Wi-Fi Security

WEP/WPA

TOPICS

- Objectives
- WEP
- WPA
- TKIP
- Improvements of WPA over WEP
- IEEE 802.11i

Objectives

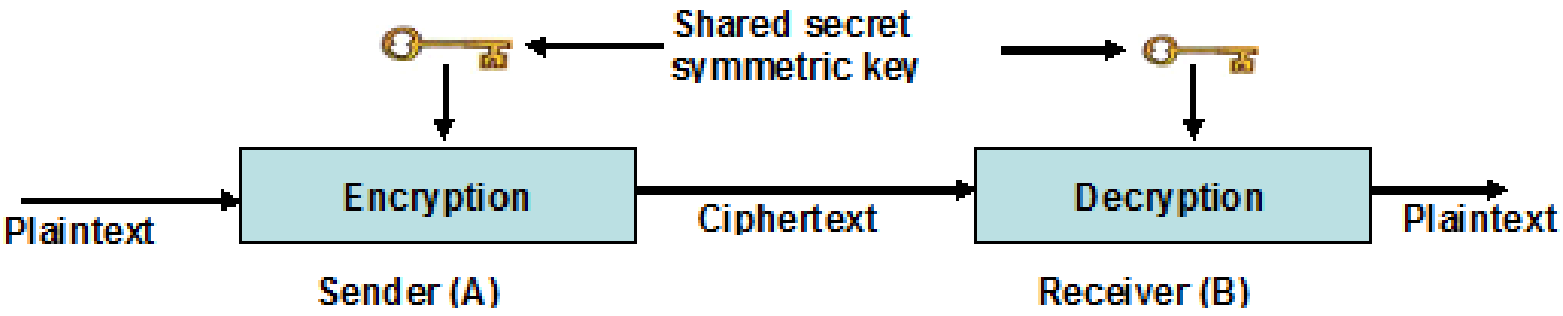
- To Understand the functionality and weakness of WEP.
- To Understand the functionality WPA and the role of TKIP in WPA.

1. Security Issues in Networks

- The five main security issues are as follows:

