AES and Wi-Fi Authentication Crack

OVERVIEW

There are two parts in this lab: AES (Step-by-step) and Wi-Fi (WEP and WPA2) authentication crack.

The step-by-step AES visualises the data manipulations in the AES algorithm. In this lab, you will watch an animation about AES details and then go through the AES algorithm with your input and observe the output of each step.

This Wi-Fi authentication crack lab conducts cracking on the cryptographic process in the Wi-Fi authentication. With this lab, the keys in WEP and WPA2 authentication processes will be cracked with Aircrack-ng. This lab shows typical threats on cryptography, i.e., weak encryption, incorrect usage, and brute-force attack.

You need to take screenshots of key steps and answer questions for your lab report. For the weekly lab, you can discuss with your group. However, you need to prepare your report with your own screenshots. You have one week to prepare your report. Please submit your report to Canvas.

Part One: Step by Step AES

In this part, we will go through the AES step-by-step using the CrypTool-Online.

1 A STEP-BY-STEP AES ENCRYPTION

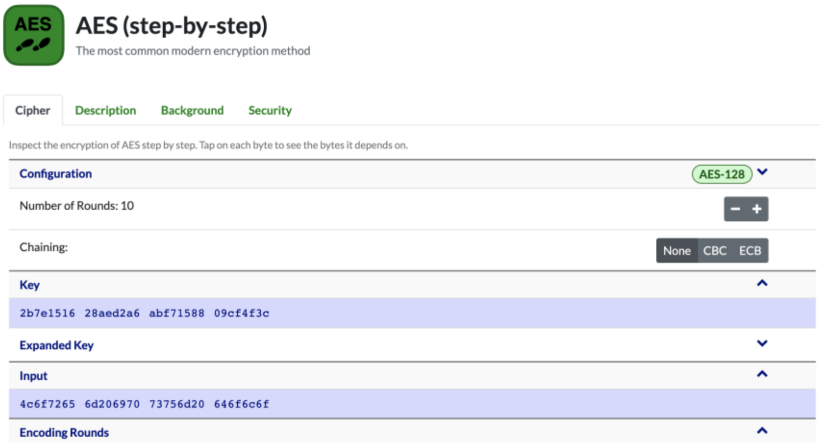
s1. Open https://www.cryptool.org/en/cto/aes-step-by-step,

s2. Choose default AES-128 configuration, 10 rounds, and None Chaining.

s3. Fill in your own 128bit (32 Hex) key and input.

One example is as follows

Part two is based on https://www.aircrack-ng.org/doku.php?id=aircrack-ng



AES (step-by-step)

The most common modern encryption method

Inspect the encryption of AES step by step. Tap on each byte to see the bytes it depends on.

Configuration AES-128

Number of Rounds: 10

Chaining: None CBC ECB

Key

```
2b7e1516  28aed2a6  abf71588  09cf4f3c
```

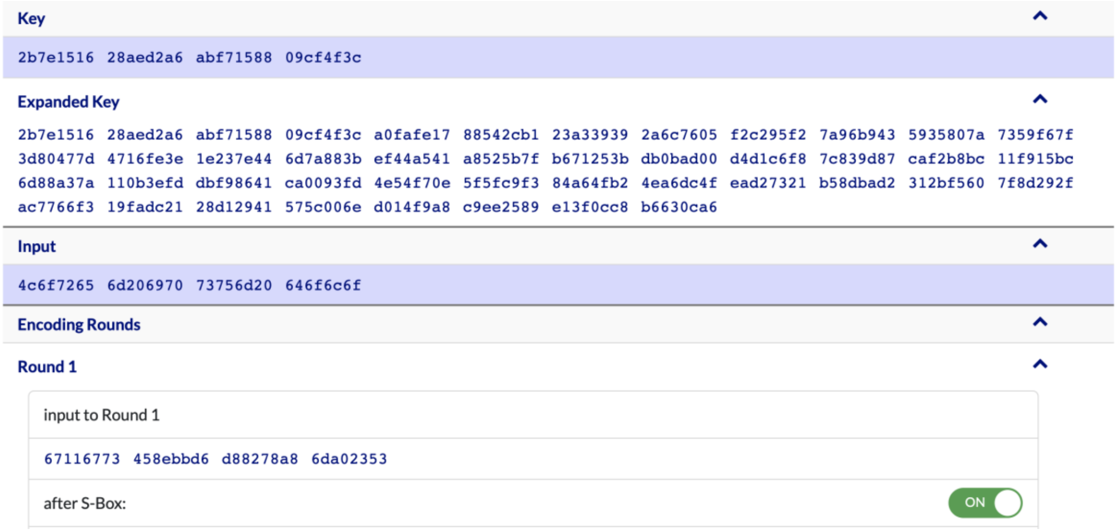
Expanded Key

Input

```
4c6f7265  6d206970  73756d20  646f6c6f
```

Encoding Rounds

s4. Compare the input to Round 1 and the input plaintext.



