CWSP Guide to Wireless Security

Wireless Security Models

Objectives

- Explain the advantages of WPA and WPA2
- Explain the technologies that are part of the personal security model
- List the features of the transitional security model
- Define the enterprise security model

Wireless Security Solutions

- WEP suffers from serious weakness
- “Band-aid” solutions
  - WEP2 and Dynamic WEP
- Better solutions
  - IEEE 802.11i
  - Wi-Fi Protected Access (WPA)
  - Wi-Fi Protected Access 2 (WPA2)

IEEE 802.11i

- Addresses the two weaknesses of wireless networks: encryption and authentication
- Encryption
  - Replaces the RC4 stream cipher algorithm with a block cipher
    - Manipulates an entire block of text at one time
  - 802.11i uses the Advanced Encryption Standard (AES)
    - Designed to be an encryption technique that is secure from attacks

Block Ciphers vs Stream Cipher

- Block ciphers – ie. DES, 3DES, AES
  - Message is broken into blocks, each of which is then encrypted
  - Operate with a fixed transformation on large blocks of plaintext data

- Stream ciphers – ie. RC4
  - Process the message bit by bit (as a stream)
  - Operate with a time-varying transformation on individual plaintext digits

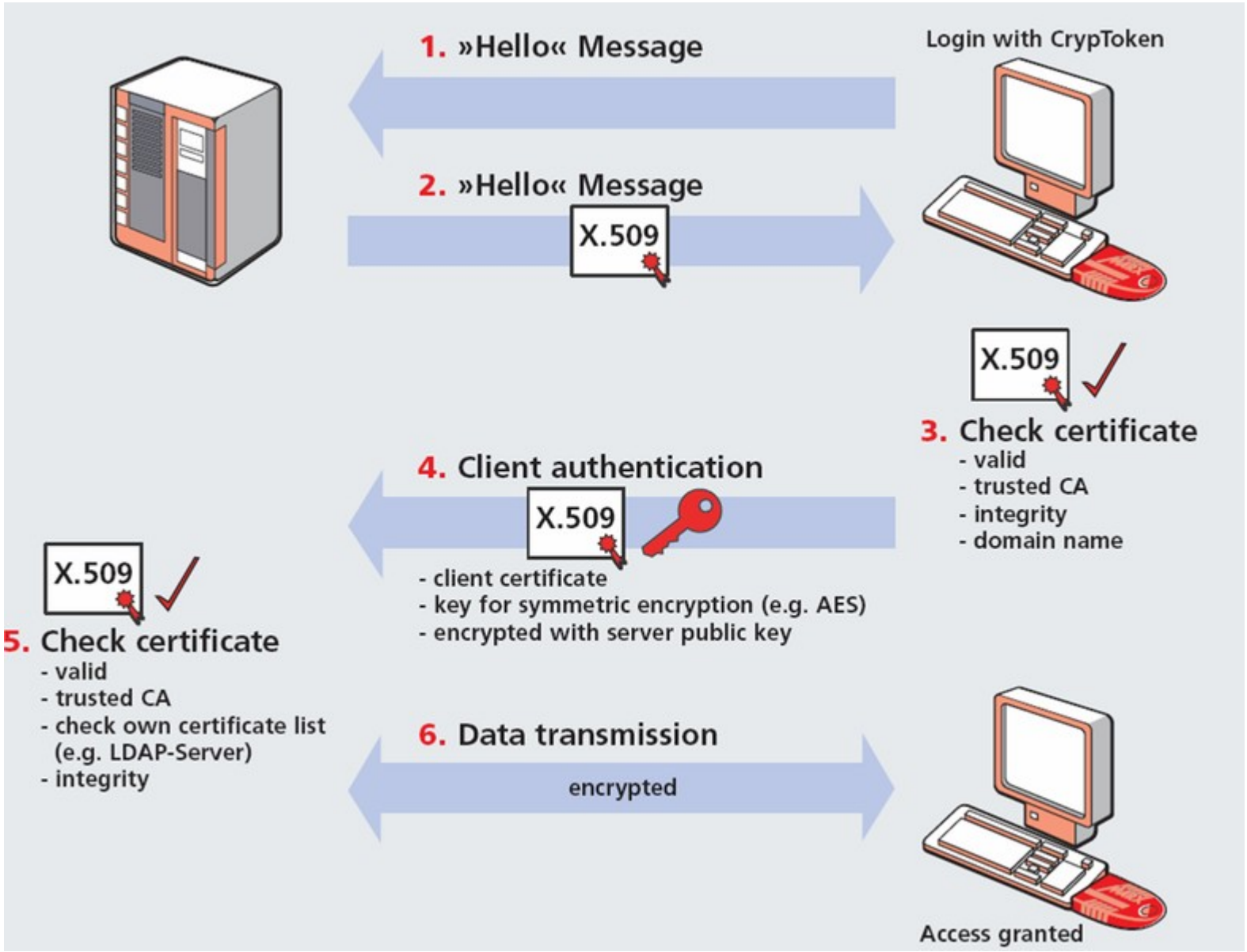
RC4

- RC4 was designed by Ron Rivest of RSA Security in 1987, it is officially termed “Rivest Cipher 4”.
- RC4 algorithm is capable of key lengths of up to 256 bits and is typically implemented in 64 bits, 128 bits and 256 bits.
- RC4 is used in WEP, TKIP (Temporal Key Integrity Protocol, (SSL) Secure Socket Layer , (TLS) Transport Layer Security

Encryption Algorithm Characteristics

Name	Cipher Type	Key Size	Common Use
RC4	Stream	64,128 up to 256 bits	WEP,WPA (TKIP),SSL/TLS
DES	Block	64-bit (56-bit key + 8 Parity bits)	SSH, IPSec
3DES	Block	Three-Key Mode: 192-bit (168-bit key + 24 Parity bits) Two-Key Mode: 128-bit (112-bit key + 16 Parity bits)	SSL/TLS,SSH, IPSec
AES	Block	128,192,256-bits	802.11i-CCMP, SSH,PGP

Client Authentication SSL



WEP vulnerabilities, and usage of WPA

Cracking WEP and WPA wireless networks and How to Better Secure Wireless Networks



In this section we will discuss

- How to crack WEP and WPA
- Tactics to better secure your network

WEP cracking

- WEP is outdated and week
- Novice hackers will hack WEP very easily
- WEP uses a 3-byte vector (IV) Initialization Vector – IV is placed in packets – based on pre-shared key
- Capturing thousands of these packets from the client or AP you will have enough data gathered to crack WEP

Tools

- AirCrack,
  - Aircrack contains several tools
    - Tools will be using
      - Airodump – capturing IVs
      - Aircrack – cracking IVs
- Kismet
  - For sniffing and locating networks

Getting Started

- The device (laptop) wireless card must be put into “monitor mode” aka. (promiscuous mode)
  - allows wireless card to locate and crack wlan network
  - putting wireless card in this mode is not very easy. Web browsing will not be possible when wireless card is placed in promiscuous mode.
  - Rollback wireless card drivers to undo monitor mode.