1. Authentication
2. Authorisation
3. Confidentiality
4. Integrity
5. Non-repudiation

Symmetric Key Encryption

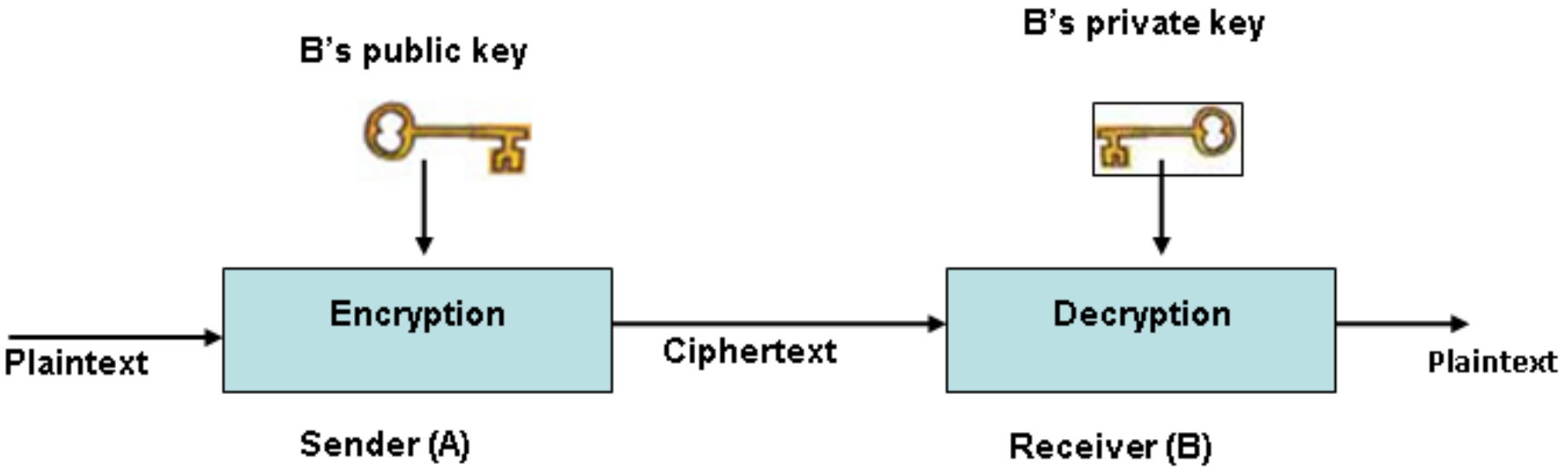


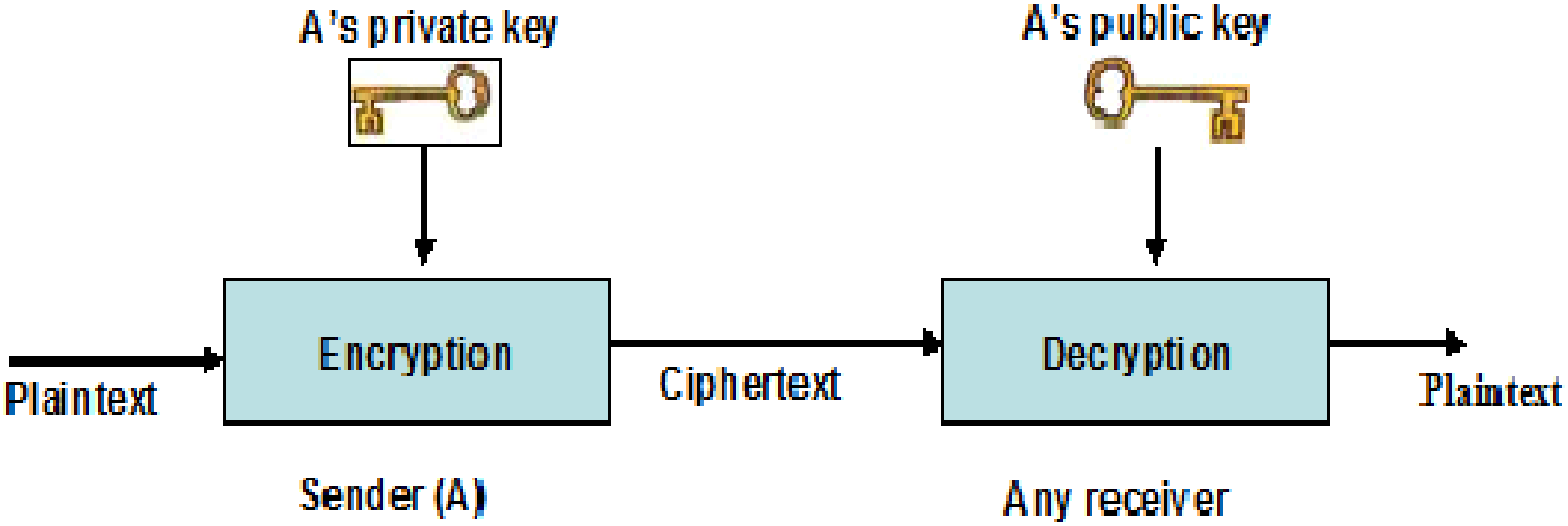
Encryption using bit-by-bit XOR

Plaintext: 0 1 1 0 0 1 1 0
Key: 1 0 1 1 0 0 1 1
Ciphertxt: 1 1 0 1 0 1 0 1
Same key: 1 0 1 1 0 0 1 1
Plaintext: 0 1 1 0 0 1 1 0

X	Y	X xor Y
0	0	0
0	1	1
1	0	1
1	1	0

Asymmetric Key Encryption





- public key' consists of two binary integers: k & n.
- These are the 'Public key' itself (k)
- and the associated 'public key modulus' n.
- n is chosen to be the product of two large prime integers, i.e. $n = p \times q$
- where p and q are large PRIME integers which must be kept secret.
- The private key is a binary number 'd' which cannot be deduced from d and k with feasible computation unless p and q are known (which they will not be).

- To encrypt a binary integer m < n with the public key, compute as :

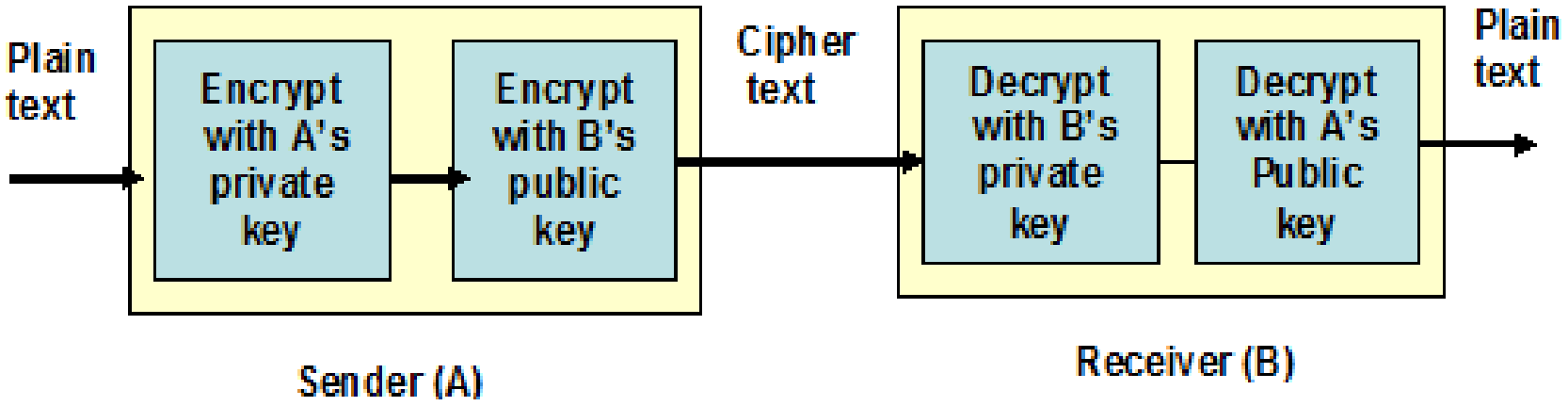
$$e = m^k \text{ modulo } n$$

- To decrypt 'e', using the corresponding private key' d' and the known modulus 'n', compute as:

$$m = e^d \text{ modulo } n$$

d must be such that $m^{kd} = m$ modulo n, or equivalently $m^{kd-1} = 1$ modulo n. Modulo n means 'remainder after dividing by n'.

Public and private key encryption may be used for combined confidentiality



Wireless LANs (802.11) Security

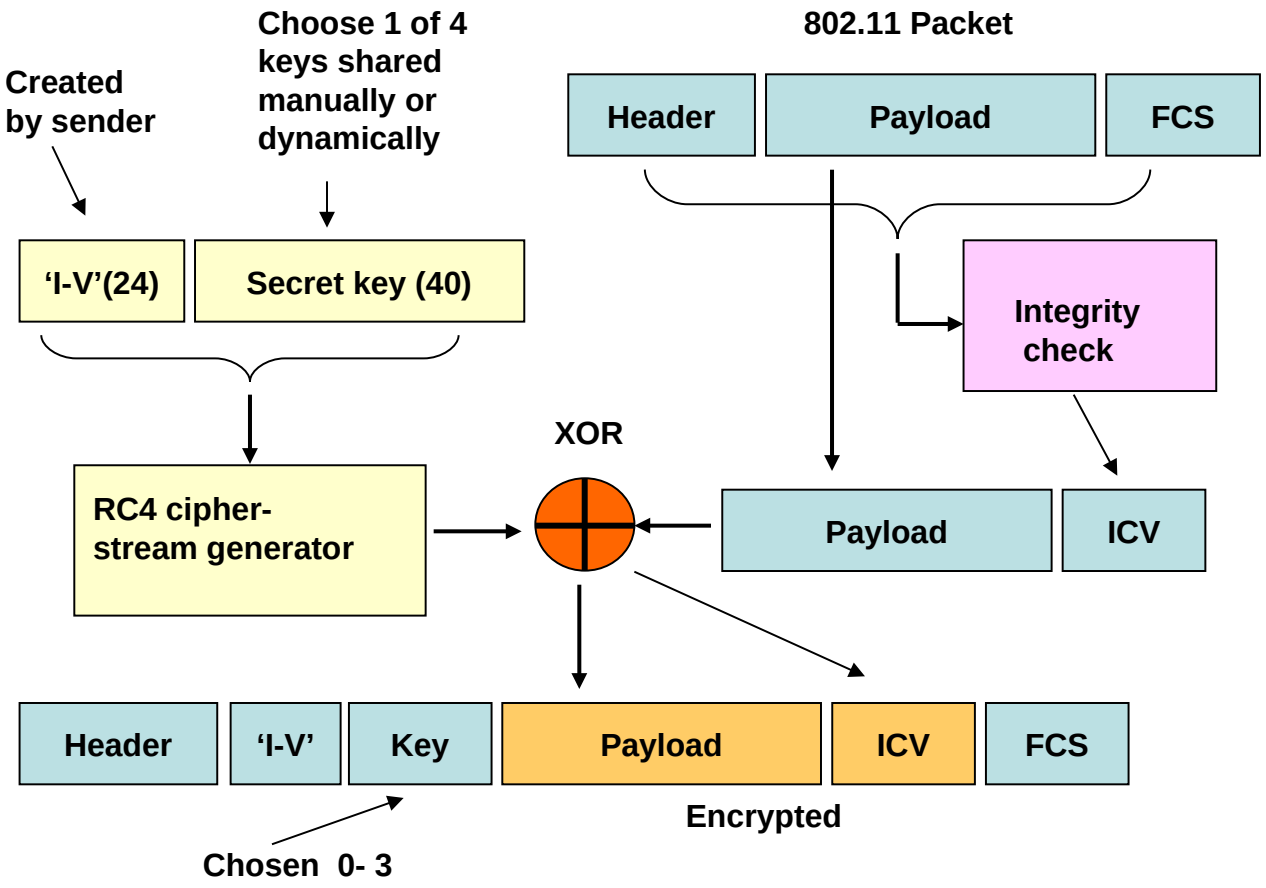
Access to WLAN provided by:

- SSID
- MAC-address filtering
- WEP

A bock diagram illustrating the components of WEP is given below:

1. Confidentiality; 2. Integrity; 3. Authentication

Note: WEP-keys were limited to 64-bit with 24 bits for the I-V, and 40 for the shared secret key. The integrity check (ICV) is appended to the payload



ICV – Integrity Check Vector
FCS – Frame Check Sequence

INTRODUCTION

- IEEE has introduced 802.11 standard for wireless LAN.

- The use of wireless raises big security issues:
  - How do we keep intruders from:
    - Reading our traffic?
    - Modifying our traffic?
    - Accessing our network?

- In1997 IEEE 802.11 spec called for an optional security mechanism called Wired Equivalent Privacy (WEP)
  - WEP was only intended to give wireless users the level of security implied on a wired network.
  - Packets are encrypted with 64/128-bit RC4 cipher stream.
    - 40/104-bit WEP key (symmetric , secret)
    - 24-bit Initialization Vector (IV)
  - Easy to crack
  - Multiple weakness : Key Management, Collisions, Message Injection, Authentication Spoofing.

Limitations of WEP

- Secret Key lack of a standardised distribution mechanism
- Original manual distribution led to infrequent key updating
- ‘Dynamic WEP’, using two frequently refreshed keys
- The use of a (CRC)
- The initialisation vector (I-V)
- The I-V is only 24-bit long
- Some choices of I-V (‘weak’ I-Vs)
- Originally, WEP-keys were limited to 64-bit with 24 bits for the I-V, and 40 for the shared secret key.

Illustration of security weakness when same RC4 bit-stream is repeated

Assume we have messages A & B encrypted by the same RC4

$$[A \text{ xor } R] \text{ xor } [B \text{ xor } R] = [A \text{ xor } B] \text{ xor } [R \text{ xor } R]$$
$$= [A \text{ xor } B] \text{ xor } [0 \ 0 \ 0 \ \ldots \ 0]$$
$$= A \text{ xor } B$$

What happened here?

Illustration of security weakness when same RC4 bit-stream is repeated

Assume we have messages A & B encrypted by the same RC4

$$[A \text{ xor } R] \text{ xor } [B \text{ xor } R] = [A \text{ xor } B] \text{ xor } [R \text{ xor } R]$$
$$= [A \text{ xor } B] \text{ xor } [0\ 0\ 0\ \ldots\ 0]$$
$$= A \text{ xor } B$$

The encryption has been cancelled out,
though we still have a problem deducing A and B.

Example Exercise

Let's Think!

Two bytes are known to have been encrypted by the same 8-bit RC4 stream producing

$C_1 = 1110\ 1011$
$C_2 = 1111\ 1111$

The bytes are believed to be capitalised vowels 'A':41(Hex) 'E':45, 'I':49, 'O':4F 'U':55.
What are they? What is the 8 bit key?

Solution

C_1 xor C_2 = 0001 0100

Which combination of two vowels will produce 0001 0100. **Think!!**

'A' 0100 0001
'E' 0100 0101
'I' 0100 1001
'O' 0100 1111
'U' 0101 0101

One of them has to be 'U' to produce 0001 XXXX
So the other must be 'A'.
They can be in either order.
If C_1 corresponds to ''A', the key is: 'A' xor C_1 = 1010 1010 ,
or if C_1 corresponds to 'U' , the key is 'U' xor C_1 = 1011 1110

Just to check: 'U' xor C_2 = 1010 1010 Same as 1st key
'A' xor C_2 = 1011 1110 Same as 2nd key

Exercise 2

Let's Think!

Two 3 character words are known to have been encrypted by the same 24 bit RC4 stream producing:

C1 = 1101 1110 1100 0010 1010 1001
C2 = 1101 1001 1100 1111 1010 1001

Assuming that one of the two words is one of three commonly found English words in EMAILs:
'the', 'sex' & 'mp3'
find the other & the key.

Note: Use the table of ASCII character codes

Solution

From a table of ASCII chartacter codes:

