4 Wireless Encryption

Ref: http://www.asecuritysite.com/wireless/wireless04

4.1 Introduction

The key elements of wireless security are:

- **Authentication**. This is used to identify the user, the wireless client and the wireless access point.
- **Authorization**. This is used to determine that users and wireless devices have the authorization to connect to the network.
- **Accounting**. This is used to log information on the usage of the network, and may set restrictions of the access.
- **Assurance**. This defines that the data that is received and transmitted has not been changed in any way.
- **Confidentiality**. This allows the details of the connection to be kept secret. It typically involves preserving the contents of the transmitted data, but may also include hiding the source and destinations addresses, and the TCP ports used for the connection. Most often, in wireless networks, encryption is used to protect the confidentiality.
- **Data Integrity**. This gives an assurance that the data that is transmitted or retrieved is free from errors, and should be taken as the same as being the original data. Typically data integrity is achieved at differing levels, such as error detection bits in the data frame, check sums within the IP and TCP headers, and also higher-level protocol errors.

One of the major problems in wireless networks is that in certain situations it is possible to by-pass the main security elements of a network, such as the main organisational firewall. This is illustrated in Figure 4.1 where a wireless access point (WAP) allows a user to connect to the inside of the network. The position of the WAP is often placed on the outside of the organisational network, such as in Figure 4.2. Unfortunately this reduces the access to resources from inside the network.

4.2 Wireless Security Problem

Wireless networks have many problems which are due to the inherent openness of wireless networks. Unlike networks based on cables, it is difficult to shield the communications from intruders into the network, as the radio wave typically propagates outside the main communications boundary. Improvements in encryption and authentication have helped with this problem, and there are many other issues which need to be carefully considered between properly implementing a secure wireless network.

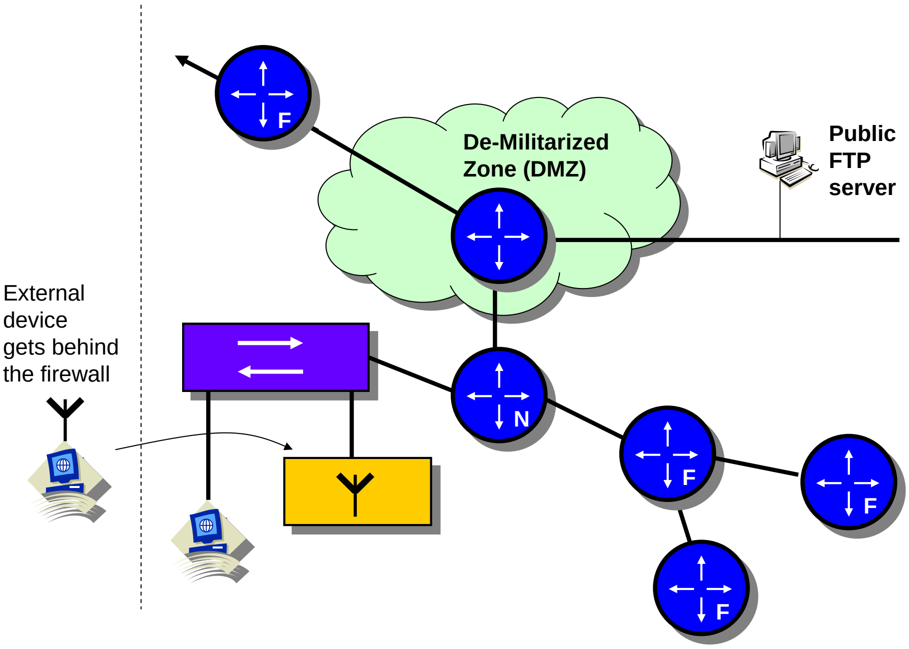


Figure 4.1 WAP on the inside of the organizational network

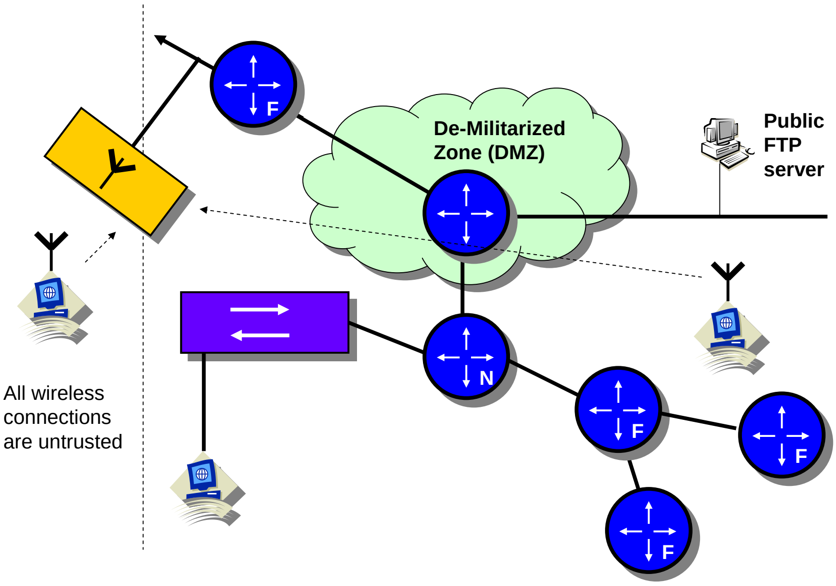


Figure 4.2 WAP on the outside of the organizational network

3.2.1 Radio frequency problems

IEEE 802.11 uses frequencies around the 2.4GHz (for IEEE 802.11b) and 5GHz (for IEEE 802.11a) radio spectrum. These frequencies can obviously be affected by other radio equipment, but obviously can be jammed by a radio transmitter which transmits on the radio frequencies used by a network. It is thus not recommended in military networks (Figure 3).

3.2.2 Denial-of-service attacks

As wireless access points are fairly public in the way that they can be accessed, they can be open to attacks from intruders. A common one is a denial-of-service (DOS) where an intruder continually tries to connect to a WAP, which means that the device takes as much time to setup the connection as it does with its other connections (Figure 4.3). The quality of service (QoS) will thus reduce for other clients which connect to the WAP. In the most extremely case, it may be possible for an intruder to reduce the data throughput to the WAP to almost zero. Along with a DOS attack, it is also possible for an intruder, once connected to the WAP, to continually download files and thus use up much of the available bandwidth. This is known as deprivation of service (DepS), and also results in a reduction in the QoS, and can be overcome by not allowing clients to connect unless they are a valid device, and also to monitor downloads and bandwidth usage. A key factor for both the DoS and DepS attacks is for the administrator to setup system logs which monitor the usage of the wireless network.

