# Csci388 Wireless and Mobile Security – Wireless LAN: Introduction, WEP

Xiuzhen Cheng
cheng@gwu.edu

## Outline

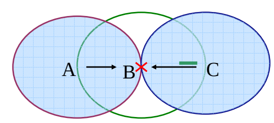
- Challenges in Wireless Communications
- Introduction to IEEE 802.11 Wireless LAN
- Break (5 minutes)
- The Insecurity of WEP

## Uniqueness of Wireless Communication

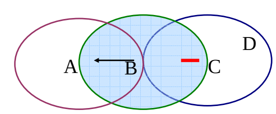
- **Uniqueness of Wireless Communication**
  - Interference and Noise; Full connectivity can not be assumed; Battery usage; Security
- **Requirements of a wireless MAC standard:**
  - Single MAC to support multiple PHY mediums
  - Robust to interference
  - Need to deal with the hidden/exposed terminal problem
  - Need provision for time bounded services
  - Support for power management to save battery power
  - Ability to operate world wide: ISM band (915M, 2.45G, 5.8G)

## Problems of wireless networks

- **Hidden Terminal**
  - Decrease throughput
  - Increase delay
- **Exposed Terminal**
  - Decrease channel utilization
- **Limited energy**
  - Network partition
- **Mobility**
- **Security**




At B: Transmission from C collides with transmission from A




C unnecessarily defers its transmission to D

## Basic Technology Concepts WiFi b-a-g

802.11b- 11Mbps DSSS, 2.4GHz spectrum, failovers to 5.5, 2, 1 Mbps

802.11a- 54Mbps max, 5GHz spectrum, failovers to 48, 36, 24, 18, 12, 6Mbps

802.11g -54Mbps max, 2.4GHz spectrum, backward compatible with 802.11b

## Basic Technology Concepts Wi-Fi b-a-g

802.11d- Extensions in other Regulatory Domains

802.11e -MAC Enhancements-Security/QoS

802.11f- Inter-Access Point Protocol

802.11h- Spectrum Managed 802.11a, European compatible

802.11i- Enhanced Security (TKIP and 802.1x)

## Basic Technology Concepts WiFi b-a-g

| | 802.11b | 802.11a | 802.11g |
|---|---|---|---|
| Frequency band | 2.4GHz | 5GHz | 2.4GHz |
| Max data rate | 11Mbps | 54Mbps | 54Mbps |
| availability | Worldwide | US | Worldwide |
| Interference sources | Cordless phone<br>Microwave oven<br>Bluetooth | Hiperlan devices | Cordless phone<br>Microwave oven<br>Bluetooth |

The Rules of Thumb of Radio
Higher data rates usually imply shorter transmission range
Higher power output increases range, but increases power consumption (less battery life)
The higher the frequency, the higher the data rate (but smaller range).

## Basic Technology Concepts WiFi b-a-g

| | 802.11b @100Mw | 802.11a @40Mw | 802.11g *estimates* |
|---|---|---|---|
| 50 ft | 11Mbps | 54Mbps | 54Mbps |
| 100 ft | 11Mbps | 36Mbps | 36Mbps |
| 125 ft | 11Mbps | 12Mbps | 11Mbps |
| 150 ft | 5.5Mbps | 6Mbps | 5.5Mbps |
| 250 ft | 2Mbps | | ? |
| 350 ft | 1Mbps | | |