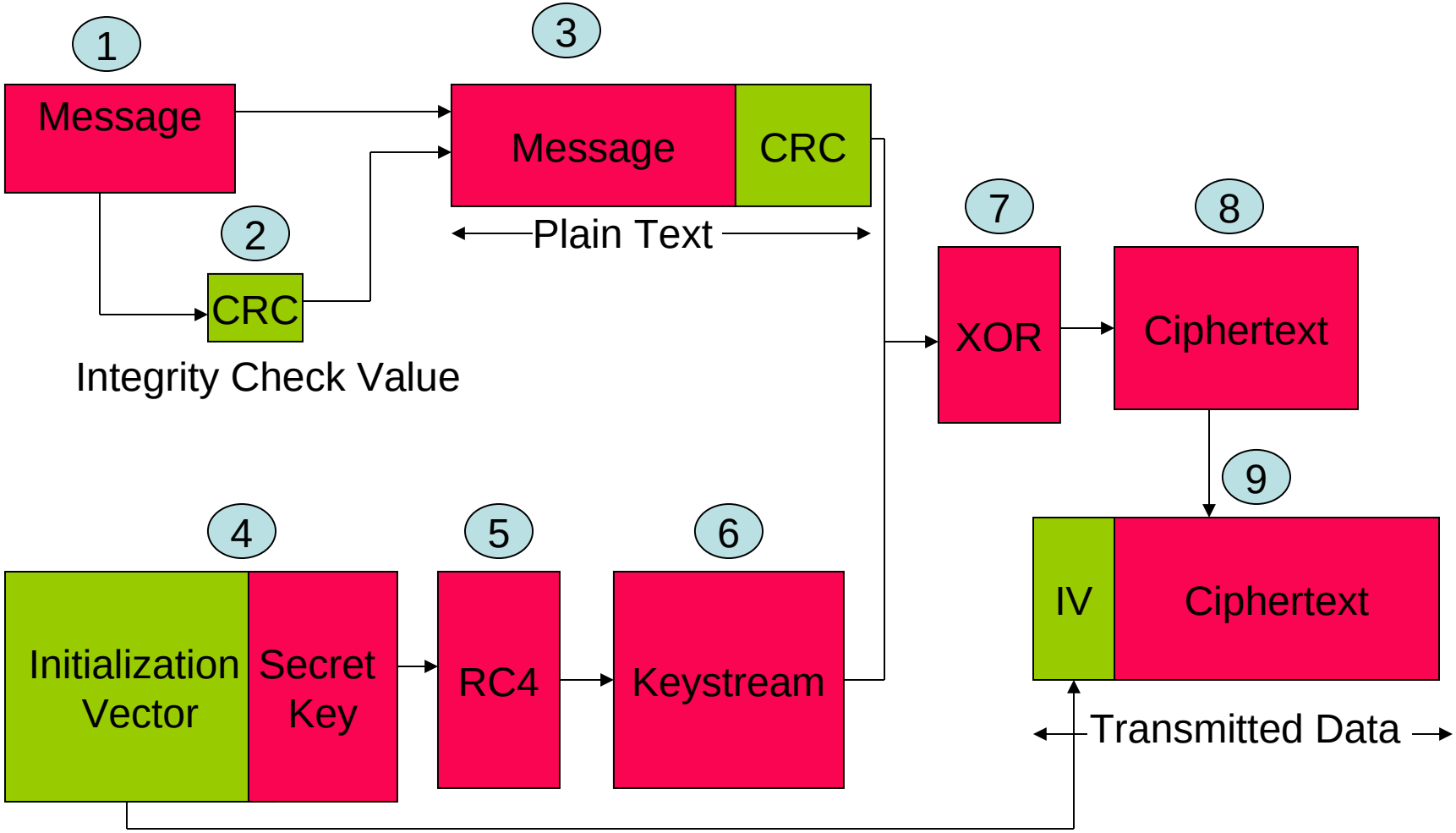
‘t’ 0111 0100 ‘h’ 0110 1000 ‘e’ 0110 0101
‘s’ 0111 0011 ‘e’ 0110 0101 ‘x’ 0111’ 1000’
‘m’ 0110 1101 ‘p’ 0111 0000’ ‘3’ ‘0011 0011’

C1 xor C2 = 0000 0111 0000 1101 0000 0000 = E say

E xor ‘the’ = 0111 0011 0110 0101 0110 0101 ‘see’
E xor ‘sex’ = 0111 0100 0110 1000 0111 1000 ‘thx’
E xor ‘mp3’ = 0110 1010 0111 1110 0011 0011 ‘j)3’.

So C1 must be ‘the’ & C2 is: ‘see’ (or vice versa)
Key is C1 xor ‘the’ = 10101010 10101010 11001100
or C1 xor ‘see’

Another illustration to show How WEP works:



Encryption

- In order to transmit a Plaintext Message M
- WEP performs a 32-bit CRC checksum operation on the message c(M).
- Concatenate c(M) to the end of message M.
- Pick an IV v and a secret key k which the sender and receiver share.
- Plug v+k combination into RC4 Pseudo-Random Number Generator (PRNG).
- A key stream sequence is generated.
- XOR (M,c(M)) with the key stream get the cipher text.
- V is prepended to the cipher text and included as a part of the transmitted data.

Decryption

- Decryption is the same as encryption, but in reverse.
- Take the v, which is sent in the clear text and prepend it to the secret key.
- Plug (v,k) in to the RC4 cipher to regenerate key stream.
- XOR key stream with the cipher text, to get (M’,c’)
- Check to see if c’=c(M’)
- If it is, accept M’ as the message transmitted.
- If it is not, then the packet is assumed to have been tampered with and discarded.

Initialization Vector

- To avoid encrypting two Plain texts with the same key stream, an Initialization Vector (IV) is used to augment the shared secret key and produce a different RC4 key for each packet.
- Drawback: IV is too short
  - It is 24- bit which results in 16.7 million(2^24) ,
    - in a high traffic Network , the entire IV space can be used in a matter of hours.
  - Forced to repeat IVs and violate RC4's cardinal rule of never repeating keys.
  - IV selection is not specified in standard.

CRC-32

- To ensure that a packet has not been modified in transit, it uses an Integrity Check (IC) field in the packet
- The Integrity check field is implemented as CRC-32 checksum, which is part of the encrypted payload of the packet.
- Drawback: CRC-32 is linear
  - Flipping bit “n” in the message, results in a deterministic set of bits in the CRC that must be flipped to produce a correct checksum on the modified message.
  - Because flipping bits carries through after an RC4 decryption, this allows the attacker to flip arbitrary bits in an encrypted message and correctly adjust the checksum so that the resulting message appears valid.

Key Management Problems

- WEP uses a symmetric key encryption mechanism.
- One of the problem with 802.11 protocol is that it does not address the issue of key management.
  - Example: Deploy WEP across a campus of 5000.
    - Each user must know the key and keep it a secret.
    - When a person leave a company or has a laptop stolen:
      - A new key must be given to all users and re-entered in their client configuration.

    An attacker gets the key from one session, the same key can be used to decrypt any other session, because everybody is using the same key.

Collisions

- When an IV is reused, it is termed as a collision.
- When it occurs: The combination of the shared secret and the repeated IV, result in a key stream that has been used before.
- Key stream attack : If both cipher texts are known (presumably captured from sniffer data) and one plain text is known, then the second plain text can be derived.