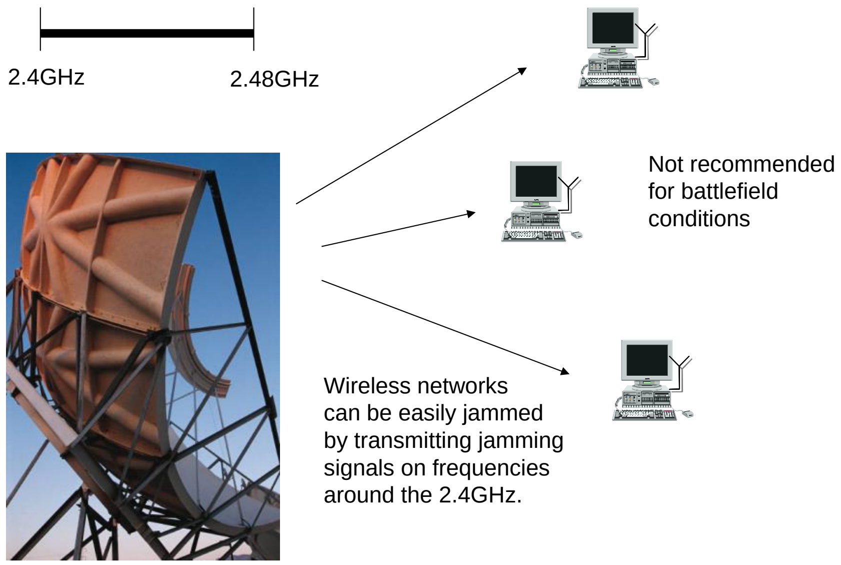

2.4GHz
2.48GHz
Not recommended for battlefield conditions
Wireless networks can be easily jammed by transmitting jamming signals on frequencies around the 2.4GHz.

Figure 4.3 Wireless network jamming

4.3 Spoofing attacks

Most wireless networks use DHCP where a device passes its MAC address which has been registered in the DHCP database. For this only valid MAC addresses will be given an IP address. Unfortunately this type of system can be breached by an intruder who determines a valid MAC address, and uses intruder software to pass the valid MAC address to the WAP (Figure 4.4). It will then be allocated with a valid IP address. Along with this it is possible, in some wireless networks, to setup a valid IP address on the wireless client which allows it to connect to the network.

Along with clients spoofing themselves, another problem can be were a rogue access point is setup for clients to connect to, as many clients are setup to connect to the access point with the strong signal strength. The rouge device can thus overcome any encryption that a client might use.

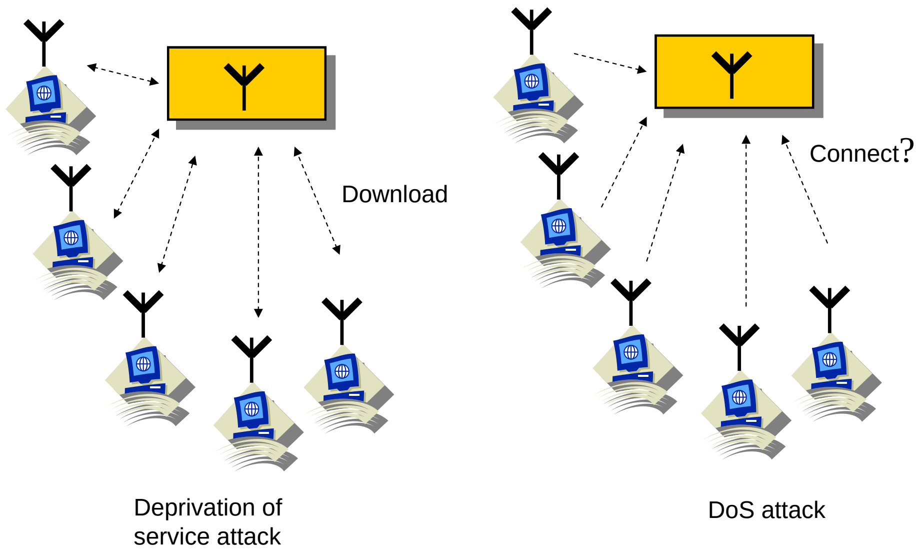


Figure 4.4 Wireless deprivation of service and denial of service problems

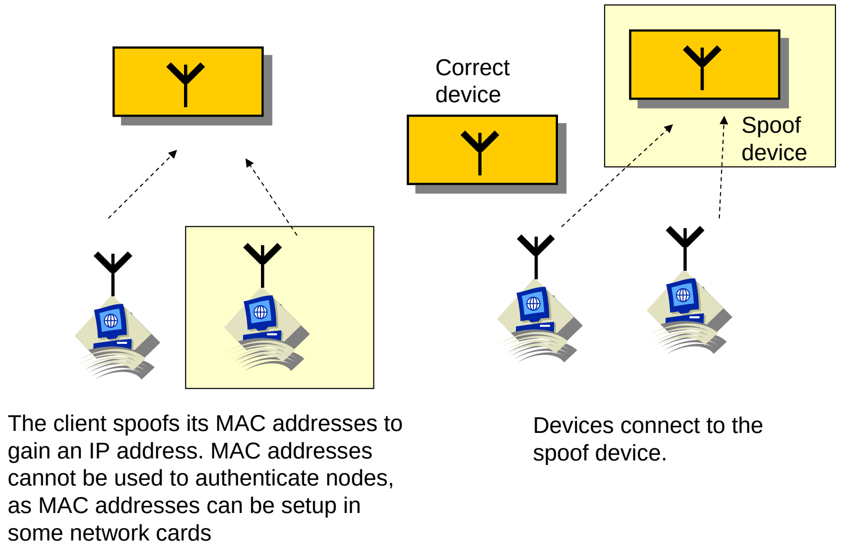

Correct device
Spoof device
The client spoofs its MAC addresses to gain an IP address. MAC addresses cannot be used to authenticate nodes, as MAC addresses can be setup in some network cards
Devices connect to the spoof device.