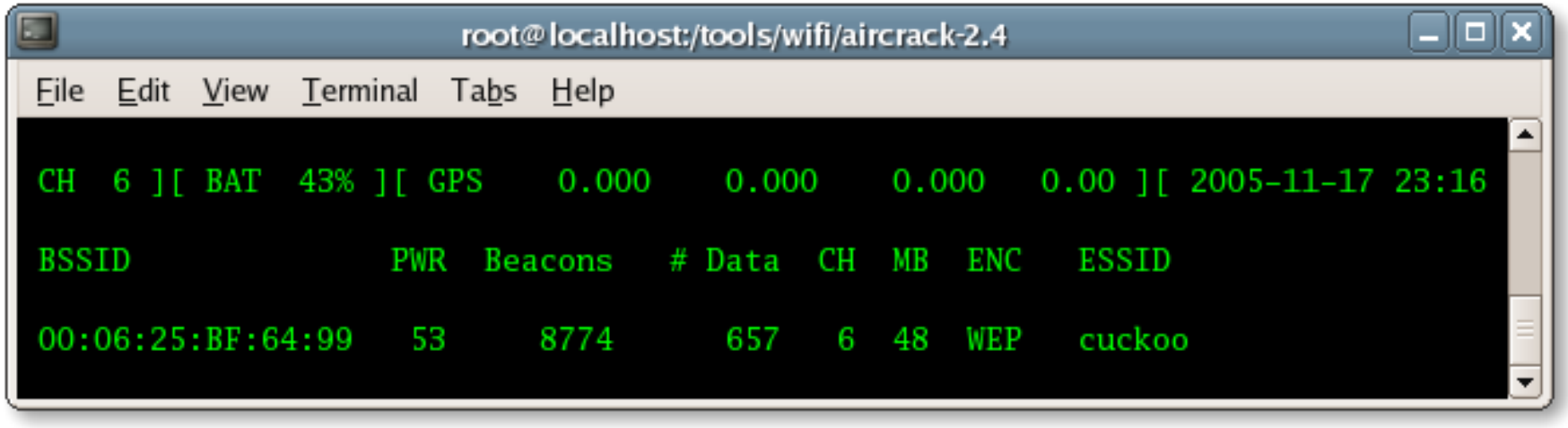
Getting Started – cont.

- Run kismet or airodump and locate nearby networks
- The info we need:
  - Encryption type
  - Channel no.
  - IP address
  - MAC address (BSSID)
- Ie. Let’s use a channel 6 – and SSID (MAC address) 00:23:1F:55:04:BC

Capturing

- Capturing IVs
  - Use airodump – type command: /airodump <interface> <output prefix> [channel] [IVs flag]
- Example
  - /airodump cardname **test** 6 1
    - "**test**" is the filename with our captured IVs
    - "1" is always used for IVs flag when cracking WEP
    - Note: (the more the merrier) meaning: we will need over 100,000 IVs to crack the WEP key

Airodump or Kismet output

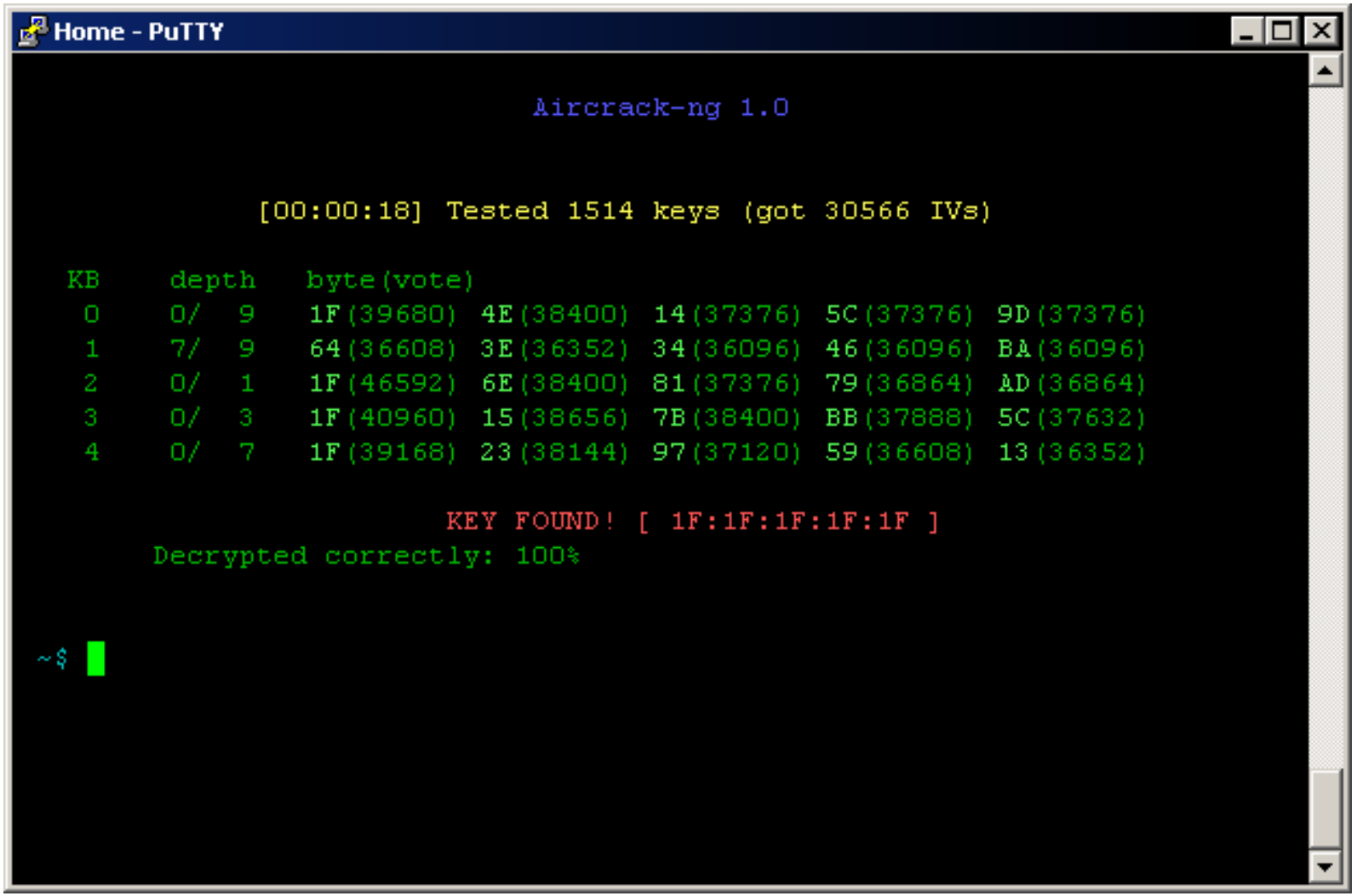


1. BSSID = MAC
2. CH = Channel Number
3. # Data = Number of IVs captured so far

Cracking

- Cracking IVs
  - Using aircrack command: /aircrack [option] <input file>
    - The options are
      - -a 1 for WEP
      - -b for BSSID
      - (the input file is the file we generated using airdump command earlier) : Ie. /aircrack –a 1 –b 00:23:1F:55:04:BC test.ivs

Screenshot from aircrack



- Info from airodump is fed into aircrack the program will return the WEP key used on that network. Program gave out over 30566 IVs in 18 seconds. Could do 3000000 in less than 3 min.

WEP finale

- The time needed for cracking the WEP key is determined by the number of the IVs collected.
- Any number of IVs over 100000 is reasonable and should yield the WEP key within minutes.