Example

Plain text 10011001
Keystream 10101010
Cipher text 00110011

Plaintext 11100101
Keystream 10101010
cipher text 01001111

Ciphertext 00110011
Ciphertext 01001111
01111100

plaintext1 10011001
plaintext 11100101
01111100

Message Injection

- Injection of a fake message of the adversary choice into the wireless net so that it will be accepted by a receiver as genuine.
- Adversary just need to know a single plaintext and its corresponding encrypted packet.
- Able to create a new forged cipher text
- P2 xor (P1 xor c1)=c2

Example

- Plaintext1: 11010011
- Cipher text1: ⊕ 10100110
- Keystream: 01110101

- Plaintext2: ⊕ 00101101
- Keystream1: 01110101 → **Forged new cipher**
- Ciphertest2: 01011000

Authentication Spoofing

- The goal of the Access Point is to verify that a user joining the network really knows the shared secret key.
- Shared Key authentication Process is as follows:
  1. Upon Client request of authentication process, AP sends a challenge string to the Client (Unencrypted)
  2. Client sends back the challenge response, (Cipher text), by encrypting the challenge text with key.
  3. AP validates the challenge response and sends the client with success or failure message.

Authentication Spoofing cont..

- If an attacker monitors this negotiation process, he will know the plain text and its associated cipher text.
- Using this information,
  - He can perform Message Injection.
  - He can join the network as a valid user.

Available tools to crack WEP

- In 2005, a group from the U.S. Federal Bureau of Investigation gave a demonstration where they cracked a WEP-protected network in 3 minutes using publicly available tools
- Several software tools are available to compute and recover WEP keys by passively monitoring transmissions.
  - aircrack
  - Aircrack-ng (aircrack-ng is the next generation of aircrack)
  - AirSnort
  - WEPCrack
  - Weplab
  - KisMAC

Breaking WEP

$$\begin{aligned} \text{Cyphertext} \oplus \text{Plaintext} &= \text{Key} \oplus \text{Plaintext} \oplus \text{Plaintext} \\ &= \text{Key} \oplus [\text{Plaintext} \oplus \text{Plaintext}] \\ &= \text{Key} \oplus [0000..00] = \text{Key} \end{aligned}$$

WPA

1. TKIP
2. CBC_MAC / CCMP

WPA

- WPA (Wi-Fi Protected Access) was announced October 31, 2002
- User authentication
  - 802.1X + Extensive Authentication Protocol (EAP)
- Encryption
  - Temporal Key Integrity Protocol (TKIP)
  - 802.1X for dynamic key distribution
  - Message Integrity Code (MIC) ; Michael algorithm
- WPA = 802.1X + EAP + TKIP + MIC

Cont…

- Implement majority of 802.11i
- Acts as an intermediate step before full implementation of 802.11i (WPA2)
  - Same encryption standard : RC4
  - TKIP can implement by firmware
- Can be used:
  - With an 802.1X authentication server (distributes different keys to each user)
  - In less secure “pre-shared key” (PSK) mode (every user given the same pass-phrase)

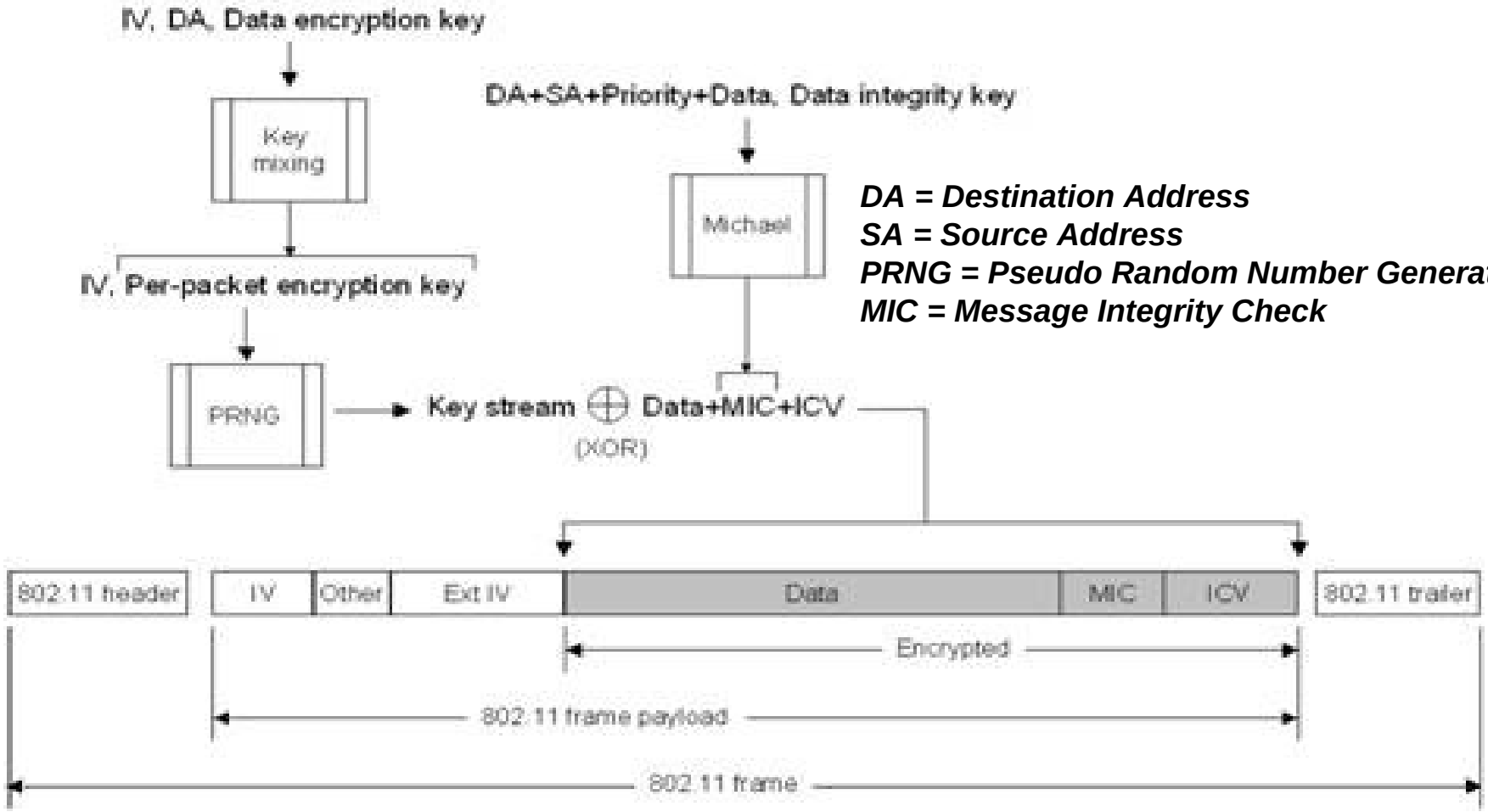
TKIP

- Replaces WEP with a new encryption algorithm
- TKIP, like WEP, uses a key scheme based on RC4
- TKIP provides:
  - per-packet key mixing
  - a message integrity check
  - a re-keying mechanism
- TKIP ensures that every data packet is sent with its own unique encryption key