Figure 4.5 Wireless spoofing problems

4.4 Wireless security standards

As wireless networks have limited physical security and also that the data transmitted is broadcast to all the nodes in an area, it is important that the data is encrypted and also that clients are properly authenticated when they connect to the wireless network. For the encryption, standards such as IPSec and VPN's can be used to allow the data to be secured for that the contents of the data packets cannot be viewed. Unfortunately IPSec and VPN's can cause a reduction in performance, especially where the available bandwidth is limited. As wireless has evolved new standards are being developed to support it. For encryption the first standard was WEP (Wireless Encryption Protocol), which while stopping eavesdroppers, it has been shown to have security flaws. Newer standards include WPA (Wireless Protected Access) and IEEE 802.11i. For authentication there are many different standards which can be used on a range of applications. This includes EAPS (Extensible Authentication Protocol), LEAP (Lightweight EAP) and EAP-TLS (EAP - Transport Layer Security).

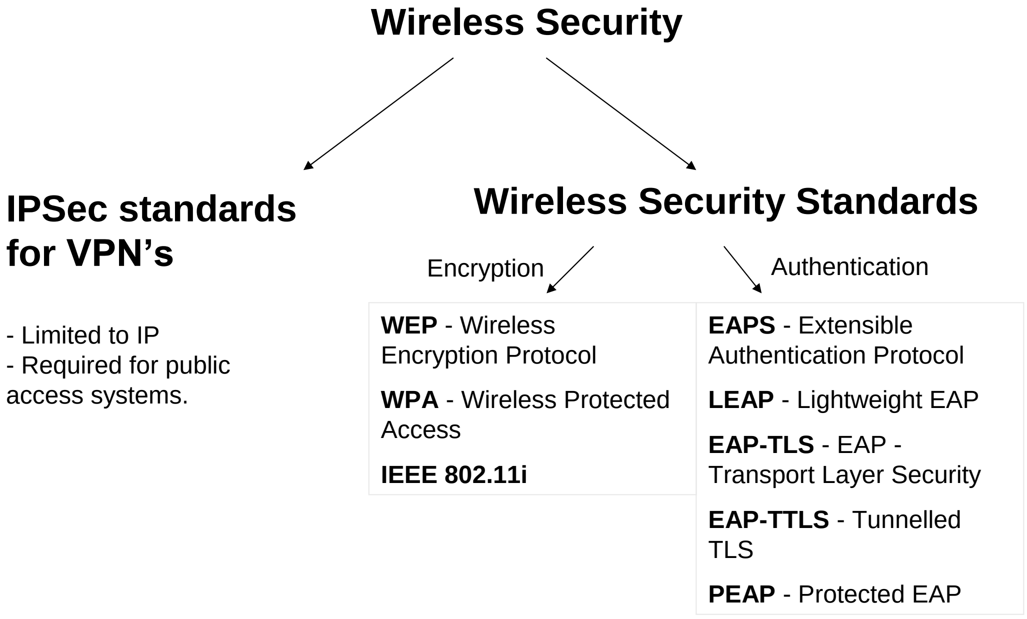

Wireless Security
IPSec standards for VPN's
- Limited to IP
- Required for public access systems.
Wireless Security Standards
Encryption
Authentication
WEP - Wireless Encryption Protocol
WPA - Wireless Protected Access
IEEE 802.11i
EAPS - Extensible Authentication Protocol
LEAP - Lightweight EAP
EAP-TLS - EAP - Transport Layer Security
EAP-TTLS - Tunnelled TLS
PEAP - Protected EAP

Figure 4.6 Wireless security standards

4.5 WEP

WEP was one of the weakest wireless standard , and had three main modes.

- **Disable**. No encryption used.
- **64-bit WEP**. Data encryption with an access point using a 64-bit key.
- **128-bit WEP**. Data encryption with an access point using a 128-bit key.

It has two main weaknesses:

- It has a shared encryption key, which is used by all the nodes on the network. This means that when the key is cracked, then it can be used to decrypt all the network packages within the wireless domain.
- It uses stream encryption, which encrypts each bit one-at-a-time, which is a weaker method of encryption than block ciphers.

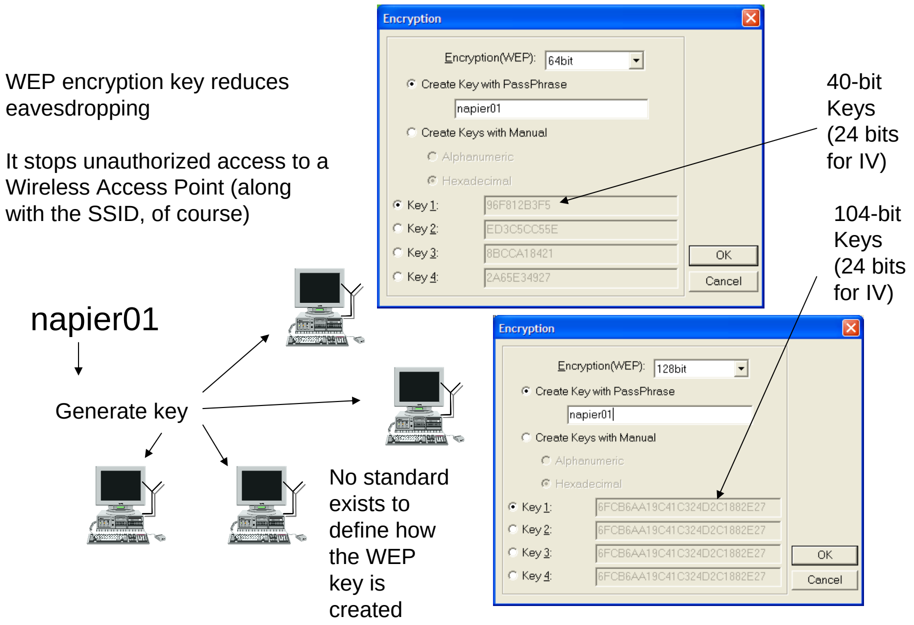
Figure 4.7 shows that that it is possible to set the encryption key as a pass phase or manually. For 64-bit encryption, 5 alphanumeric characters or 10 hexadecimal values is used to define the encryption key, or for 128-bits encryption, the key is specified with 13 alphanumeric values or a 26 hexadecimal characters. The system will only use one of the four keys for its encryption. All the stations and connected access point, if connected, must use the same encryption key. For example a 64-bit key could be:

```
Edin1
```

Whereas 128-bit encryption could use:

```
Edinburgh Net
```

This encryption can be optional (only use, if necessary) or mandatory (where it will only ever use encryption).