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

```
4c6f7265  6d206970  73756d20  646f6c6f
```

Encoding Rounds

Round 1

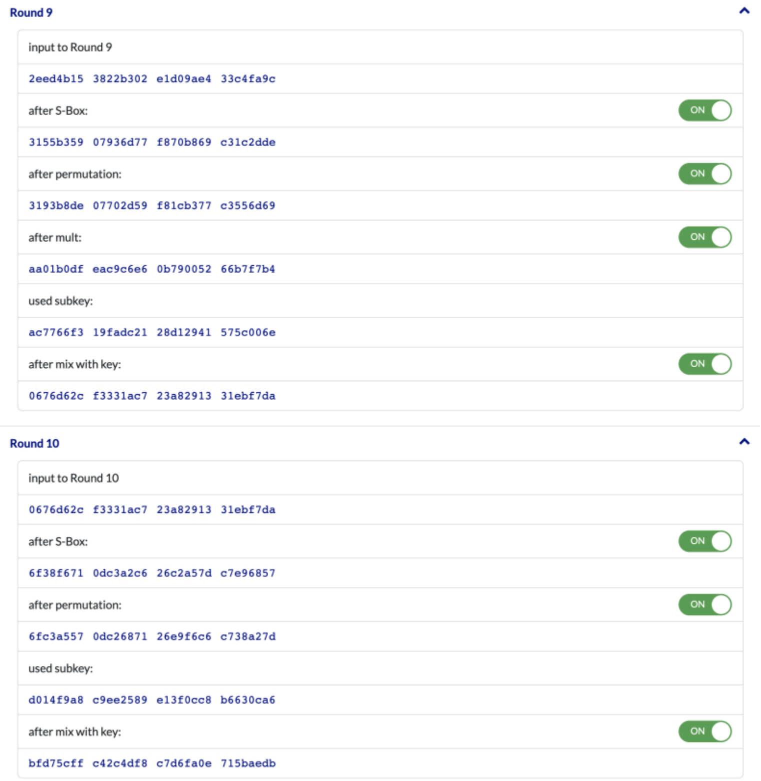
input to Round 1

```
67116773  458ebbd6  d88278a8  6da02353
```

after S-Box: ON

s5. Compare the operations in all rounds and identify the difference between the last round and the others.

Part two is based on https://www.aircrack-ng.org/doku.php?id=aircrack-ng



Round 9

input to Round 9

2eed4b15 3822b302 e1d09ae4 33c4fa9c

after S-Box: ON

3155b359 07936d77 f870b869 c31c2dde

after permutation: ON

3193b8de 07702d59 f81cb377 c3556d69

after mult: ON

aa01b0df eac9c6e6 0b790052 66b7f7b4

used subkey:

ac7766f3 19fadc21 28d12941 575c006e

after mix with key: ON

0676d62c f3331ac7 23a82913 31ebf7da

Round 10

input to Round 10

0676d62c f3331ac7 23a82913 31ebf7da

after S-Box: ON

6f38f671 0dc3a2c6 26c2a57d c7e96857

after permutation: ON

6fc3a557 0dc26871 26e9f6c6 c738a27d

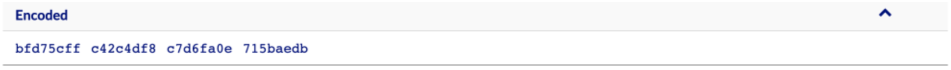
used subkey:

d014f9a8 c9ee2589 e13f0cc8 b6630ca6

after mix with key: ON

bfd75cff c42c4df8 c7d6fa0e 715baedb

s6. Note down the encoded output.



Encoded

bfd75cff c42c4df8 c7d6fa0e 715baedb

s7. Go through the decoding rounds by yourself.