TKIP Problem

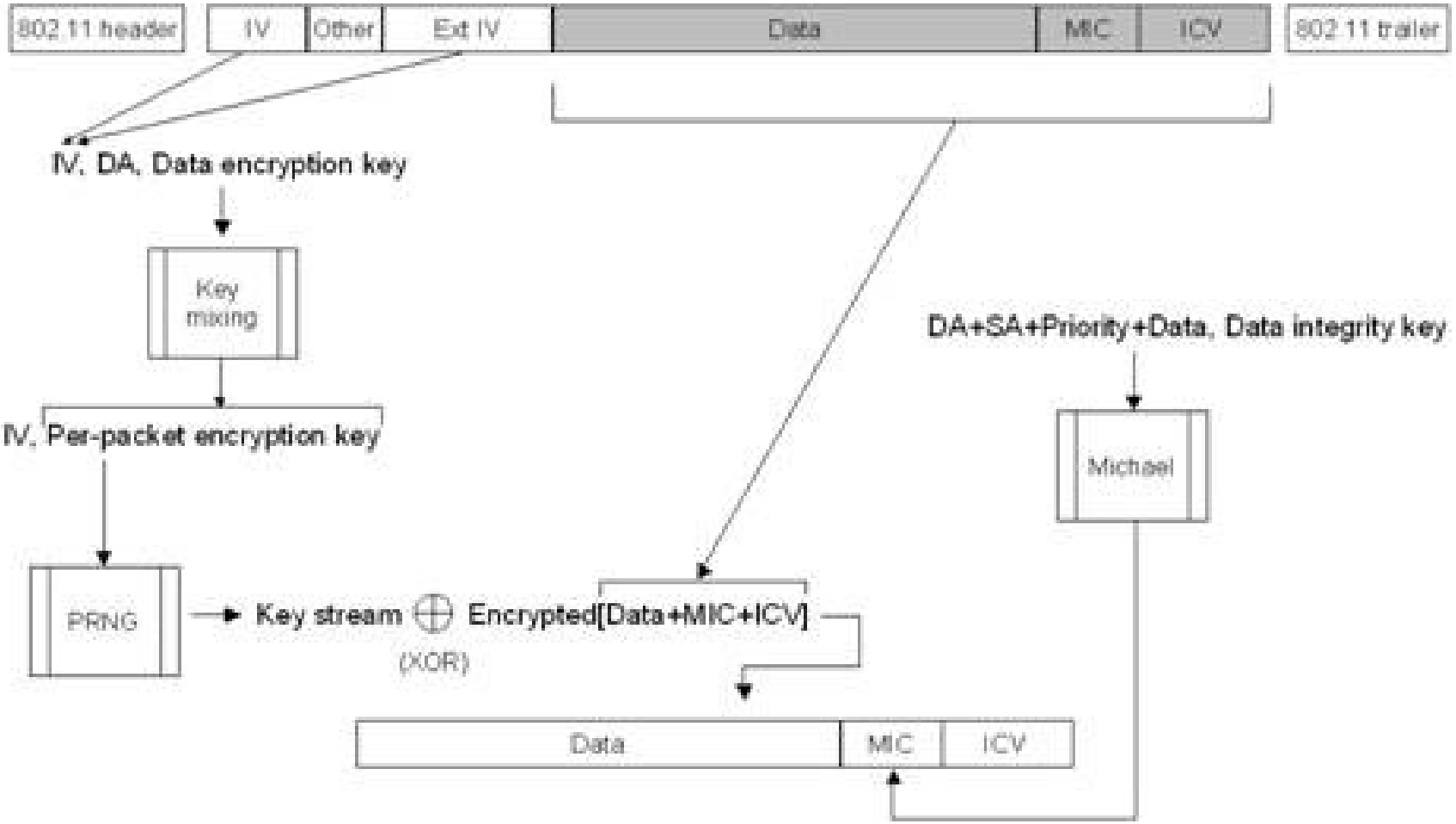
- TKIP hashes the Initialization Vector (IV) values, which are sent as plaintext, with the WPA key to form the RC4 traffic key, addressing one of WEP's largest security weaknesses

WPA Encryption Process



DA = Destination Address
SA = Source Address
PRNG = Pseudo Random Number Generator
MIC = Message Integrity Check

WPA Decryption Process



Improvement of WPA

- Initialization Vector (IV) is too short
- Weak data integrity
- Uses the master key rather than a derived key

- IV has been doubled in size to 48 bits in TKIP
- CRC-32 checksum calculation has been replaced with Michael
- TKIP and Michael use a set of temporal keys that are derived from a master key and other values

WPA2

- Interoperable implementation of the full 802.11i as WPA2, also called RSN (Robust Security Network).
- MIC in TKIP replaced by CCMP
- RC4 replaced by AES

WPA2 Characteristic

- CCMP
  - an IEEE 802.11i encryption protocol
  - uses the Advanced Encryption Standard (AES) algorithm
- Key length 128 bits (AES)

Improvement of WPA2

- Initialization Vector (IV) is too short
- Weak data integrity
- Uses the master key rather than a derived key

- IV has doubled in size to 48 bits in AES CCMP
- AES CBC-MAC algorithm provide strong data integrity
- AES CCMP uses a set of temporal keys that are derived from a master key and other values