Intro to cracking WPA

- WPA keys are much harder than WEP to crack
- WPA cracking nearly impossible
- WPA fills out holes that WEP can’t

Getting started

- WPA passwords are real words
  - dictionary word list

Capturing

- Run kismet to gather network info required
- Open airodump, enter command: /airodump cardname test 2
  - Cardname is the name of the wireless card
  - Test is the name of the output file
  - 2 is the channel we retrieved using Kismet

Cracking

- Open aircrack and type: /aircrack –a 2 –b 00:25:1G:45:02:ad –w/path/to/wordlist
  - to crack WPA use –a 2
  - -b is the MAC (BSSID)
  - -w is path on your computer to the dictionary word list

Conclusion

- WEP is easier to crack than WPA
- AirCrack is one tool used to crack WEP

Reasons you should secure your network

- Your resources are exposed to unknown users
- Your network can be captured, examined
- Your network and connectivity may be used for illegal activities

Countermeasures

- Use these tips to prevent unwanted users
  - Change default setting on your router
    - When you install router modify id and pwd to something else rather than default
  - Disable SSID broadcast
    - Hides network from beginner intruder. Ie. Windows Wireless Zero config utility
    - Will not keep you safe from more advance hackers
  - Turn off network when not in use
    - Impossible to hack a network that it is not running
  - MAC address filtering
    - AP grants access to certain MAC addresses
    - Not fully proof, but good countermeasure
  - Encryption
    - Use of WPA
    - Use long and random WPA keys

IEEE 802.11i (continued)

Table 5-1 Time needed to break AES

Key Length	Number of Possible Keys	Time Needed to Break with $1 Million Worth of Computers
40 bits	1,099,551,627,776	Less than 1 minute
56 bits	72,057,594,037,927,936	30 minutes
64 bits	18,446,744,073,709,551,616	4 days
80 bits	1.21×10^{24}	800 years
128 bits	3.40×10^{38}	2.20×10^{17} years
192 bits	6.28×10^{57}	10^{36} years
256 bits	1.16×10^{77}	10^{56} years

IEEE 802.11i (continued)

- Authentication and key management
  - Accomplished by the IEEE 802.1x standard
    - Implements port security
    - Blocks all traffic on a port-by-port basis
      - Until the client is authenticated using credentials stored on an authentication server
- Key-caching
  - Stores information from a device on the network
  - If a user roams away and later returns
    - She does not need to re-enter all of the credentials

IEEE 802.11i (continued)

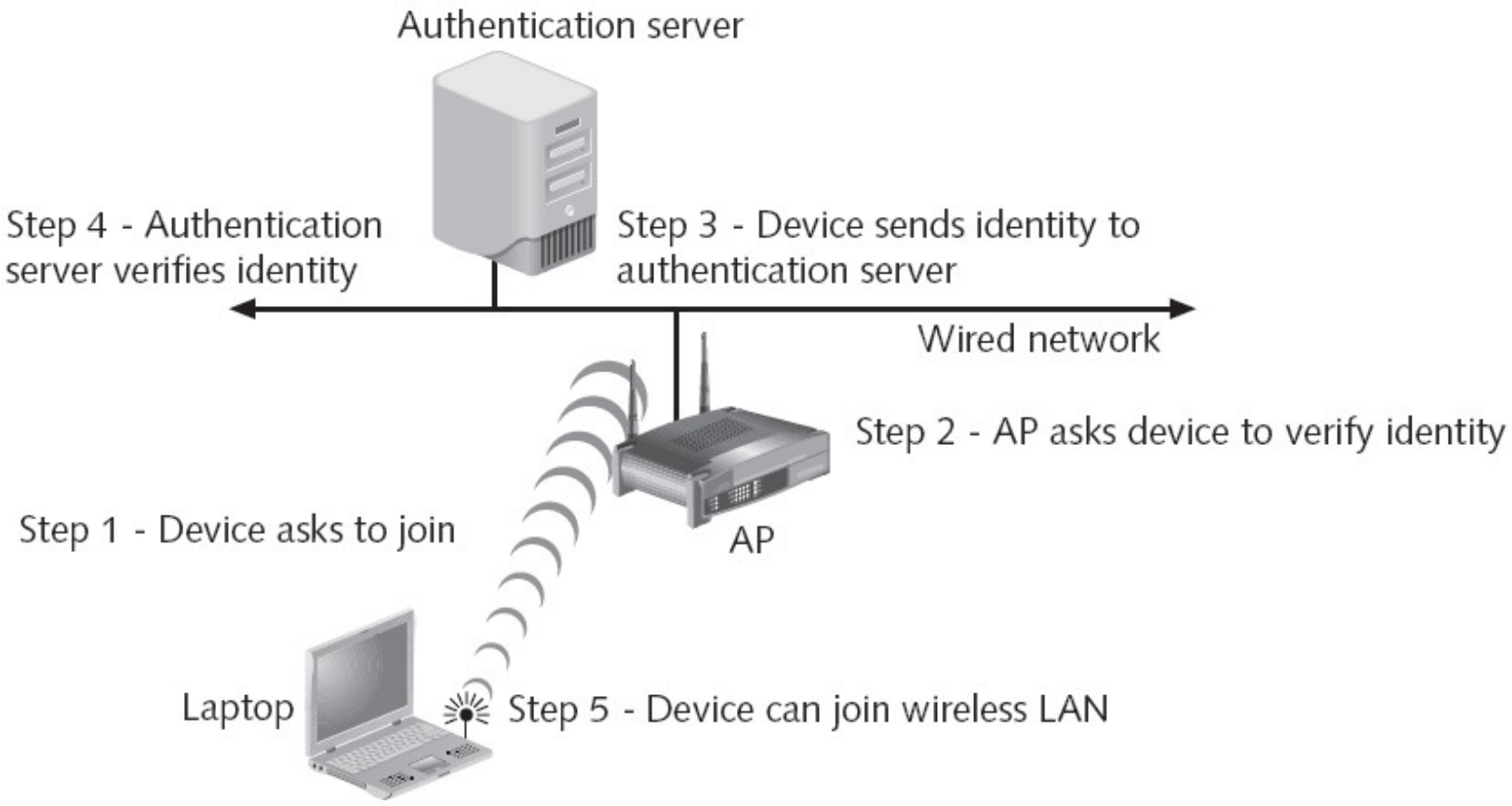


Figure 5-1 IEEE 802.1x

IEEE 802.11i (continued)

- Pre-authentication
  - Allows a device to become authenticated to an AP
    - Before moving into range of the AP
  - Device sends a pre-authentication packet to the AP which the user is currently associated with
    - And the packet is then routed to a remote AP or APs
  - Allows for faster roaming between access points

Wi-Fi Protected Access (WPA)

- Subset of 802.11i
- Addresses both encryption and authentication
- Temporal Key Integrity Protocol (TKIP)
  - TKIP keys are known as per-packet keys
  - TKIP dynamically generates a new key for each packet that is created
  - Prevent collisions
    - Which was one of the primary weaknesses of WEP
- Authentication server can use 802.1x to produce a unique master key for that user session

Wi-Fi Protected Access (WPA) (continued)