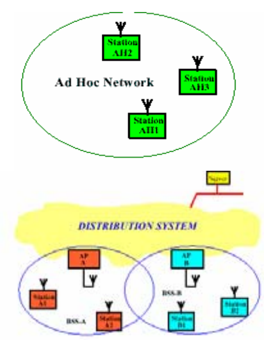
## 802.11 Protocol Summery

http://en.wikipedia.org/wiki/IEEE_802.11

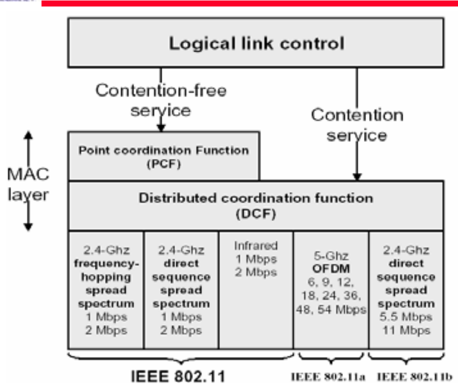
| Protocol | Release Date | Op. Freq. | Throughput (Typ) | Data Rate (Max) | Modulation Technique | Range (Radius indoor) Depends, # and type of walls | Range (Radius Outdoor) Loss includes one wall |
|---|---|---|---|---|---|---|---|
| Legacy | 1997 | 2.4G | 0.9Mbps | 2Mbps | | ~20m | ~100m |
| 802.11a | 1999 | 5G | 23Mbps | 54bps | OFDM | ~35m | ~120m |
| 802.11b | 1999 | 2.4G | 4.3Mbps | 11Mbps | DSSS | ~38m | ~140m |
| 802.11g | 2003 | 2.4G | 19Mbps | 54Mbps | OFDM | ~38m | ~140m |
| 802.11n | June 2009 (est.) | 2.4G 5G | 74Mbps | 248Mbps | | ~70m | ~250m |
| 802.11y | June 2008 (est.) | 3.7G | 23Mbps | 54Mbps | | ~50m | ~5000m |

## 802.11 System Architecture

- **Two basic system architectures**
  - Ad hoc
  - Infrastructure based
- **Access Point**
  - Stations select an AP and "associate" with it
  - Support roaming
  - Provide other function
    - time synchronization (beaconing); power management, PCF;




## 802.11 Protocol Stack

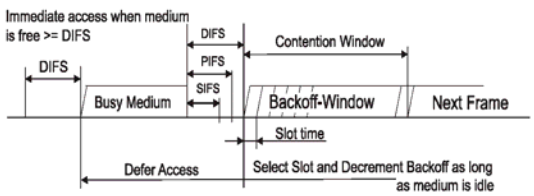



## 802.11 MAC Layer

- **Three basic access mechanisms**
  - CSMA/CA; **DCF(CSMA/CA+RTS/CTS); PCF**
  - **DIFS: lowest priority, asynchronous data**
  - **PIFS: media priority, time-bounded service**
  - **SIFS: highest priority, short control message**
- **Carrier sense at two levels**
  - **Physical carrier sense: done by physical layer**
  - **Virtual carrier sense at MAC layer using Network Allocation Vector (NAV) set while RTS/CTS/Data/Ack are overheard:** Intend to solve problem of Hidden and Exposed terminal
  - **Reduces collision by deferring transmission if any of the carrier sense mechanisms sense the channel busy**

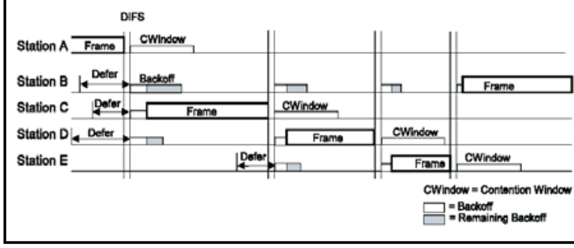
## DCF Basic Access

- **Basic Access**
  - **When a STA has data to send, it senses medium**
  - **The STA may transmit a MAC Protocol Data Unit (MPDA) when medium idle time is greater or equal to DIFS**
  - **If medium is busy, wait for a random backoff time**
  - **Two-way handshake: DATA/ACK**




## DCF

- **Backoff Procedure**
  - **Backoff procedure is invoked for a STA to transfer a frame but the medium is busy**
  - **Set *Backoff Timer* to be random backoff time**
  - **Backoff Timer start decreasing after an idle time of DIFS following the medium busyness**
  - **Backoff Timer is suspended when medium is busy, and won't resume until the medium is idle for DIFS**
  - **A frame may be transmitted immediately when Backoff Timer is 0**