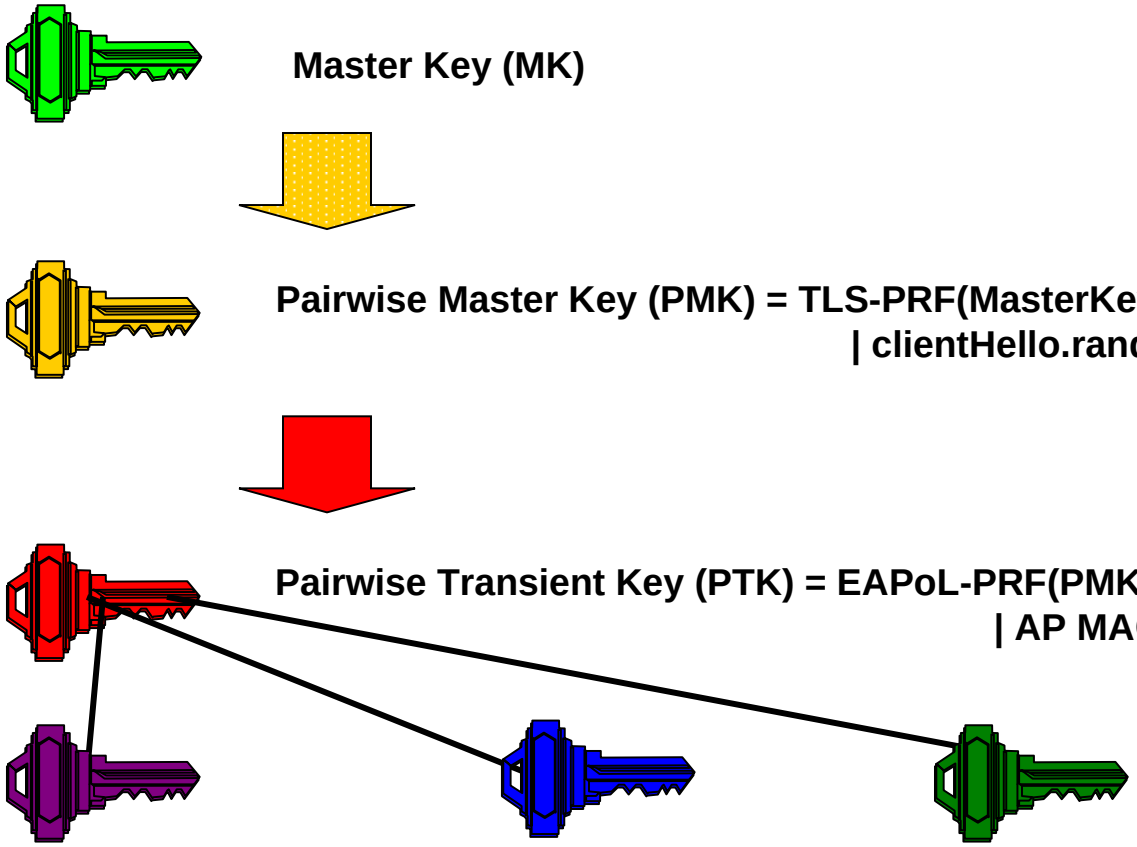
IEEE 802.11i

- IEEE 802.11i was ratified in summer 2004 and is now a finalized amendment to the 802.11 standard.
- The 802.11 I architecture contains the following components:
  - 802.1X/Extensible Authentication Protocol (EAP)
  - RSN for keeping track of associations.
  - Advanced Encryption Standard (AES) based Cipher Block Chaining-Message Authentication Code protocol (CCMP) to provide confidentiality , integrity and origin authentication.
  - Four-way Handshake

Key Hierarchy

- The 802.11i RSNA has two different key hierarchies that are used to protect either unicast or multicast/broadcast type traffic.
  - Unicast traffic is protected by Pairwise key hierarchy.
  - Broadcast traffic is protected by Group key hierarchy.

Pairwise Key Hierarchy



Pairwise Keys

- Master Key : It represents positive access decision
- Pairwise Master Key : It represents authorization to access 802.11 medium
- Pairwise Transient Key : Collection of operational keys:
  - **Key Confirmation Key (KCK):** It is used to bind PTK to the AP, STA; used to prove possession of the PMK
  - **Key Encryption Key (KEK) :** It is used to distribute Group Transient Key (GTK)
  - **Temporal Key (TK) :** It is used to secure data traffic

Group Keys Hierarchy

- Group Keys Hierarchy is made up of two components:
  - **Group Master Key (GMK):** It is derived by the access point and securely distributed to other authorized devices.
  - **Group Transient Key (GTK):** Its value is derived by running inputs, including the GMK through pseudo-random function process to generate the group temporal key
- 802.11i specification defines a “Group key hierarchy”
  - Entirely gratuitous: impossible to distinguish GTK from a randomly generated key

Key Distribution

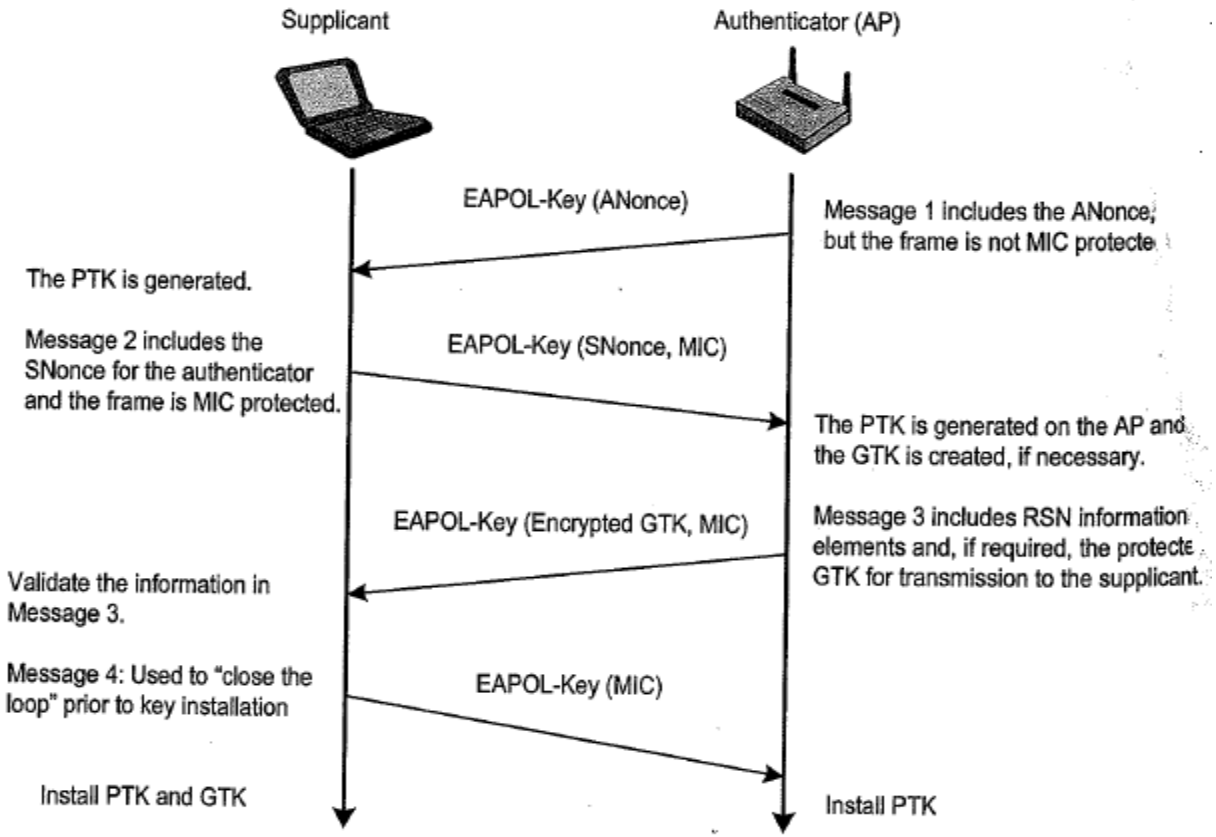
- Multiple Key distribution processes are defined in the 802.11i amendment and can be categorized in to three areas:
  - 4-way Handshake
  - Group Key Handshake
  - STAKey Handshake
- To facilitate the three handshake processes, EAPOL-key frames are used to perform various key related services.