- TKIP distributes the key to wireless devices and AP
  - Setting up an automated key hierarchy and management system
- WPA replaces the Cyclic Redundancy Check (CRC) with the Message Integrity Check (MIC)
  - Designed to prevent an attacker from capturing, altering, and resending data packets
  - Provides a strong mathematical function
  - Clients are de-authenticated and new associations are prevented for one minute if an MIC error occurs
    - Optional feature

Wi-Fi Protected Access (WPA) (continued)

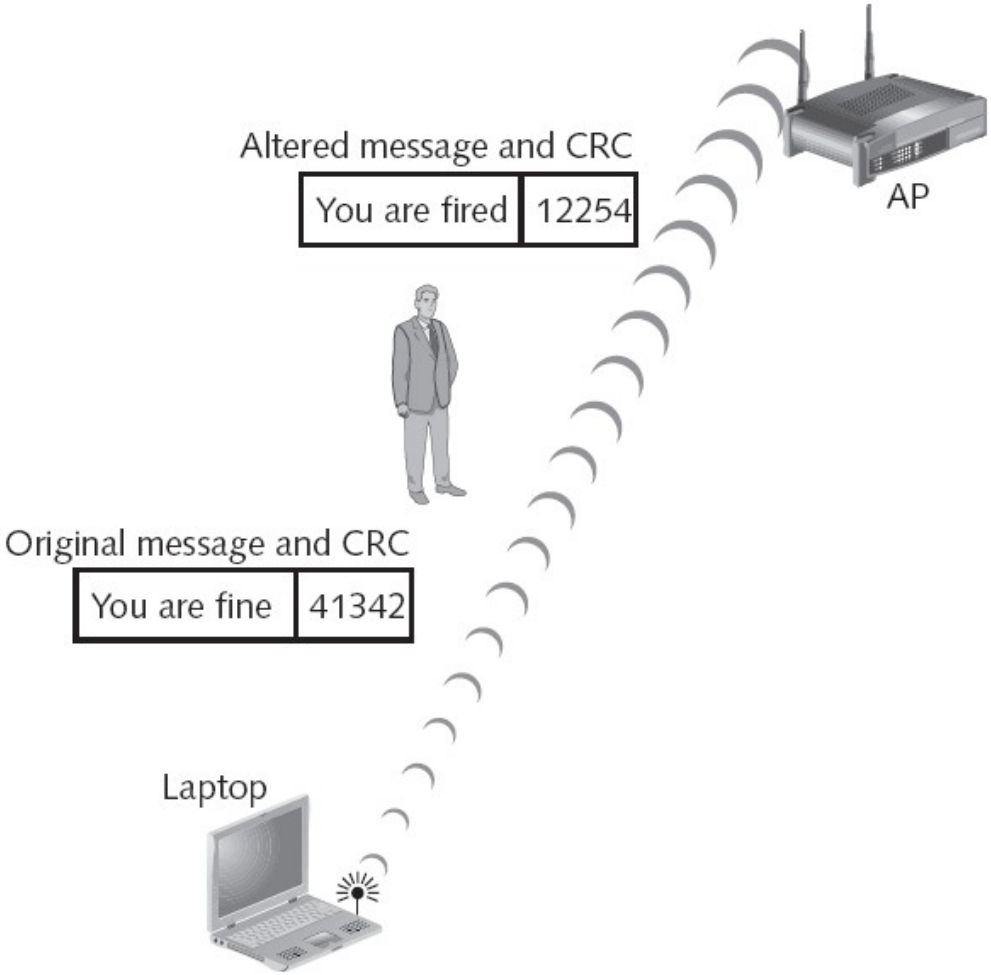


Figure 5-2 Message Integrity Check (MIC)

Wi-Fi Protected Access (WPA) (continued)

- WPA authentication
  - Accomplished by using either IEEE 802.1x or preshared key (PSK) technology
- PSK authentication uses a passphrase to generate the encryption key
  - Passphrase must be entered on each access point and wireless device in advance
  - Passphrases serve as the seed for mathematically generating the encryption keys
- WPA was designed to address WEP vulnerabilities with minimum inconvenience

Wi-Fi Protected Access 2 (WPA2)

- Second generation of WPA security
- Based on the final IEEE 802.11i standard
- Uses the Advanced Encryption Standard (AES) for data encryption
- Supports IEEE 802.1x authentication or PSK technology
- WPA2 allows both AES and TKIP clients to operate in the same WLAN

Advanced Encryption Standard
AES ENCRYPTION

- Rijndael is the selected (NIST competition) algorithm for AES (advanced encryption standard).
- It is a block cipher algorithm, operating on blocks of data.
- It needs a secret key, which is another block of data.