2 An AES encryption Visualisation

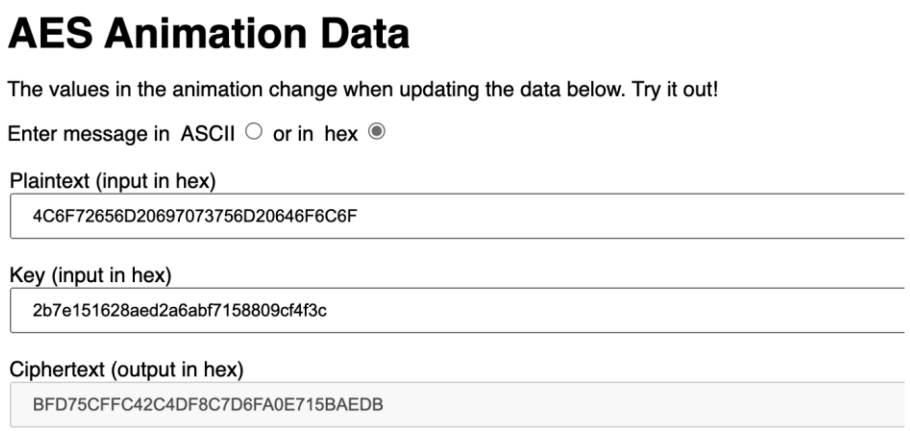
In this task, we will visualise AES Encryption algorithm and explain how the intermedia results are obtained.

s1. Open https://www.cryptool.org/en/cto/aes-animation

s2. Fill in your own 128bit (32 Hex) key and input (same as the last task).

My example is as follows

Part two is based on https://www.aircrack-ng.org/doku.php?id=aircrack-ng



AES Animation Data

The values in the animation change when updating the data below. Try it out!

Enter message in ASCII ○ or in hex ●

Plaintext (input in hex)

4C6F72656D20697073756D20646F6C6F

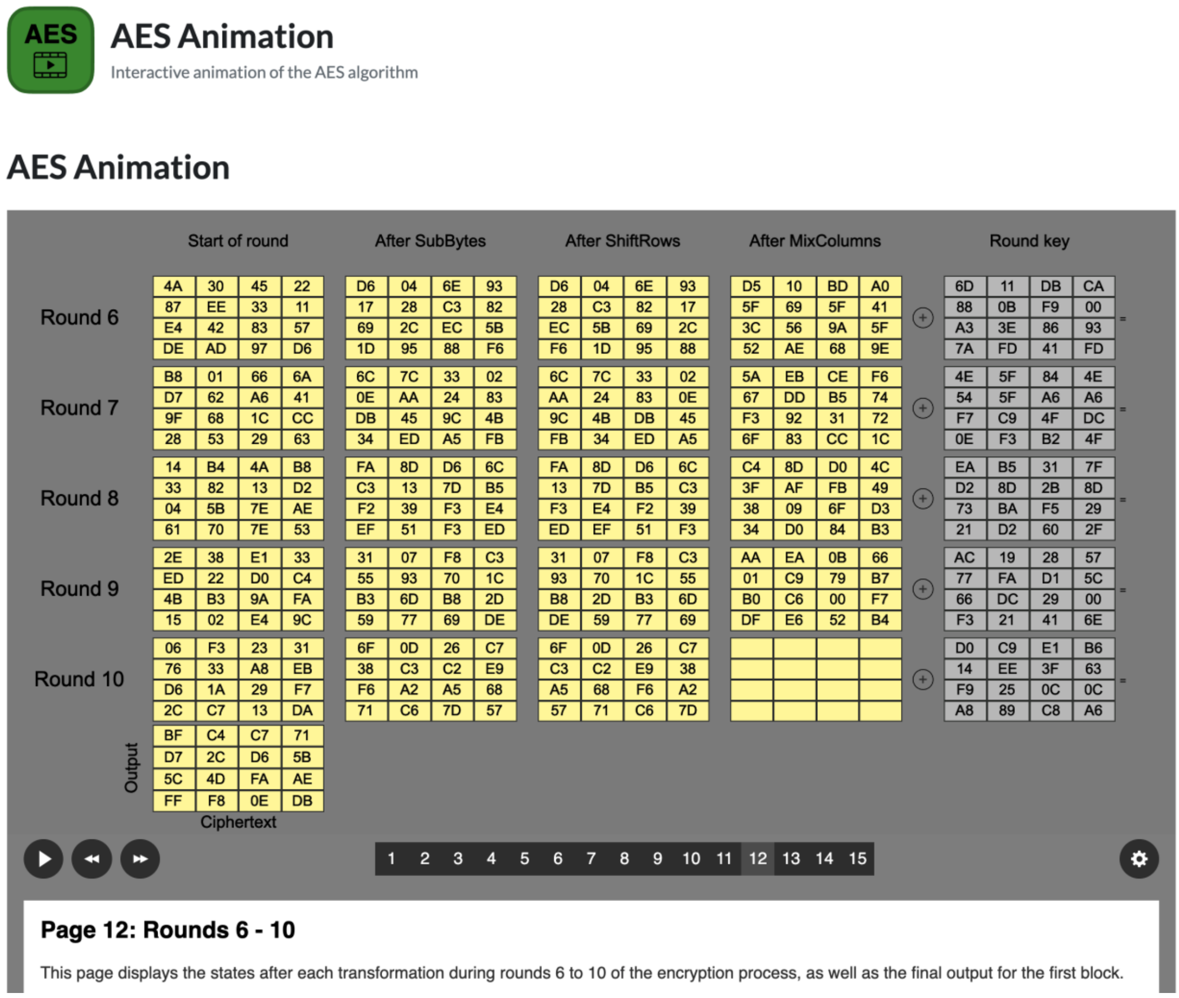
Key (input in hex)