WEP encryption key reduces eavesdropping
It stops unauthorized access to a Wireless Access Point (along with the SSID, of course)
napier01
Generate key
No standard exists to define how the WEP key is created
40-bit Keys (24 bits for IV)
104-bit Keys (24 bits for IV)
Encryption
OK
Cancel

Encryption(WEP): 64bit
● Create Key with PassPhrase
napier01
○ Create Keys with Manual
○ Alphanumeric
● Hexadecimal
● Key 1: 96F812B3F5
○ Key 2: ED3C5CC55E
○ Key 3: 8BCCA18421
○ Key 4: 2A65E34927

Encryption(WEP): 128bit
● Create Key with PassPhrase
napier01
○ Create Keys with Manual
○ Alphanumeric
● Hexadecimal
● Key 1: 6FCB6AA19C41C324D2C1882E27
○ Key 2: 6FCB6AA19C41C324D2C1882E27
○ Key 3: 6FCB6AA19C41C324D2C1882E27
○ Key 4: 6FCB6AA19C41C324D2C1882E27

Figure 4.7 Wireless security standards

WEP only encryptions the data between the wireless clients, and once on a wired network it will not apply. The 64-bit bit encryption uses a 24-bit initialization vector (IV), and a 40-bit secret shared encryption key (Figure 7.8). WEP then uses the IV to generate the encryption seed key. From this it uses the RC4 algorithm to generate an infinite pseudo key (Figure 4.9) which is EX-OR'ed with the data stream. The IV thus lengthens the length of the seed value, and changes the key for every data packet.

Unfortunately the IV is a 24-bit value, which is sent as **cleartext**. There are thus only be 2^{24} vectors (16,777,216). If we use 1500 byte packets, the time to send each packet is:

$$1500\times8/11e6 = 1.1\text{ms}$$

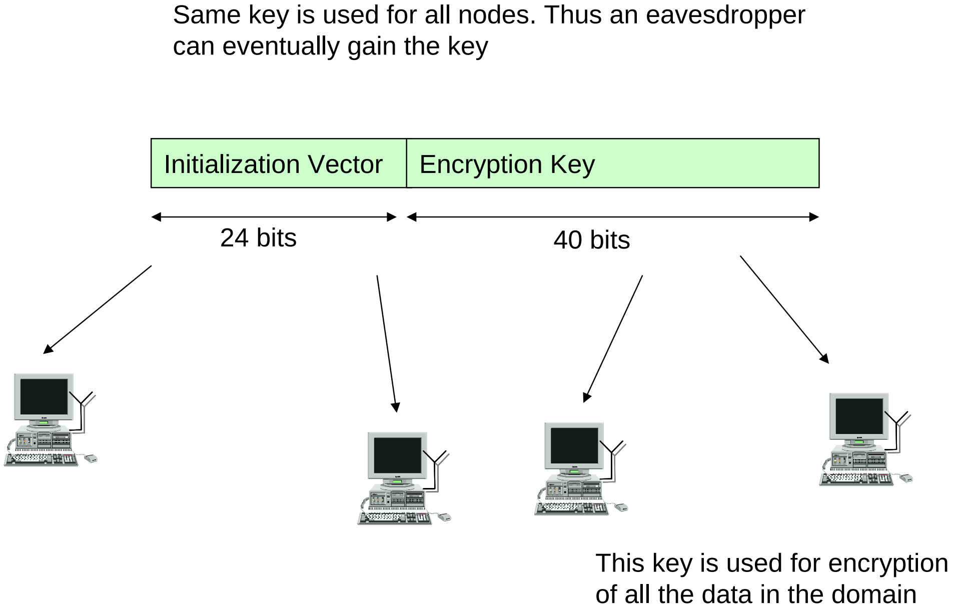
Thus, if the device is continually sending the same vector will repeat after:

$$1.1\text{ms} \times 16{,}777{,}216 = 18{,}302.4 \text{ seconds}$$

which is **5 hours.** The attacker then takes the two cipher texts which have been encrypted with the same key, and performs a statistical analysis on it. Figure 10.12 show the method that packages such as AirSnort use to detect the WEP key.

Another problem is that WEP is open to a man-in-the-middle attack (Figure 10.12) where an intruder reads the message, and, if they know where the letters are in the message, they can flip some of the bits to change the message. Thus an **Integri-**

ty Checker (IC), which is a 32-bit CRC (Cyclic Redundancy Check), is added. Thus, if bits are flipped, it will not give the same CRC value, and an error is caused (Figure 10.13). Unfortunately it is possible to still achieve the same CRC if the bits are flipped across the 32-bit values (Figure 10.14). The same thing can also occur with the data bits in the higher levels protocols, such as changing the IP address of the destination packet (Figure 10.15).



Same key is used for all nodes. Thus an eavesdropper can eventually gain the key

This key is used for encryption of all the data in the domain

Figure 4.8 WEP

WEP uses a stream cipher based on the RC4 algorithm.

- Expands a short key into an infinite pseudo-random key.