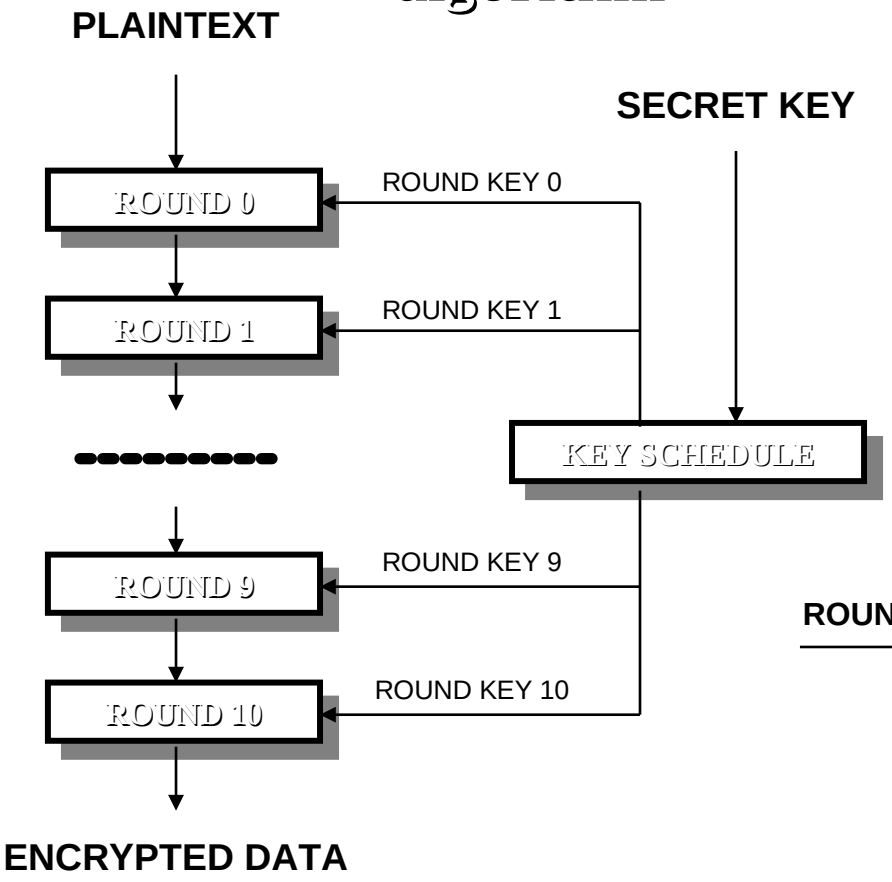
AES ENCRYPTION

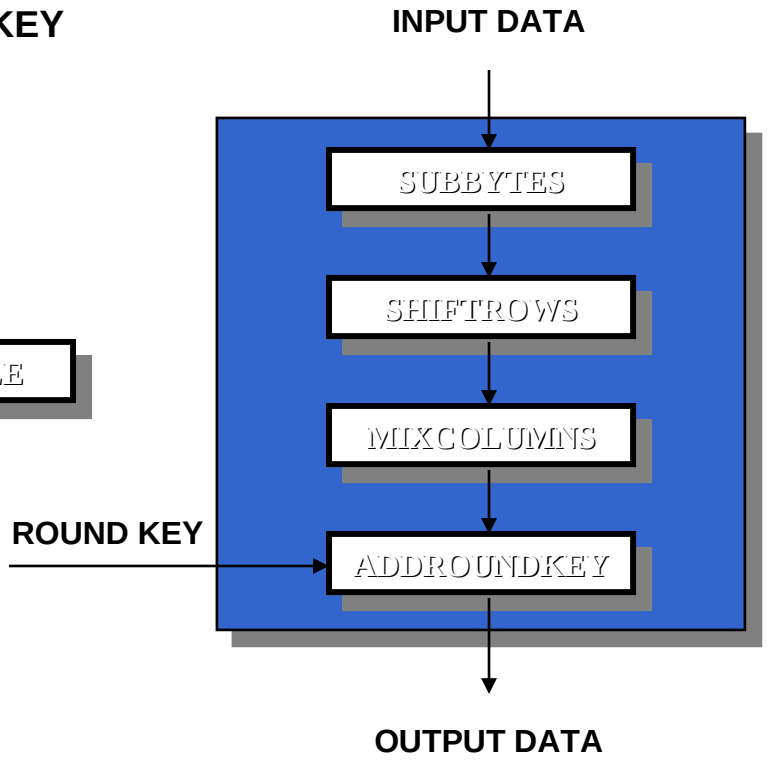
- Performs encryption and the inverse operation, decryption (using the same secret key).
- It reads an entire block of data, processes it in rounds and then outputs the encrypted (or decrypted) data.
- Each round is a sequence of four inner transformations.
- The AES standard specifies 128-bit data blocks and 128-bit, 192-bit or 256-bit secret keys.

AES Algorithm – Encryption

encryption algorithm

structure of a generic round





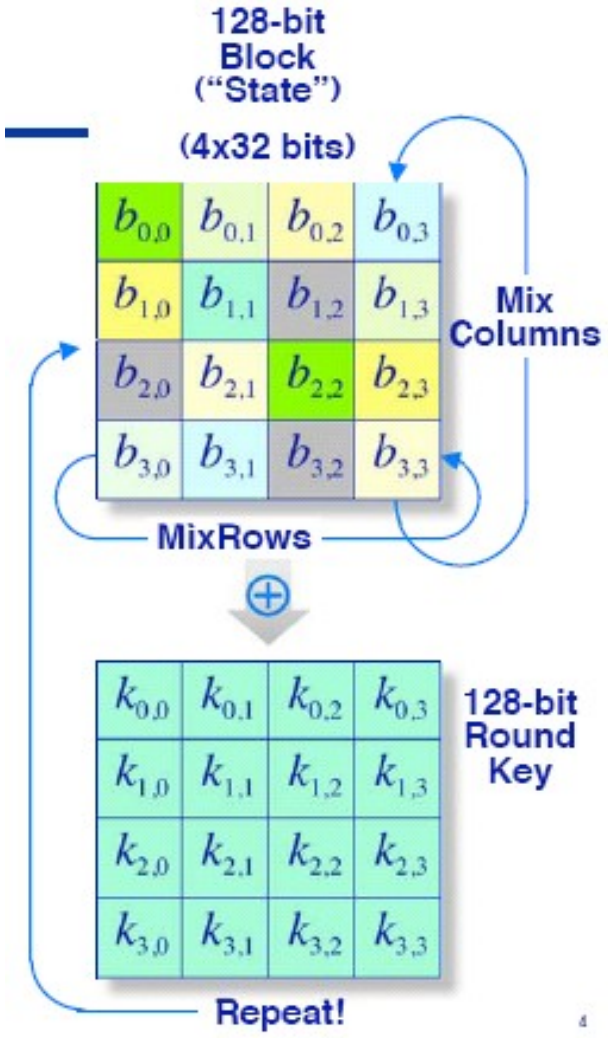
AES Algorithm – Encryption
A little closer look

1. Perform a byte by byte substitution
2. Perform a row by row shift operation
3. Perform a column by column transformation
4. Perform a XOR with a round key