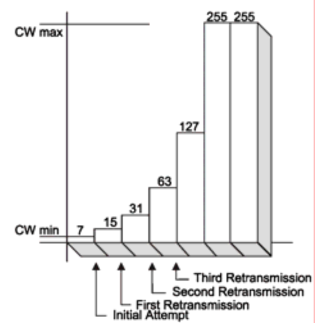



## DCF

- **Recovery procedures**
  - Collision may happen during contention
  - When collision happens, retransmission with a new random selection of the backoff time, contention window is doubled.
  - No special rights for retransmission

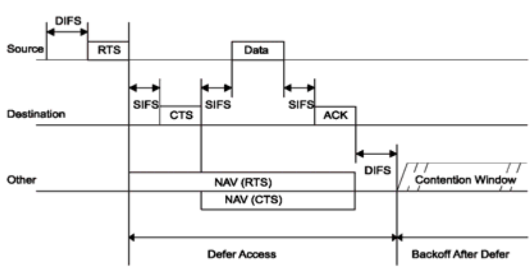
## DCF

- **Random backoff time=random()xaSlotTime**
  - aSlotTime: the value of the correspondingly named PHY characteristic (20µs for DSSS)
  - Random(): a random integer uniformly distributed over [0, CW]
- **CW (contention window)**
  - Increases exponentially after each retry fails (so does average backoff time. Why to do this?)
  - Keep constant after reaching the maximum
  - Reset after a successful transmission



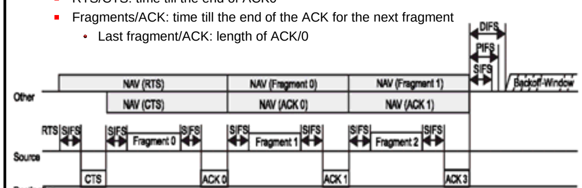

## DCF RTS/CTS Scheme

- **RTS/CTS Scheme**
  - Four way handshake: RTS-CTS-DATA-ACK
- **NAV (Network Allocation Vector)**
  - An indicator, maintained at each STA, for the period that transmission will not be initiated
- **Setting and resetting NAV according to "Duration" in MAC header when receiving a valid frame**




## DCF – Fragmentation

- **Control of the channel**
  - Once the STA has contented for the channel, it shall continue to send fragments until
    - All fragments of a MSDU or MMPDU have been sent
    - An ACK is not received
    - STA is restricted from sending additional fragments by PHY layer
- **Duration field**
  - RTS/CTS: time till the end of ACK0
  - Fragments/ACK: time till the end of the ACK for the next fragment
    - Last fragment/ACK: length of ACK/0



## PCF

- **Only available for infrastructured architecture, why?**
- **PCF is on top of DCF**
- **Super frame contains a contention-free period and a contention period**
- **Procedure (assume the media is just free):**
  - Point coordinator (PC) polls s1 after PIFS; s1 replied with data
  - PC continues to poll other stations
  - After no reply from a station, PC waits for PIFS time, then continues to poll other stations
  - After finishing, send CFE message. Then contention period starts.
- **Question: how time-bounded service is provided?**

## IEEE 802.11 MAC Packet Structure

- **Packet Type: Management (00), Control (01), and Data (10)**
- **Subtype: In control – RTS, CTS, ACK, etc**
- **MAC frames can be transmitted between mobile stations, between mobile stations and an AP, and between APs over a DS**
- **Address Interpretation**

| To DS | From DS | Addr 1 | Addr 2 | Addr 3 | Addr 4 |
|---|---|---|---|---|---|
| 0 | 0 | DA | SA | BSSID | |
| 0 | 1 | DA | BSSID | SA | |
| 1 | 0 | BSSID | SA | DA | |
| 1 | 1 | RA | TA | DA | SA |

| Frame Control (2) | Duration ID (2) | Address 1 (6) | Address 2 (6) | Address 3 (6) | Sequence Control (2) | Address 4 (6) | Data (0-2312) | CRC (4) |
|---|---|---|---|---|---|---|---|---|

| Protocol version | Type | Subtype | To DS | From DS | More Frag | Retry | Power Mgmt | More Data | WEP | Order |
|---|---|---|---|---|---|---|---|---|---|---|

## MAC Synchronization

- **In infrastructure network:**
  - The AP is responsible for generating beacons which contains a valid time stamp
  - If the channel is in use,defer beacon transmission until it is free
    - Carrier sense and contention are needed but no ACK for broadcast.
    - No virtual carrier sense.