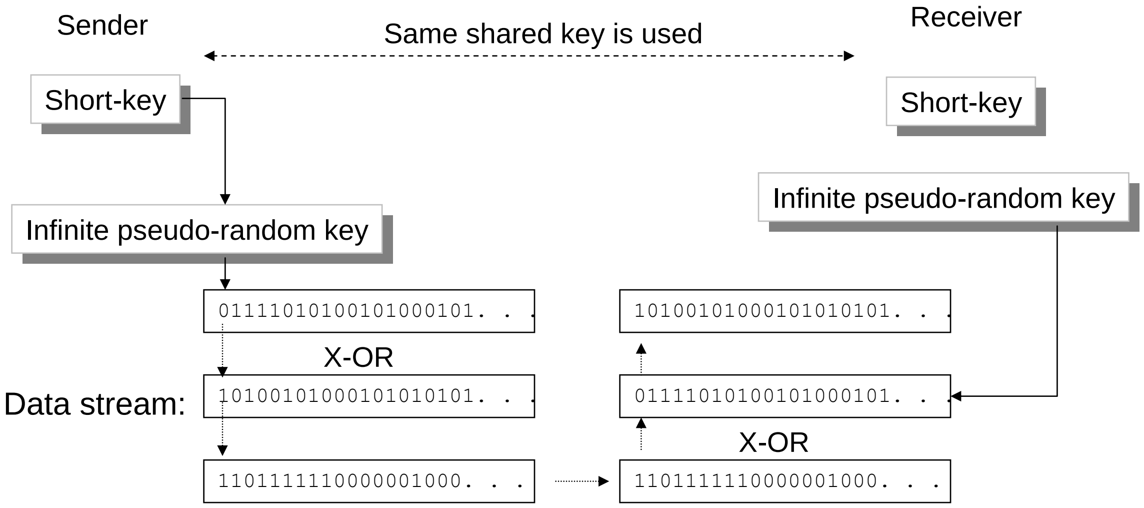
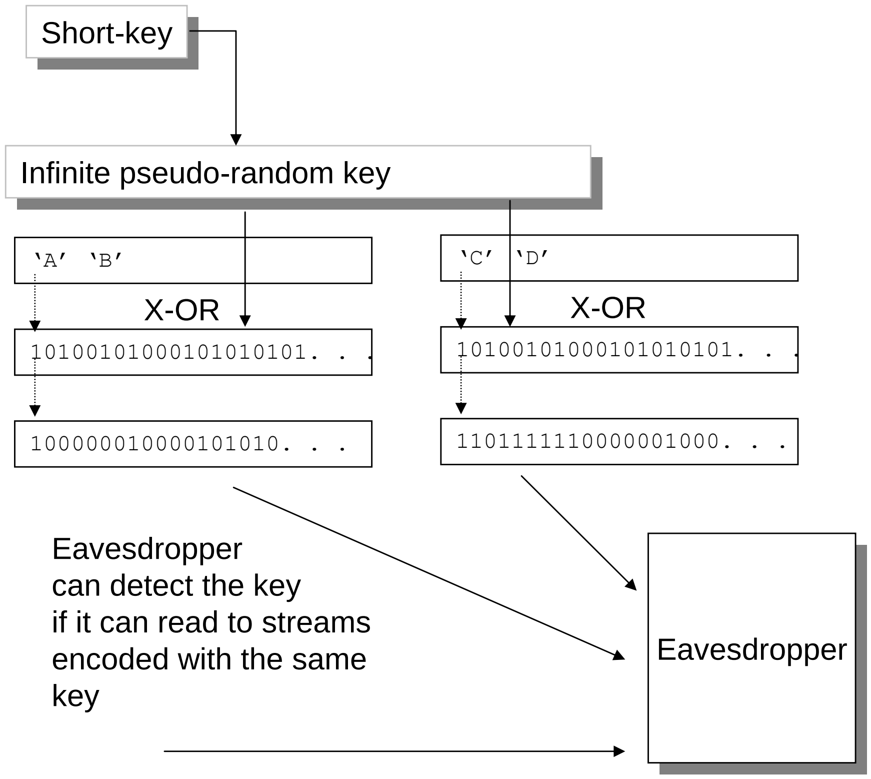
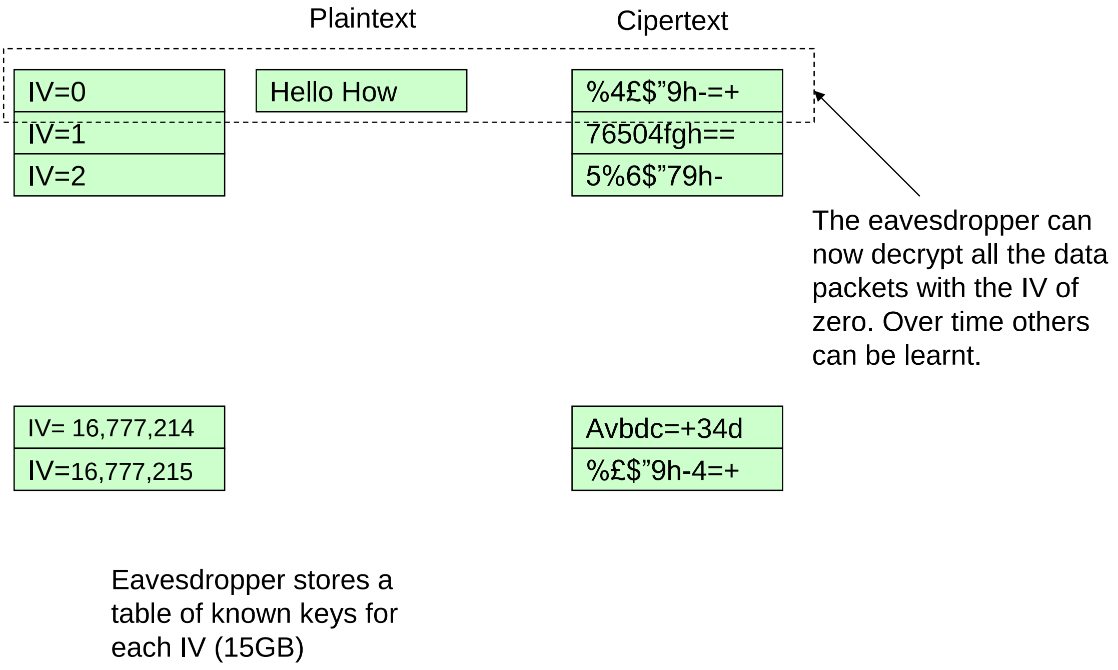


Figure 4.9 WEP



Eavesdropper can detect the key if it can read to streams encoded with the same key

