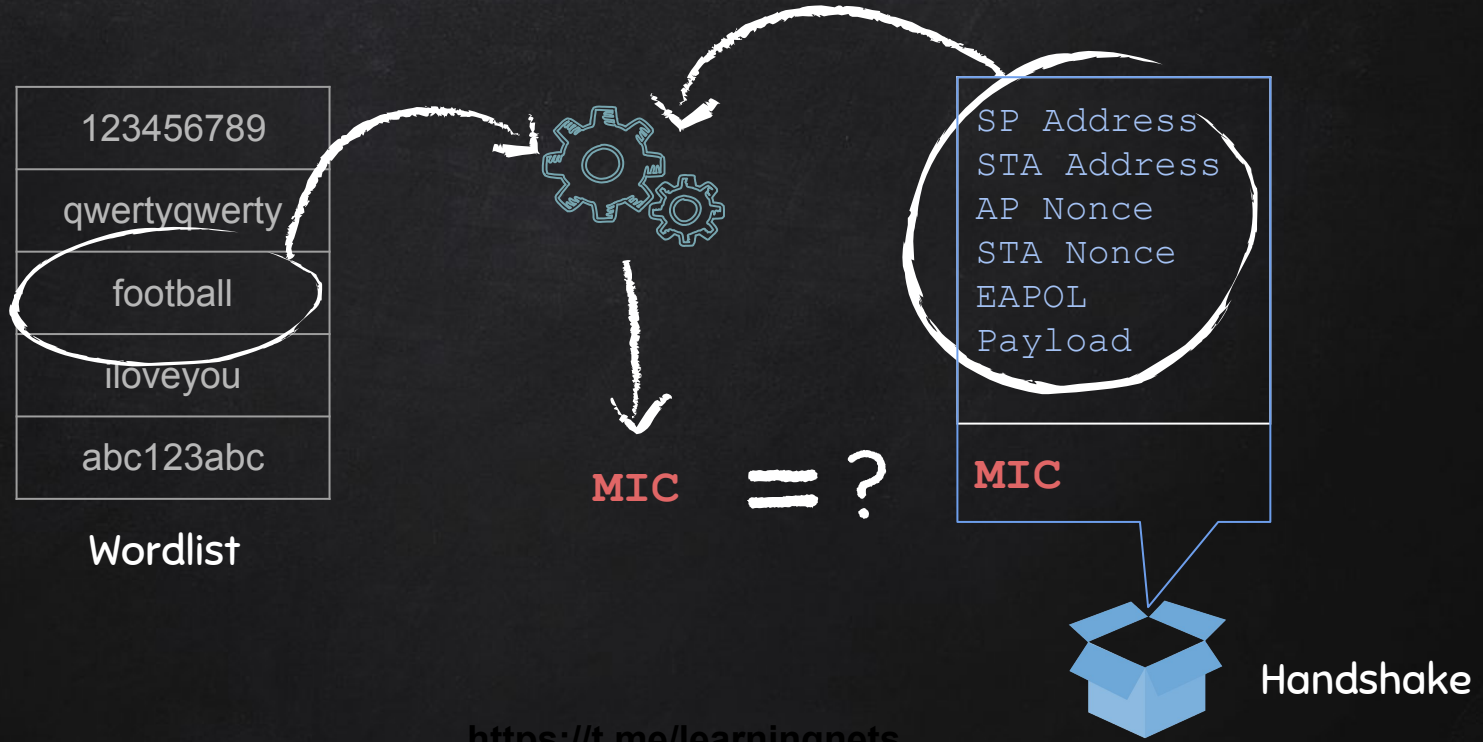
# WPA / WPA2 Cracking



# WPA / WPA2 Cracking



# WPA / WPA2 Cracking



# WPA / WPA2 Cracking