**Figure 1:** TSF for infrastructure networks in 802.11

## MAC Synchronization – (cont.)

- **Ad hoc Network:**
  - Every station is responsible for generating its beacon
  - All stations compete for transmission of the beacon using a standard random backoff algorithm
  - All others adjust their times according to the winning station

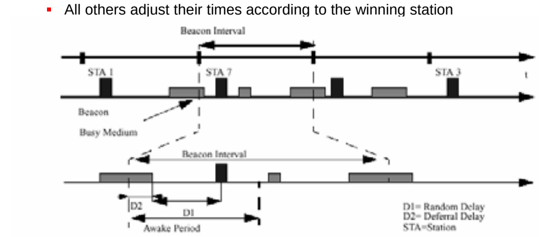


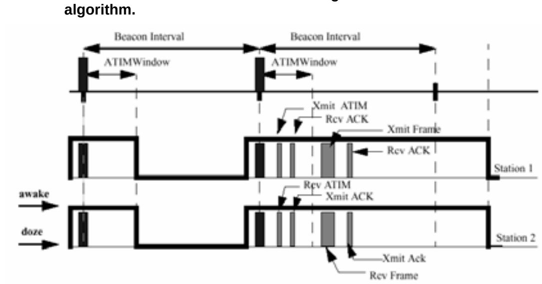

**Figure 2:** TSF for ad-hoc networks in 802.11

## Power Management

- Power states for a STA:
  - **awake - fully powered**
  - **doze – low power, cannot transmit/receive**
- PM in Infrastructure Networks
  - **when enter *doze* mode, STAs inform AP**
  - **AP buffers frames for STAs in doze mode**
  - **AP sends beacons periodically**
    - beacon contains time stamp + Traffic Indication Map (TIM)
  - **STA wakes up to get the beacon(check TIM)**
    - if traffic is pending, stay awake until transmission complete

## Power Management – (cont.)

- PM in Ad-hoc Networks
  - **ATIM window**
    - traffic for stations in *doze* mode is announced during ATIM window
    - all stations are awake during ATIM window
  - **both ATIMs and DATA are acknowledged and use standard backoff algorithm.**



## Connecting to An Access Point

- **Detecting an AP**
  - Beacons vs. probing
  - AP sends out beacons 10 times per second
    - User scanning all channels in turn to search for APs.
  - Users can send out "probe request message" for detecting a new AP
    - Compared to scanning, probing is faster
  - User select the AP with the best signal strength unless configured to connected to a specific AP
- **Authentication**
  - Users send authentication request
  - AP initiates a challenge-response protocol for authentication
- **Association – connecting to an AP**
  - Users send association request
  - AP replies with an association response
  - Roaming through disassociation and association messages

## Break

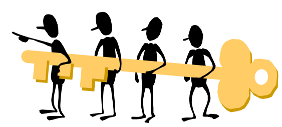
- **Question:**
  - When DHCP is applied in your home Wi-Fi network?