EAPOL Key Frame

- Extensible Authentication Protocol over LAN (EAPOL)- Key frames are created from a number of fields totaling roughly ten different components.
- Of them, few fields are briefly described as follows:
  - Replay counter : It is used to sequence GTK updates, detect replayed STA requests
  - Key RSC: where to start the replay sequence counter (required for broadcast/multicast)
  - Key MIC : Message Integrity Code, to prove data origin authenticity
  - Nonce : It is used to establish liveness, key freshness
  - IV : when used, to make key wrapping scheme probabilistic.

4-Way Handshake

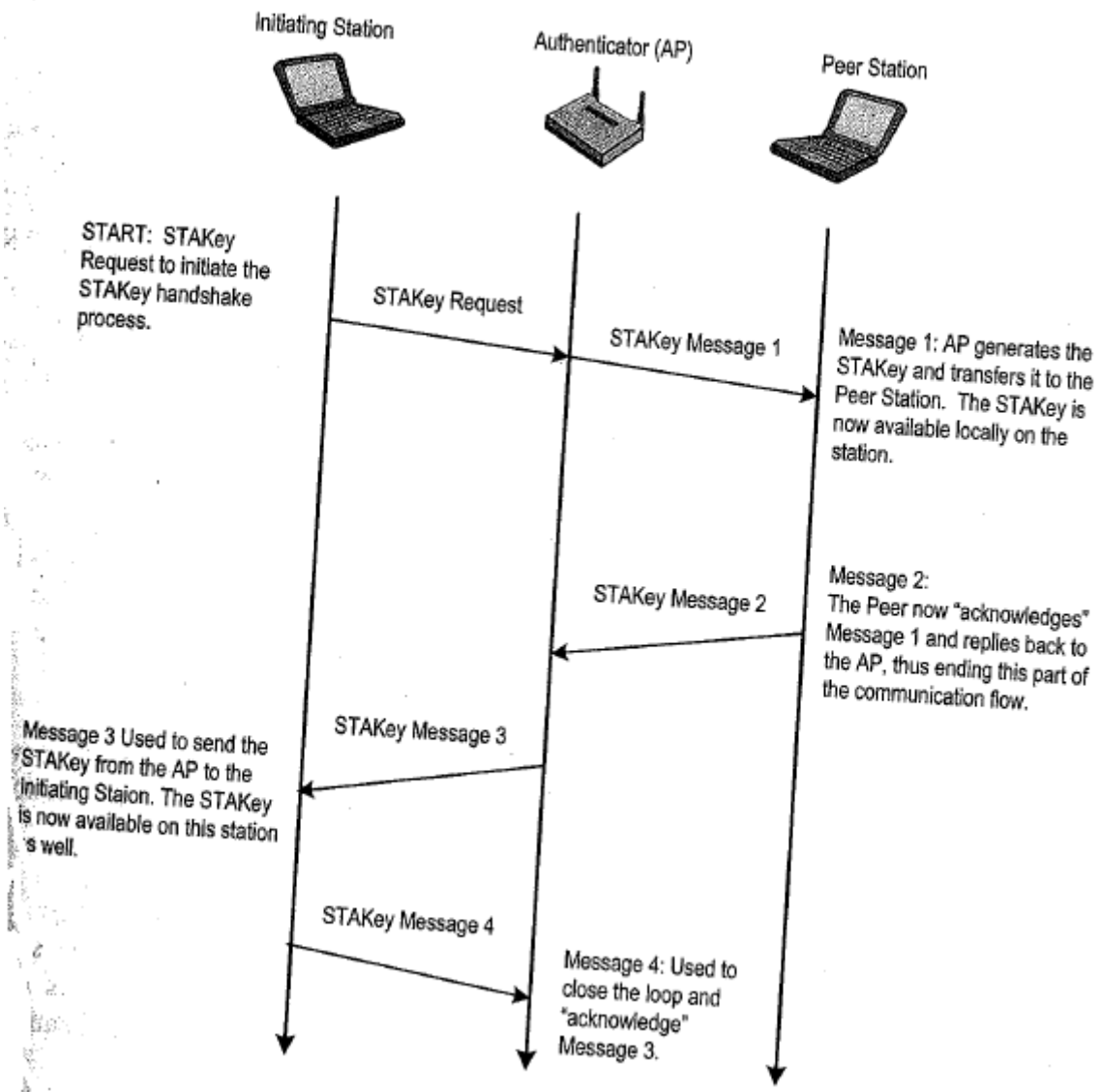
1. First the suplicant completes open authentication and association with the WLAN.
2. Next the higher level authentication (EAP or PSK) is processed to generate the PMK.
3. Third, the 4-Way Handshake is processed (illustrated below) to install the PTK and GTK



Group Handshake

- Group Handshake process has two steps:
  - EAPOL-Key is sent from the Authenticator to the supplicant with the encrypted GTK information.
  - A reply message is sent from the supplicant after the GTK has been installed, thus notifying the authenticator that it can receive GTK encrypted messages.

STAKey Handshake



Conclusion

Five aspects of security have been introduced.

1. The concepts of symmetric key & public key encryption have been explained
2. Although WLAN security is a vital issue it has not yet been fully addressed.
3. WEP is deeply flawed but still used.
4. IEEE 802.11i addresses improved security and was published in 2007
5. WPA and WPA2 are part of IEEE802.11i, and IEEE801.X is also incorporated.

Conclusion

- Numerous effective attack vectors and freely available exploit tools have sped the descent of WEP and rendered it ineffective.
- WPA leverages a number of firmware based security features centering on providing dynamic WEP via TKIP.
- The ultimate goal of IEEE802.11i is to ensure that a truly secure option is available to adequately provide confidentiality, integrity, authentication and replay protection services for the WLAN.