No of rounds = 10 for 128 bits

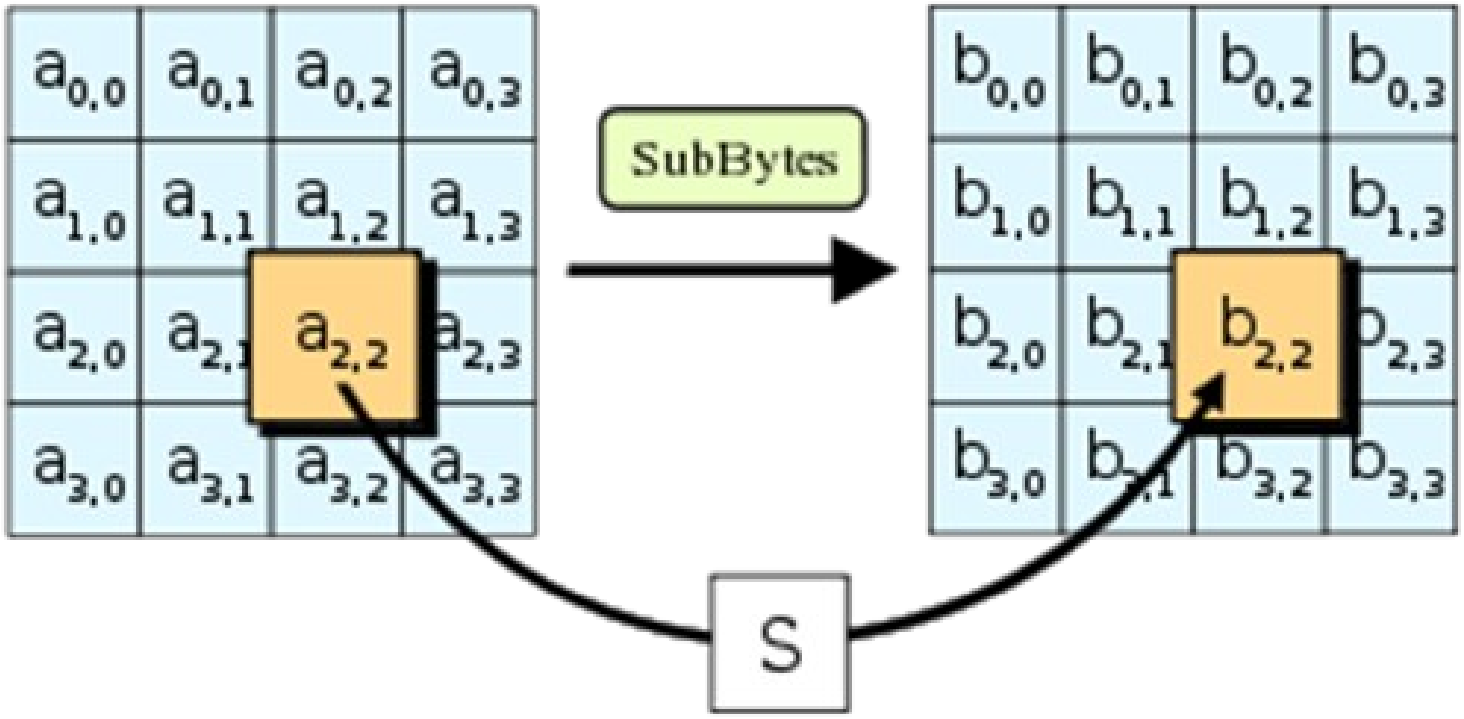
12 for 192 bits

14 for 256 bits



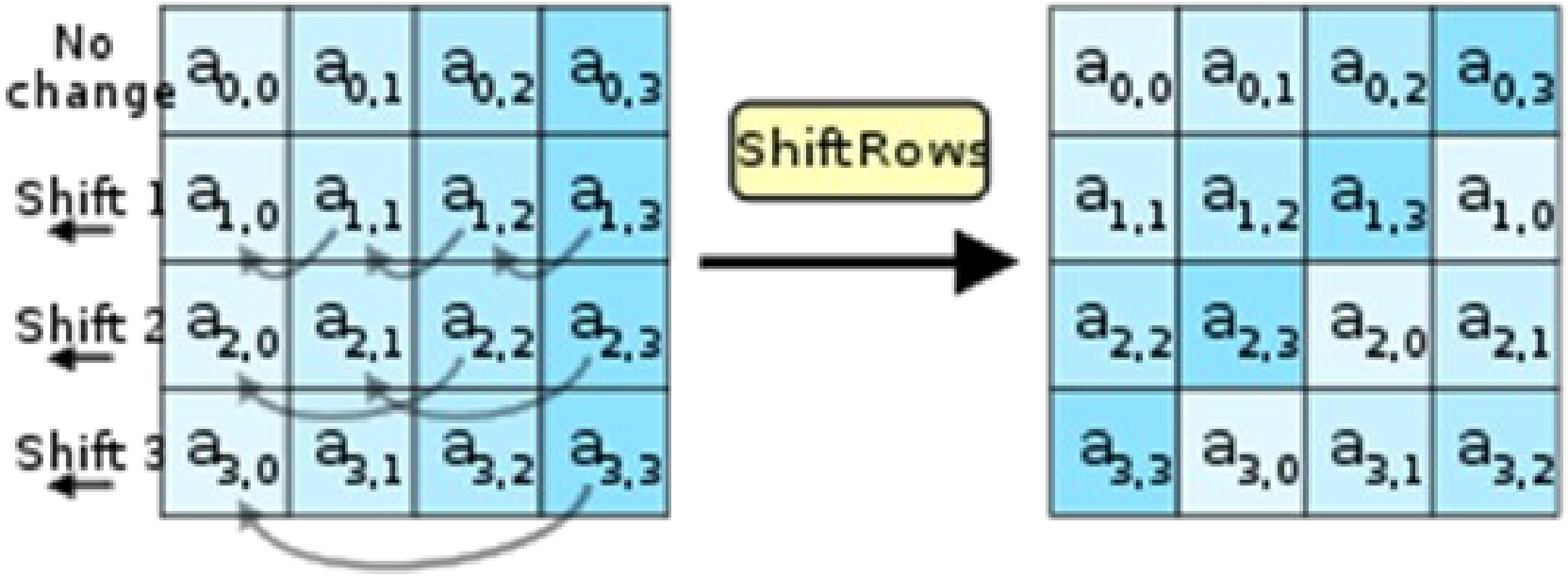
AES
Advanced Encryption Standard

1. The SubByte Step



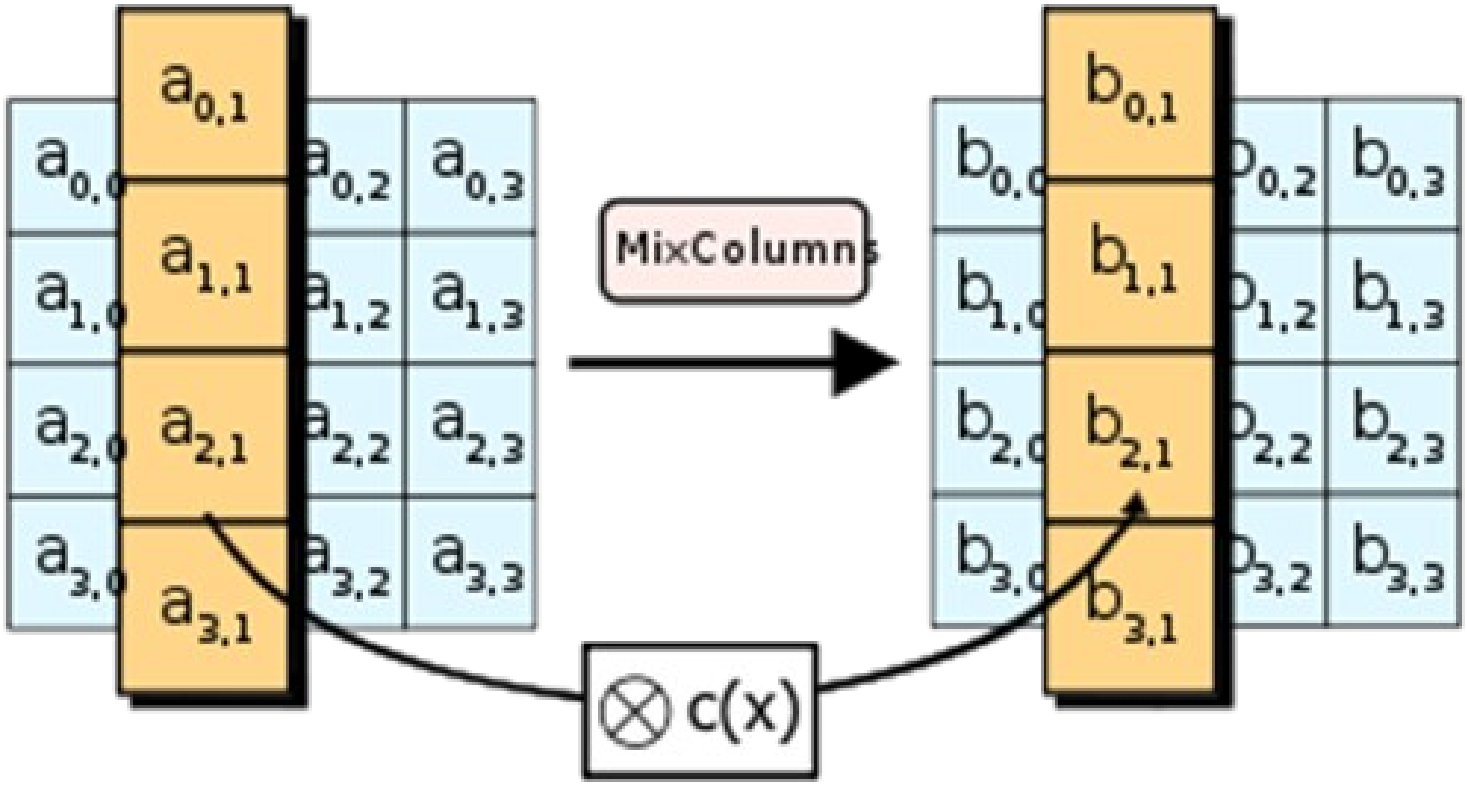
AES
Advanced Encryption Standard

2. The ShiftRow Step

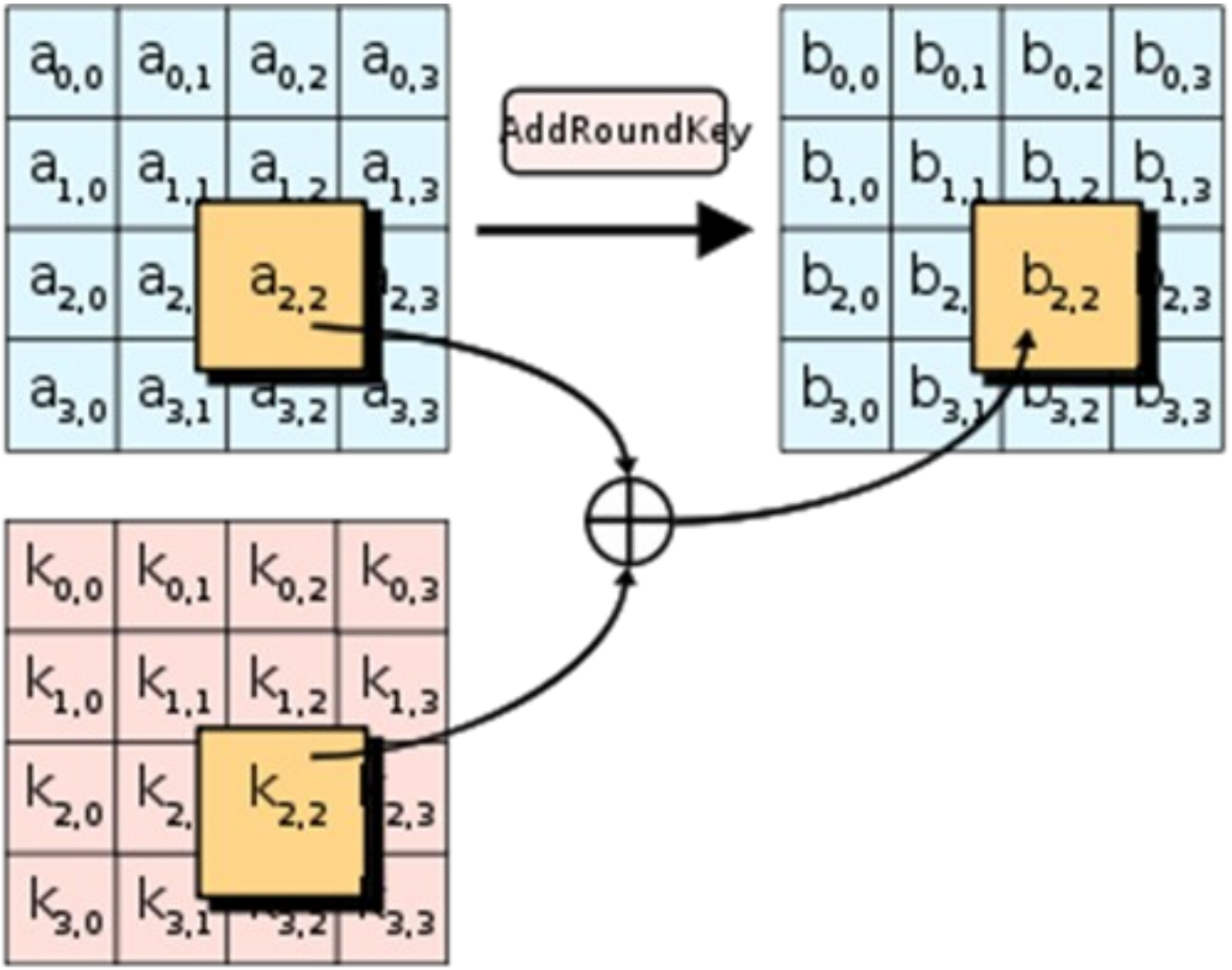


AES
Advanced Encryption Standard

3. The MixColumns Step



AES
The AddRoundKey step



Some facts about AES

- **AES keys (128bits)**

  340,000,000,000,000,000,000,000,000,000,000,000 (3.402823669209384634633746074317e+38)

  possible keys
- Suitable for a wide variety of platforms - ranging from smart cards to servers
- Much simpler, faster and more secure (than it’s predecessor 3DES)

AES ‘built-into’ products

- Navastream Crypto Phones
- PGP Mobile for the TREO 650
- Nokia’s solutions for mobile VPN client – AES 256



AES Cracking - 2006

- Assumptions
  - 3 GHz dedicated processor
  - 1 clock cycle per key generation
- 2^128 keys / 3E9 processes per second =
    - 1.13E29 seconds
    - 3.6E21 years, 3.6 Zy (Zetta years)
    - 3.6 Sextillion years

AES Cracking - Future

- 1 Week Decryption
- 5.6E32 Hz Processor, 560 MHz

Clock Cycles per Key Generation

Processor Speed Doubling Rate (Years)	1	4	8	16
0.5	38.8	155.3	310.7	621.3
1	77.7	310.7	621.3	1242.6
1.5	**116.5**	**466.0**	**932.0**	**1863.9**
2	155.3	621.3	1242.6	2485.3

Wi-Fi Protected Access 2 (WPA2) (continued)

Table 5-2 Wireless security solutions

Name	Encryption	Authentication	Security level
WEP	WEP	Shared Key	Low
WPA	TKIP	PSK or 802.11i	Medium
WPA2/IEEE 802.11i	AES	802.1x	High