2b7e151628aed2a6abf7158809cf4f3c

Ciphertext (output in hex)

BFD75CFFC42C4DF8C7D6FA0E715BAEDB

s3. Click the play button to play the animation and compare the numbers with the intermedia values in the last task.



AES Animation

Interactive animation of the AES algorithm

AES Animation

	Start of round	After SubBytes	After ShiftRows	After MixColumns		Round key	
Round 6	4A 30 45 22	D6 04 6E 93	D6 04 6E 93	D5 10 BD A0	⊕	6D 11 DB CA	=
	87 EE 33 11	17 28 C3 82	28 C3 82 17	5F 69 5F 41		88 0B F9 00	
	E4 42 83 57	69 2C EC 5B	EC 5B 69 2C	3C 56 9A 5F		A3 3E 86 93	
	DE AD 97 D6	1D 95 88 F6	F6 1D 95 88	52 AE 68 9E		7A FD 41 FD	
Round 7	B8 01 66 6A	6C 7C 33 02	6C 7C 33 02	5A EB CE F6	⊕	4E 5F 84 4E	=
	D7 62 A6 41	0E AA 24 83	AA 24 83 0E	67 DD B5 74		54 5F A6 A6	
	9F 68 1C CC	DB 45 9C 4B	9C 4B DB 45	F3 92 31 72		F7 C9 4F DC	
	28 53 29 63	34 ED A5 FB	FB 34 ED A5	6F 83 CC 1C		0E F3 B2 4F	
Round 8	14 B4 4A B8	FA 8D D6 6C	FA 8D D6 6C	C4 8D D0 4C	⊕	EA B5 31 7F	=
	33 82 13 D2	C3 13 7D B5	13 7D B5 C3	3F AF FB 49		D2 8D 2B 8D	
	04 5B 7E AE	F2 39 F3 E4	F3 E4 F2 39	38 09 6F D3		73 BA F5 29	
	61 70 7E 53	EF 51 F3 ED	ED EF 51 F3	34 D0 84 B3		21 D2 60 2F	
Round 9	2E 38 E1 33	31 07 F8 C3	31 07 F8 C3	AA EA 0B 66	⊕	AC 19 28 57	=
	ED 22 D0 C4	55 93 70 1C	93 70 1C 55	01 C9 79 B7		77 FA D1 5C	
	4B B3 9A FA	B3 6D B8 2D	B8 2D B3 6D	B0 C6 00 F7		66 DC 29 00	
	15 02 E4 9C	59 77 69 DE	DE 59 77 69	DF E6 52 B4		F3 21 41 6E	
Round 10	06 F3 23 31	6F 0D 26 C7	6F 0D 26 C7		⊕	D0 C9 E1 B6	=
	76 33 A8 EB	38 C3 C2 E9	C3 C2 E9 38			14 EE 3F 63	
	D6 1A 29 F7	F6 A2 A5 68	A5 68 F6 A2			F9 25 0C 0C	
	2C C7 13 DA	71 C6 7D 57	57 71 C6 7D			A8 89 C8 A6	
Output	BF C4 C7 71						
	D7 2C D6 5B						
	5C 4D FA AE						
	FF F8 0E DB						
	Ciphertext						

Page 12: Rounds 6 - 10

This page displays the states after each transformation during rounds 6 to 10 of the encryption process, as well as the final output for the first block.

Part two is based on https://www.aircrack-ng.org/doku.php?id=aircrack-ng

Part Two: Wi-Fi Authentication Crack

1 PRELIMINARIES

1.1 Wi-Fi

Wi-Fi uses multiple parts of the IEEE 802 protocol family and is designed to interwork seamlessly with its wired sibling Ethernet. Compatible devices can network through wireless access points to each other as well as to wired devices and the Internet. The different versions of Wi-Fi are specified by various IEEE 802.11 protocol standards, with the different radio technologies determining radio bands, and the maximum ranges, and speeds that may be achieved. Wi-Fi is potentially more vulnerable to attack than wired networks because anyone within range of a network with a wireless network interface controller can attempt access. To connect to a Wi-Fi network, a user typically needs the network name (the SSID) and a password. The password is used to encrypt Wi-Fi packets to block eavesdroppers.