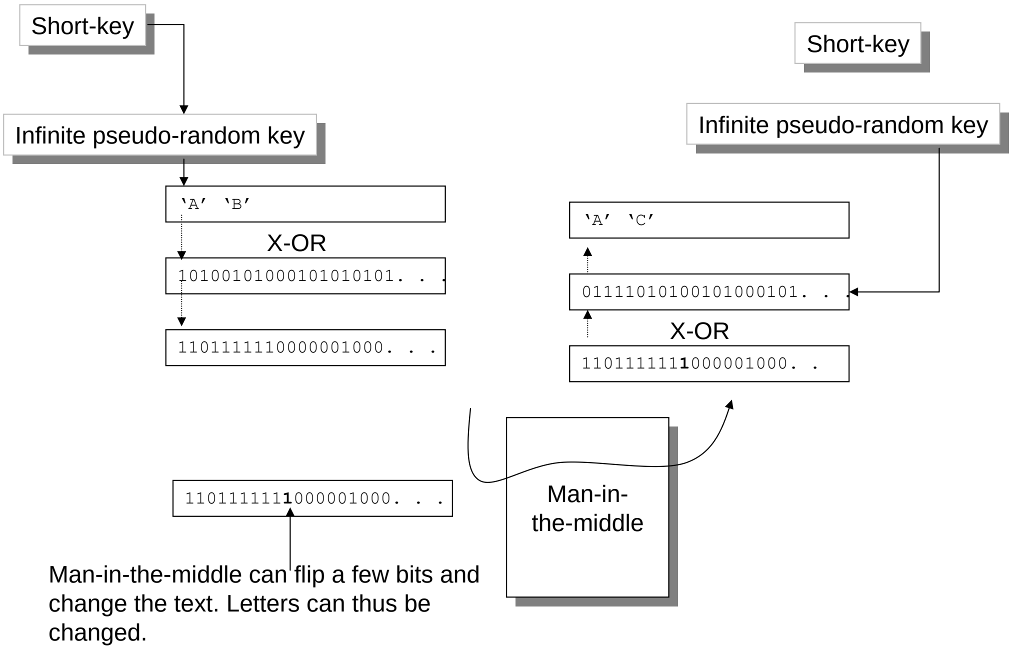
Figure 4.10 WEP



The eavesdropper can now decrypt all the data packets with the IV of zero. Over time others can be learnt.

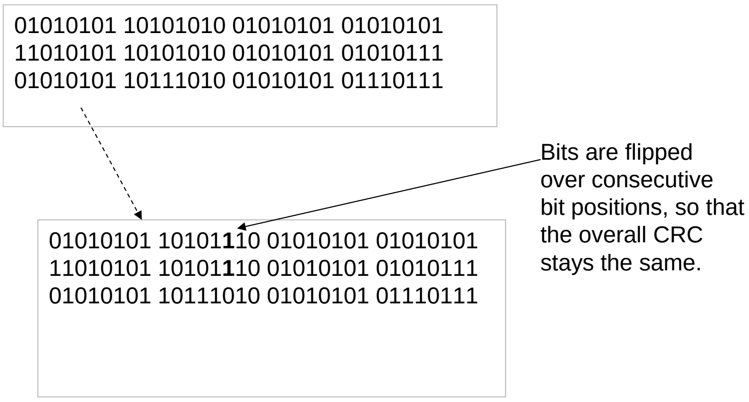
Eavesdropper stores a table of known keys for each IV (15GB)

Figure 4.11 IV vectors



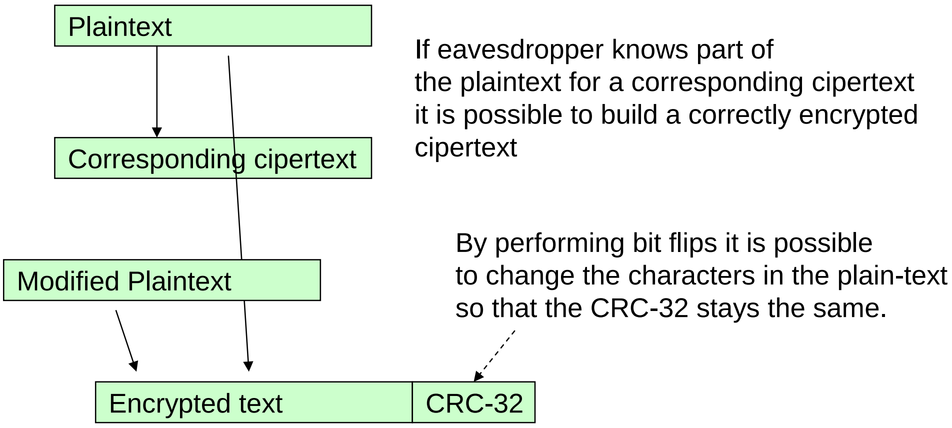
Man-in-the-middle can flip a few bits and change the text. Letters can thus be changed.

Figure 12 WEP



Bits are flipped over consecutive bit positions, so that the overall CRC stays the same.

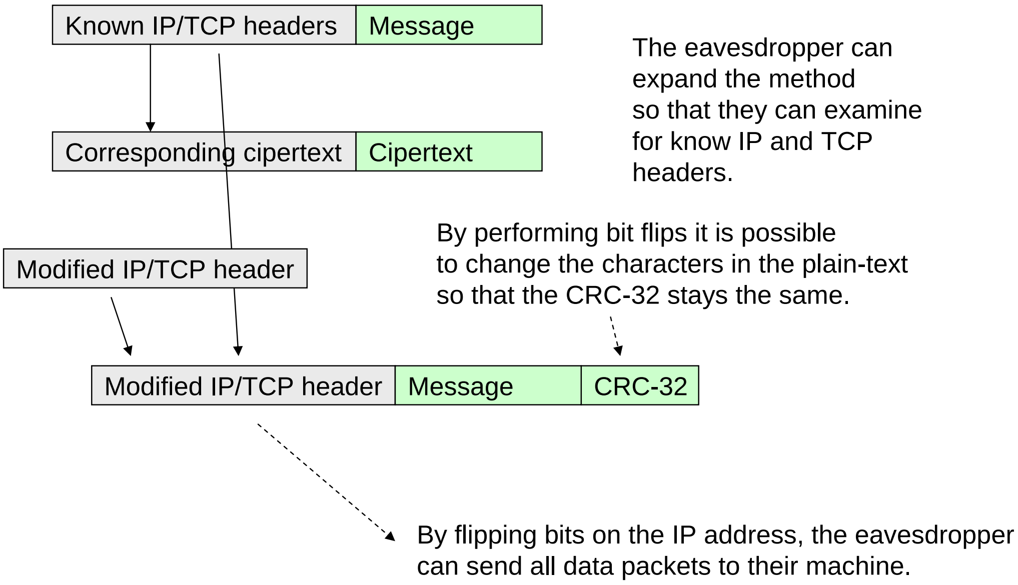
Figure 13 CRC



If eavesdropper knows part of the plaintext for a corresponding cipertext it is possible to build a correctly encrypted cipertext

By performing bit flips it is possible to change the characters in the plain-text so that the CRC-32 stays the same.