Wi-Fi Protected Access 2 (WPA2) (continued)

- Wi-Fi Alliance wireless security models based on WPA and WPA2
  - WPA—Personal Security
  - WPA—Enterprise Security
  - WPA2—Personal Security
  - WPA2—Enterprise Security
- Transitional security model
  - Used as a “bridge” solution in situations where WPA or WPA2 security is not available
  - Intended as a temporary fix

Wi-Fi Protected Access 2 (WPA2) (continued)

Table 5-3 Wi-Fi security models

Wi-Fi Model	Application	WPA	WPA2
Personal	Small office/home office Home use	Authentication: PSK Encryption: TKIP	Authentication: PSK Encryption: AES
Enterprise	Business Education Government	Authentication: 802.1x Encryption: TKIP	Authentication: 802.1x Encryption: AES

Transitional Security Model

- Should *only* be implemented as a temporary solution

Authentication

- Shared key authentication
  - Should be used instead of open system authentication
  - Uses WEP keys for authentication
  - Based on a challenge-response scheme
- SSID beaconing
  - Should be turned off
  - May prevent a “casual” unauthorized user or novice attacker from capturing the SSID
    - And entering the network
  - Use a hard-to-guess SSID in a WLAN

Authentication (continued)

- MAC address filtering limitations
  - Managing a large number of MAC addresses is difficult
  - Does not provide an easy means to temporarily allow a guest user to access the network
  - WLANs initially exchange MAC addresses in cleartext
  - A MAC address can be “spoofed” or substituted
- DHCP restrictions
  - DHCP “leases” IP addresses to clients to use while they are connected to the network

Authentication (continued)