1.2 WEP

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in 1997, its intention was to provide data confidentiality comparable to that of a traditional wired network. In 2003 the Wi-Fi Alliance announced that WEP had been superseded by Wi-Fi Protected Access (WPA).

WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity. Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5,000 packets.

1.3 WPA/WPA2

Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2), and Wi-Fi Protected Access 3 (WPA3) are three security and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). There are some security issues, such as weak password, lack of forward secrecy and WPS PIN recovery.

1.4 WPA3

Part two is based on https://www.aircrack-ng.org/doku.php?id=aircrack-ng

In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2. Certification began in June 2018.

The new standard uses an equivalent 192-bit cryptographic strength in WPA3-Enterprise mode (AES-256 in GCM mode with SHA-384 as HMAC), and still mandates the use of CCMP-128 (AES-128 in CCM mode) as the minimum encryption algorithm in WPA3-Personal mode.

1.5 Aircrack-NG

Aircrack-ng is a complete suite of tools to assess Wi-Fi network security. It focuses on different areas of Wi-Fi security:

- Monitoring: Packet capture and export of data to text files for further processing by third party tools
- Attacking: Replay attacks, deauthentication, fake access points and others via packet injection
- Testing: Checking Wi-Fi cards and driver capabilities (capture and injection)
- Cracking: WEP and WPA PSK (WPA 1 and 2).

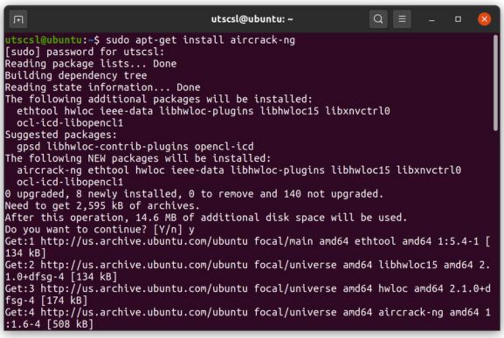
More information about Aircrack-NG can be found in https://www.aircrack-ng.org/

2 PREPARATION

2.1 Install Aircrack-NG

Install aircrack-ng with the following command

$ sudo apt-get install aircrack-ng

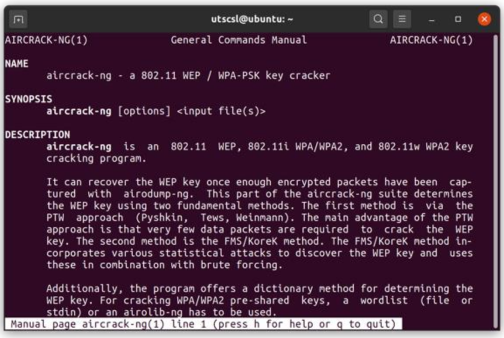


```
utscsl@ubuntu:~$ sudo apt-get install aircrack-ng
[sudo] password for utscsl:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ethtool hwloc ieee-data libhwloc-plugins libhwloc15 libxnvctrl0
  ocl-icd-libopencl1
Suggested packages:
  gpsd libhwloc-contrib-plugins opencl-icd
The following NEW packages will be installed:
  aircrack-ng ethtool hwloc ieee-data libhwloc-plugins libhwloc15 libxnvctrl0
  ocl-icd-libopencl1
0 upgraded, 8 newly installed, 0 to remove and 140 not upgraded.
Need to get 2,595 kB of archives.
After this operation, 14.6 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 ethtool amd64 1:5.4-1 [
134 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libhwloc15 amd64 2.
1.0+dfsg-4 [134 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 hwloc amd64 2.1.0+d
fsg-4 [174 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 aircrack-ng amd64 1
:1.6-4 [508 kB]
```