Figure 14 CRC

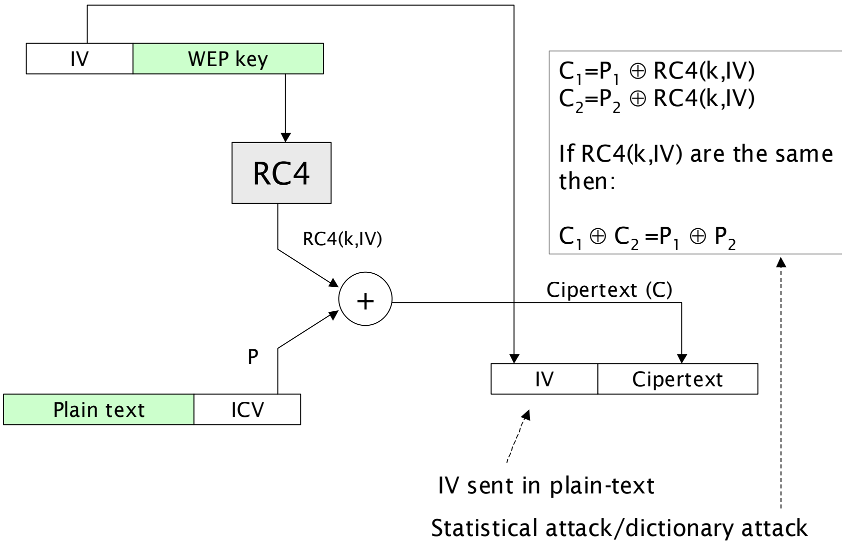


The eavesdropper can expand the method so that they can examine for know IP and TCP headers.

By performing bit flips it is possible to change the characters in the plain-text so that the CRC-32 stays the same.

By flipping bits on the IP address, the eavesdropper can send all data packets to their machine.

Figure 4.15 CRC



$C_1=P_1 \oplus RC4(k,IV)$
$C_2=P_2 \oplus RC4(k,IV)$

If RC4(k,IV) are the same then:

$C_1 \oplus C_2 = P_1 \oplus P_2$

IV sent in plain-text

Statistical attack/dictionary attack

Figure 4.16 Standard WEP

4.6 Programming WEP for a Cisco WAP

WEP is the basic encryption method used for wireless. For the key to be generated the user must define a 10-digit hexadecimal code:

```
# config t
(config)# int dot11radio0
(config-if)# encryption mode wep optional
(config-if)# encryption key 1 size 40bit 1122334455 transmit-key
(config)# exit
```

Key

Key number 1 (three other keys are possible)

The same can be done for 128-bit encryption, which is more secure. In this case we require 26 hexadecimal digits.

```
# config t
(config)# int dot11radio0
(config-if)# encryption mode wep optional
(config-if)# encryption key 1 size 128bit 12345678901234567890123456
transmit-key
(config)# exit
```

4.7 TKIP

To overcome the problems of the WEP encryption method, TKIP (802.11i) adds two things:

- **MIC** (Message Integrity Check). This adds two new fields: sequence number and an integrity check field. The access point rejects any sequence numbers which are out-of-sequence. Also the integrity check has been added which is an improved version of the IV integrity checker.
- **Per-packet keys**. This produces WEP keys which eliminate IV reuse and weak IV's.

Figure 4.16 outlines the operation of the existing WEP standard, and Figure 4.17 shows how it has been enhanced, but still keeps compatibility with existing wireless hardware. It is open to bit-flipping, and a passive attack where the intruder waits for the IV to repeat, and can then EX-OR the two cipertext streams and can determine the plaintext.

With TKIP a Packet IV (PIV) is used as a sequence number, and creates a PPK (Per-packet key) along with the shared key and the transmitter's address. The sequence number stops **replay attacks** as two frames with the same sequence number are rejected (along with sequence numbers which are less than the expected sequence number). The transmitter starts the PIV at zero, and then increments it for each transmitted frame.

The temporal key is 128 bits long, and has a certain lifetime. This is then mixed up with the 48-bit MAC address of the transmitted, in order that different stations will produce data streams which are different. TKIP uses a re-key facility which continually refreshes the encryption keys. Initially a master key is passed between the access point and the station. This is created for each session, and is passed in a secure way. This master key by the access point to pass the encryption keys. The station and the access point then generate two temporal keys; one for each direction of transmission. To avoid the same key for recurring the Packet IV (which is 16-bits) will rollover each 2^{16} packets. Thus the master key must be regenerated each 2^{16} packets.