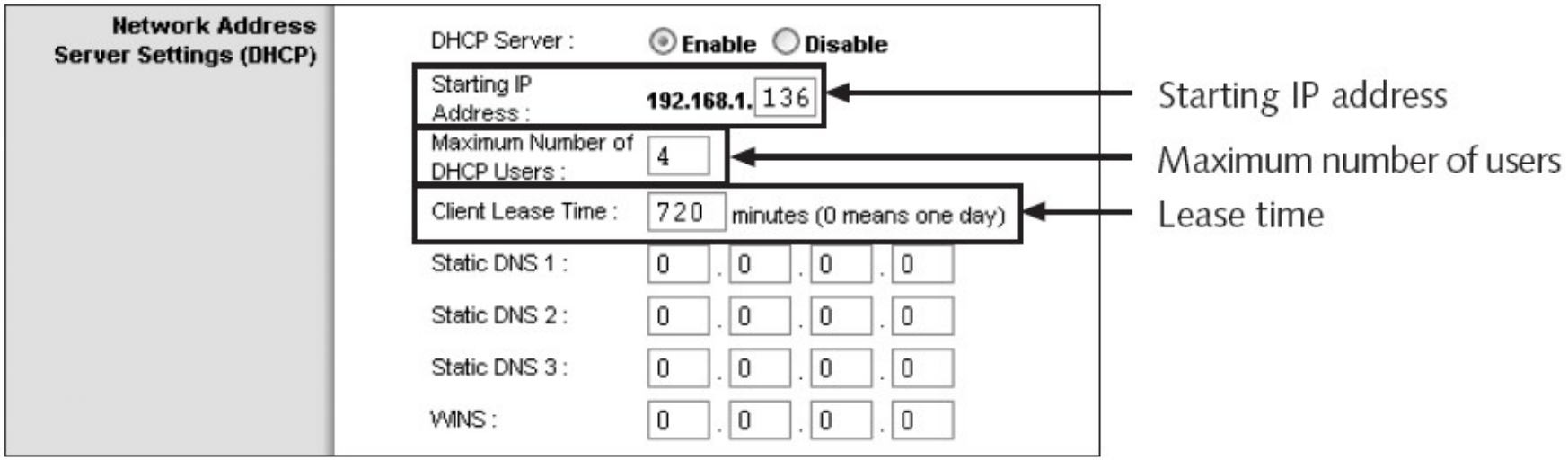


Figure 5-3 DHCP settings

Authentication (continued)

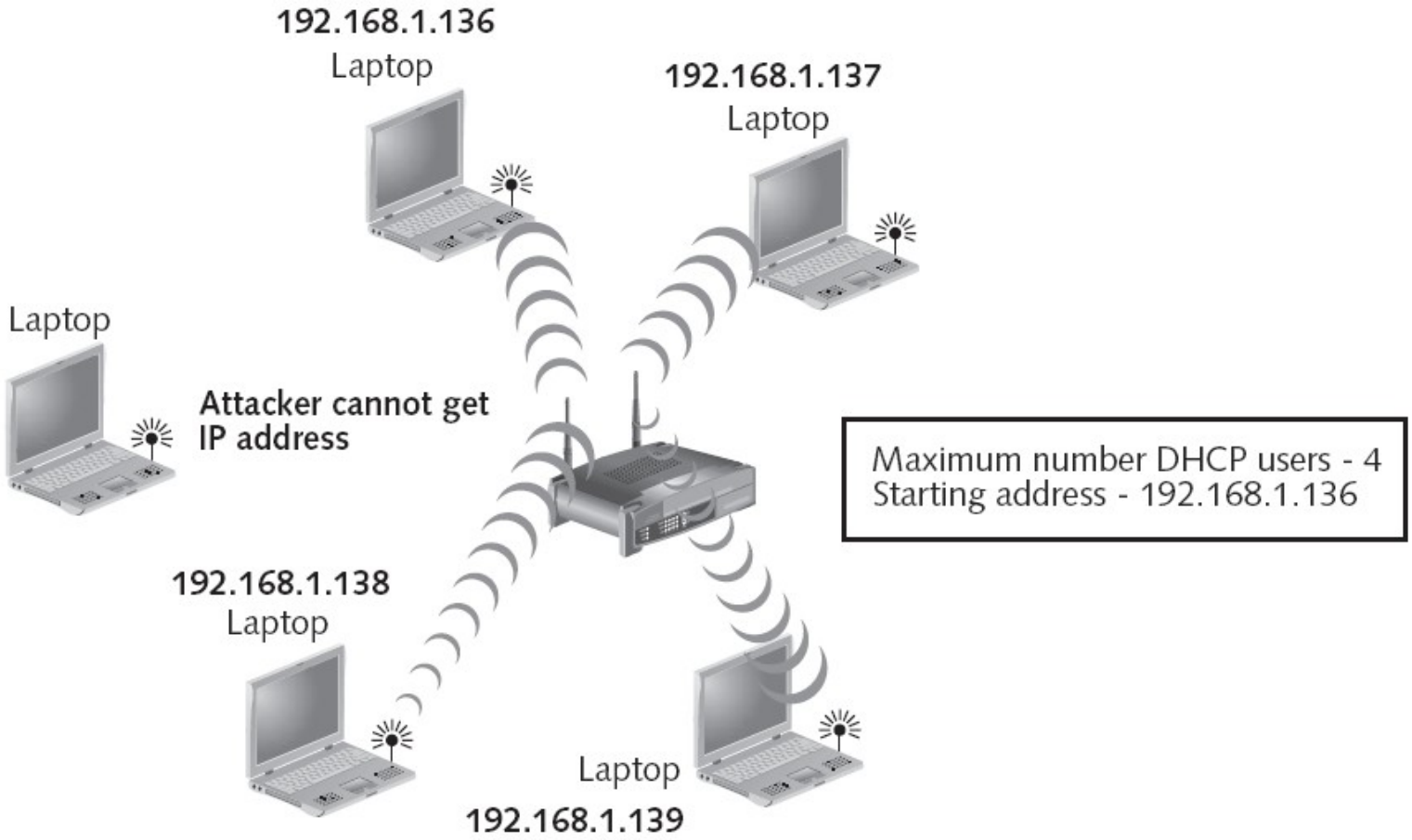


Figure 5-4 Maximum number of DHCP users

WEP Encryption

- Should be turned on
  - If no other options are available for encryption
- The longest WEP key available should be used for added security
  - Most vendors have the option of a 128-bit WEP key
- There is evidence that WEP passphrase generators may create predictable keys

WEP Encryption (continued)

Table 5-4 Transitional security model

Category	Security mechanism	Security level
Authentication	Shared key authentication	Low
Authentication	Disable SSID beaconing	Low
Authentication	MAC address filtering	Low
Authentication	DHCP restrictions	Low
Encryption	WEP	Low

Summary

- Additional security solutions
  - IEEE 802.11i
  - Wi-Fi Protected Access (WPA)
  - Wi-Fi Protected Access Version 2 (WPA2)
- IEEE 802.11i standard provided a more solid wireless security model
  - Uses AES and IEEE 802.1x port security
- WPA is a subset of 802.11i and addresses both encryption and authentication
  - Uses Temporal Key Integrity Protocol (TKIP) and a Message Integrity Check (MIC)

Summary (continued)

- The transitional security model should be implemented only as a temporary solution