Check the manual page on the aircrack-ng with the following command

$ man aircrack-ng

Part two is based on https://www.aircrack-ng.org/doku.php?id=aircrack-ng



```
AIRCRACK-NG(1)           General Commands Manual          AIRCRACK-NG(1)

NAME
       aircrack-ng - a 802.11 WEP / WPA-PSK key cracker

SYNOPSIS
       aircrack-ng [options] <input file(s)>

DESCRIPTION
       aircrack-ng  is  an  802.11  WEP, 802.11i WPA/WPA2, and 802.11w WPA2 key
       cracking program.

       It can recover the WEP key once enough encrypted packets have been  cap-
       tured  with  airodump-ng.  This part of the aircrack-ng suite determines
       the WEP key using two fundamental methods. The first method is  via  the
       PTW  approach  (Pyshkin,  Tews, Weinmann). The main advantage of the PTW
       approach is that very few data packets are required  to  crack  the  WEP
       key. The second method is the FMS/KoreK method. The FMS/KoreK method in-
       corporates various statistical attacks to discover the WEP key and  uses
       these in combination with brute forcing.

       Additionally, the program offers a dictionary method for determining the
       WEP key. For cracking WPA/WPA2 pre-shared  keys,  a  wordlist  (file  or
       stdin) or an airolib-ng has to be used.
 Manual page aircrack-ng(1) line 1 (press h for help or q to quit)
```

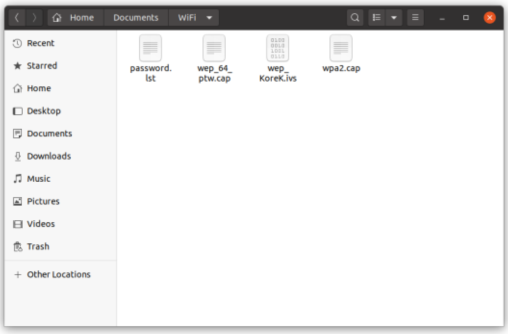
3 WEP Crack

3.1 Introduction

The simplest case is to crack a WEP key. Aircrack-ng can recover the WEP key once enough encrypted packets have been captured with airodump-ng. This part of the aircrack-ng suite determines the WEP key using two fundamental methods. The first method is via the PTW approach (Pyshkin, Tews, Weinmann). The default cracking method is PTW. The other, older method is the FMS/KoreK method. The FMS/KoreK method incorporates various statistical attacks to discover the WEP key and uses these in combination with brute forcing. It requires more packets than PTW, but on the other hand is able to recover the passphrase when PTW sometimes fail.

3.2 Preparing dump files

Copy the captured IVs and (i.e., wep_KoreK.ivs and wep_64_ptw.cap) to your working folder (indicating your name) on the virtual machine.



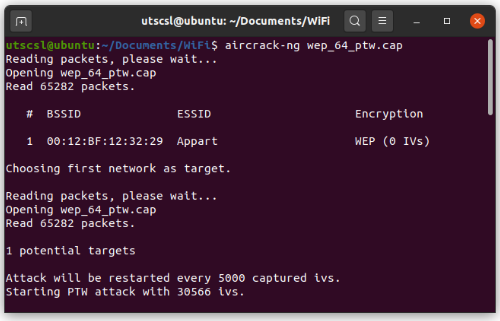
Part two is based on https://www.aircrack-ng.org/doku.php?id=aircrack-ng

3.3 Crack the WEP password

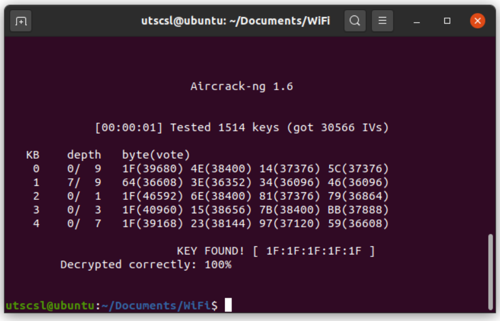
3.3.1 Crack the WEP password using the PTW mode with the command below

$ aircrack-ng wep_64_ptw.cap

You will get



```
utscsl@ubuntu:~/Documents/WiFi$ aircrack-ng wep_64_ptw.cap
Reading packets, please wait...
Opening wep_64_ptw.cap
Read 65282 packets.

   #  BSSID              ESSID                     Encryption

   1  00:12:BF:12:32:29  Appart                    WEP (0 IVs)

Choosing first network as target.

Reading packets, please wait...
Opening wep_64_ptw.cap
Read 65282 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 30566 ivs.
```



```
                           Aircrack-ng 1.6


                [00:00:01] Tested 1514 keys (got 30566 IVs)

   KB    depth   byte(vote)
    0    0/  9   1F(39680) 4E(38400) 14(37376) 5C(37376)
    1    7/  9   64(36608) 3E(36352) 34(36096) 46(36096)
    2    0/  1   1F(46592) 6E(38400) 81(37376) 79(36864)
    3    0/  3   1F(40960) 15(38656) 7B(38400) BB(37888)
    4    0/  7   1F(39168) 23(38144) 97(37120) 59(36608)

                     KEY FOUND! [ 1F:1F:1F:1F:1F ]
        Decrypted correctly: 100%


utscsl@ubuntu:~/Documents/WiFi$
```

The key is “1F:1F:1F:1F:1F”.