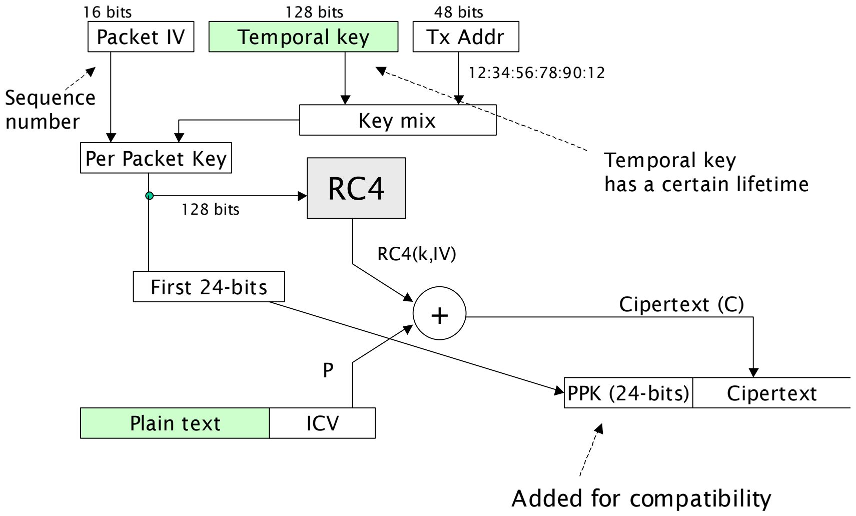


Figure 17 TKIP

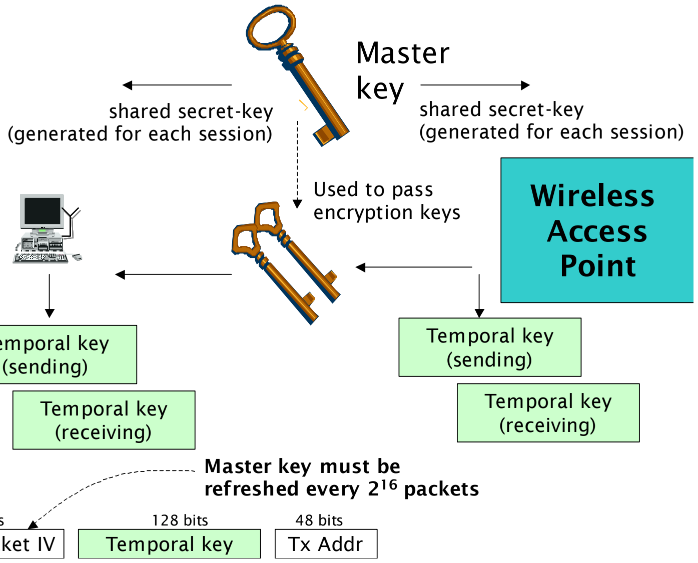


Figure 4.18 TKIP

TKIP is not a future solution to the problems of wireless security, but is compatible with existing equipment, and should provide enough security for current standards.

4.8 Tutorial

1. Prove that there are 16,777,216 IV values.

2. Show that 128-bit WEP encryption requires 26 hexadecimal digits. Why does it only require 13 ASCII digits?

3. Show that 64-bit WEP encryption requires 10 hexadecimal digits. Which of the following of valid 64-bit WEP keys:

   napier
   university

soc

4. Which of the following of valid hexadecimal 64-bit WEP keys:

   napier
   aaaaaaaaaa
   abcdefghij

5. What is the result of “ABC” exclusive-OR’ed (⊕) with 1010 1010 1010 1010 1010 1010? What is the result if the same key is used to exclusive-OR the result?

   Example: “D” ⊕ 1001 1001 gives:

   ```
   0100 0100
   1001 1001
   ---------
   1001 1101
   ---------
   ```

   The rules for ⊕ are: 0⊕0=0, 0⊕1=1, 1⊕0=1 and 1⊕1=0.

6. Approximate the time taken for the IV value to repeat for a 54Mbps connection.

7. How is the WEP key set in a wireless access point which uses Cisco IOS?

8. Complete the wireless access point tutorial.

4.9 Standard ASCII

Binary	*Decimal*	*Hex*	*Character*	*Binary*	*Decimal*	*Hex*	*Character*
00000000	0	00	NUL	00010000	16	10	DLE
00000001	1	01	SOH	00010001	17	11	DC1
00000010	2	02	STX	00010010	18	12	DC2
00000011	3	03	ETX	00010011	19	13	DC3
00000100	4	04	EOT	00010100	20	14	DC4
00000101	5	05	ENQ	00010101	21	15	NAK
00000110	6	06	ACK	00010110	22	16	SYN
00000111	7	07	BEL	00010111	23	17	ETB
00001000	8	08	BS	00011000	24	18	CAN
00001001	9	09	HT	00011001	25	19	EM
00001010	10	0A	LF	00011010	26	1A	SUB
00001011	11	0B	VT	00011011	27	1B	ESC
00001100	12	0C	FF	00011100	28	1C	FS
00001101	13	0D	CR	00011101	29	1D	GS
00001110	14	0E	SO	00011110	30	1E	RS
00001111	15	0F	SI	00011111	31	1F	US
Binary	*Decimal*	*Hex*	*Character*	*Binary*	*Decimal*	*Hex*	*Character*
00100000	32	20	SPACE	00110000	48	30	0
00100001	33	21	!	00110001	49	31	1
00100010	34	22	“	00110010	50	32	2
00100011	35	23	#	00110011	51	33	3
00100100	36	24	$	00110100	52	34	4
00100101	37	25	%	00110101	53	35	5
00100110	38	26	&	00110110	54	36	6
00100111	39	27	/	00110111	55	37	7
00101000	40	28	(	00111000	56	38	8
00101001	41	29	)	00111001	57	39	9
00101010	42	2A	*	00111010	58	3A	:
00101011	43	2B	+	00111011	59	3B	;
00101100	44	2C	,	00111100	60	3C	<
00101101	45	2D	-	00111101	61	3D	=
00101110	46	2E	.	00111110	62	3E	>
00101111	47	2F	/	00111111	63	3F	?
Binary	*Decimal*	*Hex*	*Character*	*Binary*	*Decimal*	*Hex*	*Character*
01000000	64	40	@	01010000	80	50	P
01000001	65	41	A	01010001	81	51	Q
01000010	66	42	B	01010010	82	52	R
01000011	67	43	C	01010011	83	53	S
01000100	68	44	D	01010100	84	54	T
01000101	69	45	E	01010101	85	55	U
01000110	70	46	F	01010110	86	56	V
01000111	71	47	G	01010111	87	57	W
01001000	72	48	H	01011000	88	58	X
01001001	73	49	I	01011001	89	59	Y
01001010	74	4A	J	01011010	90	5A	Z
01001011	75	4B	K	01011011	91	5B	[
01001100	76	4C	L	01011100	92	5C	\
01001101	77	4D	M	01011101	93	5D	]
01001110	78	4E	N	01011110	94	5E	`
01001111	79	4F	O	01011111	95	5F	_
Binary	*Decimal*	*Hex*	*Character*	*Binary*	*Decimal*	*Hex*	*Character*
01100000	96	60		01110000	112	70	p
01100001	97	61	a	01110001	113	71	q
01100010	98	62	b	01110010	114	72	r
01100011	99	63	c	01110011	115	73	s
01100100	100	64	d	01110100	116	74	t
01100101	101	65	e	01110101	117	75	u
01100110	102	66	f	01110110	118	76	v
01100111	103	67	g	01110111	119	77	w
01101000	104	68	h	01111000	120	78	x
01101001	105	69	i	01111001	121	79	y
01101010	106	6A	j	01111010	122	7A	z
01101011	107	6B	k	01111011	123	7B	{
01101100	108	6C	l	01111100	124	7C	:
01101101	109	6D	m	01111101	125	7D	}
01101110	110	6E	n	01111110	126	7E	~
01101111	111	6F	o	01111111	127	7F	DEL