Take a screenshot of your result and attach the screenshot to your report.

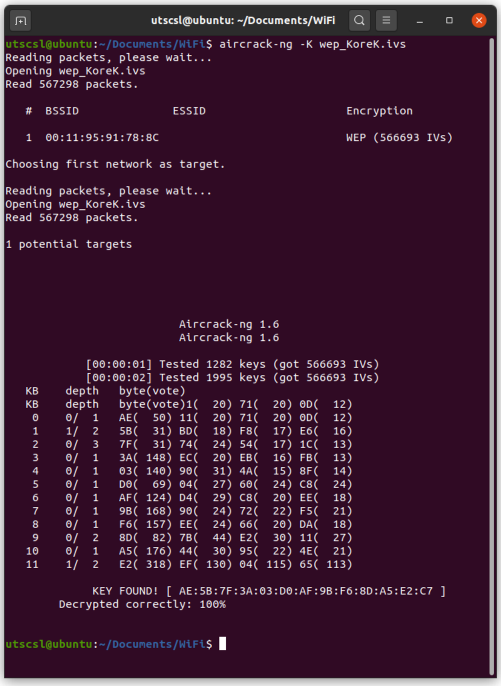
3.3.2 Crack the WEP password using the Korek mode with the command below

$ aircrack-ng -K wep_KoreK.ivs

-K: Use KoreK attacks only; wep_KoreK.ivs is the file name containing IVS.

You will get

Part two is based on https://www.aircrack-ng.org/doku.php?id=aircrack-ng



utscsl@ubuntu: ~/Documents/WiFi

```
utscsl@ubuntu:~/Documents/WiFi$ aircrack-ng -K wep_KoreK.ivs
Reading packets, please wait...
Opening wep_KoreK.ivs
Read 567298 packets.

   #  BSSID              ESSID                     Encryption

   1  00:11:95:91:78:8C                            WEP (566693 IVs)

Choosing first network as target.

Reading packets, please wait...
Opening wep_KoreK.ivs
Read 567298 packets.

1 potential targets





                          Aircrack-ng 1.6
                          Aircrack-ng 1.6

            [00:00:01] Tested 1282 keys (got 566693 IVs)
            [00:00:02] Tested 1995 keys (got 566693 IVs)
   KB    depth   byte(vote)
   KB    depth   byte(vote)1(  20) 71(  20) 0D(  12)
    0    0/  1   AE(  50) 11(  20) 71(  20) 0D(  12)
    1    1/  2   5B(  31) BD(  18) F8(  17) E6(  16)
    2    0/  3   7F(  31) 74(  24) 54(  17) 1C(  13)
    3    0/  1   3A( 148) EC(  20) EB(  16) FB(  13)
    4    0/  1   03( 140) 90(  31) 4A(  15) 8F(  14)
    5    0/  1   D0(  69) 04(  27) 60(  24) C8(  24)
    6    0/  1   AF( 124) D4(  29) C8(  20) EE(  18)
    7    0/  1   9B( 168) 90(  24) 72(  22) F5(  21)
    8    0/  1   F6( 157) EE(  24) 66(  20) DA(  18)
    9    0/  2   8D(  82) 7B(  44) E2(  30) 11(  27)
   10    0/  1   A5( 176) 44(  30) 95(  22) 4E(  21)
   11    1/  2   E2( 318) EF( 130) 04( 115) 65( 113)

             KEY FOUND! [ AE:5B:7F:3A:03:D0:AF:9B:F6:8D:A5:E2:C7 ]
        Decrypted correctly: 100%


utscsl@ubuntu:~/Documents/WiFi$ 
```

The key is "AE:5B:7F:3A:03:D0:AF:9B:F6:8D:A5:E2:C7".

Take a screenshot of your result and attach the screenshot to your report.

4 WPA2 CRACK

4.1 Introduction

For cracking WPA/WPA2 pre-shared keys, only a dictionary method is used. A "four-way handshake" is required as input. For WPA handshakes, a full handshake is composed of four packets. However, aircrack-ng is able to work successfully with just 2 packets. EAPOL packets (2 and 3) or packets (3 and 4) are considered a full handshake.

Note: handshake scheme can be found https://en.wikipedia.org/wiki/IEEE_802.11i-2004

4.2 Preparing the dump file and dictionary list

Copy the captured hand-shake file (i.e., wpa2.cap) and the dictionary list (i.e., password.lst) to your working folder on the virtual machine

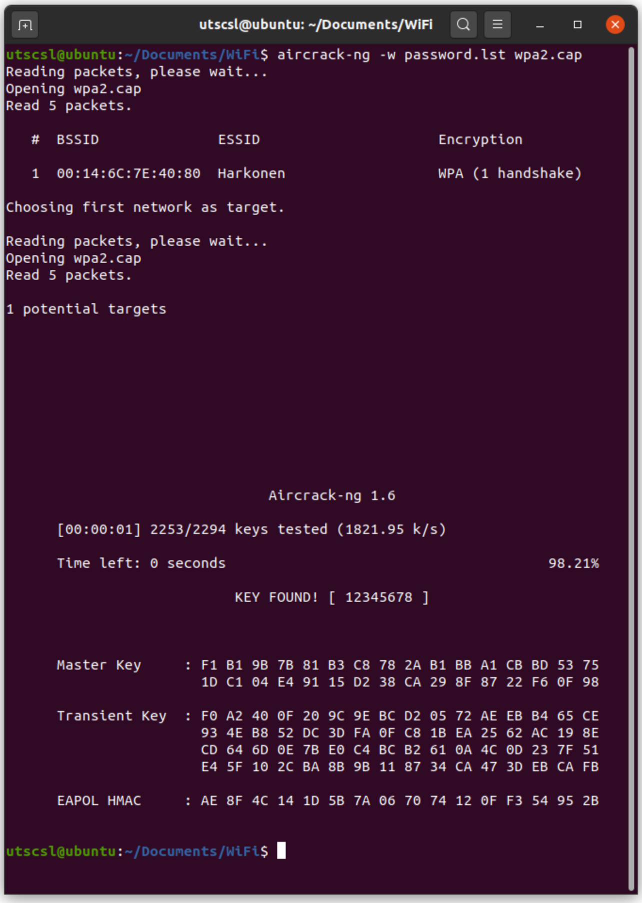
4.3 Crack the WPA2 password

Crack the WPA2 password with the brute-force attack, where potential keys are given in the password.lst. The command is given below.

Part two is based on https://www.aircrack-ng.org/doku.php?id=aircrack-ng

$ aircrack-ng -w password.lst wpa2.cap

You will get



```
utscsl@ubuntu:~/Documents/WiFi$ aircrack-ng -w password.lst wpa2.cap
Reading packets, please wait...
Opening wpa2.cap
Read 5 packets.

   #  BSSID              ESSID                     Encryption

   1  00:14:6C:7E:40:80  Harkonen                  WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening wpa2.cap
Read 5 packets.

1 potential targets





                               Aircrack-ng 1.6

      [00:00:01] 2253/2294 keys tested (1821.95 k/s)

      Time left: 0 seconds                                      98.21%

                           KEY FOUND! [ 12345678 ]


      Master Key     : F1 B1 9B 7B 81 B3 C8 78 2A B1 BB A1 CB BD 53 75
                       1D C1 04 E4 91 15 D2 38 CA 29 8F 87 22 F6 0F 98

      Transient Key  : F0 A2 40 0F 20 9C 9E BC D2 05 72 AE EB B4 65 CE
                       93 4E B8 52 DC 3D FA 0F C8 1B EA 25 62 AC 19 8E
                       CD 64 6D 0E 7B E0 C4 BC B2 61 0A 4C 0D 23 7F 51
                       E4 5F 10 2C BA 8B 9B 11 87 34 CA 47 3D EB CA FB

      EAPOL HMAC     : AE 8F 4C 14 1D 5B 7A 06 70 74 12 0F F3 54 95 2B

utscsl@ubuntu:~/Documents/WiFi$
```

The passphrase is “12345678”.

Take a screenshot of your result and attach the screenshot to your report.

5 WPA3

WPA3 was released in 2018 to improve the Wi-Fi security and solve some WPA2 vulnerabilities. Read the provided reading materials and answer following questions

Q1: What is the vulnerability of WPA2 Personal?

Q2: How does WPA3 solve WPA2 shortcomings?

Q3: Is there any possible attacks against WPA3?

Part two is based on https://www.aircrack-ng.org/doku.php?id=aircrack-ng

6 Answer Questions with Simple Words

Q1: How to capture the four-way handshake?

Q2: What is the vulnerability of WEP used in this cracking?

Q3: What is the vulnerability of WPA2 used in this cracking?

Q4: What have you learnt in this lab?

Lab Summary and Discussion

Summarise and discuss the lab using your words.

Part two is based on https://www.aircrack-ng.org/doku.php?id=aircrack-ng