## The WEP Protocol

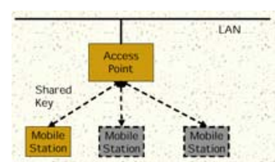
- **Security goals of the WEP (Wired Equivalent Privacy) protocol:**
  - Confidentiality: Prevent an adversary from learning the contents of your wireless traffic.
  - Access Control: Prevent an adversary from using your wireless infrastructure.
  - Data Integrity: Prevent an adversary from modifying your data in transit.
- **WEP Protocol was designed to protect the confidentiality of user data from eavesdropping**
- **Part of 802.11**
- **It has been integrated by manufacturers into their 802.11 hardware.**
- **Widespread in use.**

## The WEP Protocol (cont.)

- **Sender and receiver share a secret key k.**



- **Two classes of WEP implementation:**
  - classic WEP as documented in standard (40-bit key)
  - extended version developed by some vendors (128-bit key)




## The WEP Protocol (cont.)

- **In order to transmit a message M:**

  $P = \langle M, c(M) \rangle$

  pick Initial Vector(IV) v and generate RC4(v,k)—is a keystream

  $C = P \oplus RC4(v,k)$

  $A \to B: v, (P \oplus RC4(v,k))$

- **Upon receipt:**

  generate RC4(v,k)

  $P' = C \oplus RC4(v,k)$

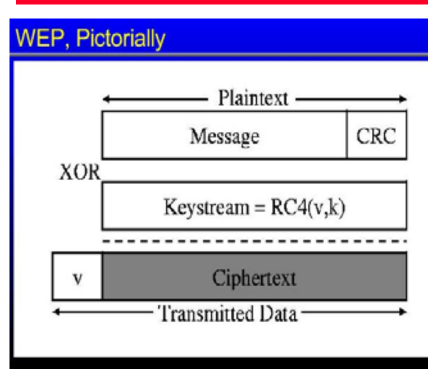
  $= P \oplus RC4(v,k) \oplus RC4(v,k)$

  $= P$

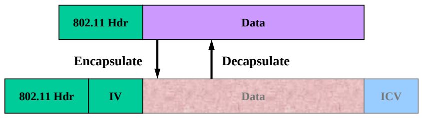
  check if c=c(M)

  If so, accept the message M as being the one transmitted

## WEP, Pictorially



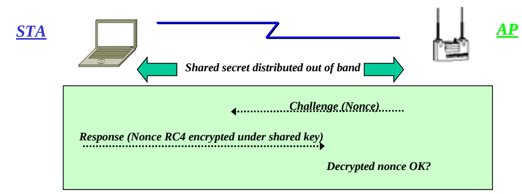
## WEP Encapsulation




WEP Encapsulation Summary:

- Encryption Algorithm = RC4
- Per-packet encryption key = 24-bit IV concatenated to a pre-shared key
- WEP allows IV to be reused with any frame
- Data integrity provided by CRC-32 of the plaintext data (the "ICV")
- Data and ICV are encrypted under the per-packet encryption key

## WEP Authentication




802.11 Authentication Summary:

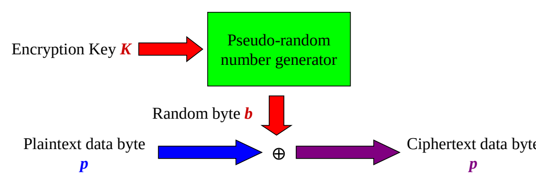
- Authentication key distributed out-of-band, it is the same as the encryption key
- Access Point generates a "randomly generated" 128-bit challenge
- Station encrypts challenge using pre-shared secret

## So What's Wrong with WEP?

- Properties of Vernam Ciphers (RC4)
- How to read WEP Encrypted Traffic
- How to authentication without the key
- Traffic modification
- Requirements for a networked data encapsulation scheme

## Properties of Vernam Ciphers (1)

The WEP encryption algorithm RC4 is a Vernam Cipher:




Decryption works the same way: $p = c \oplus b$

## Properties of Vernam Ciphers (2)

***Thought experiment 1***: what happens when $p_1$ and $p_2$ are encrypted under the same "random" byte $b$?

$c_1 = p_1 \oplus b$ $\qquad$ $c_2 = p_2 \oplus b$

Then:

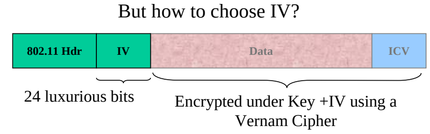
$$c_1 \oplus c_2 = (p_1 \oplus b) \oplus (p_2 \oplus b) = p_1 \oplus p_2$$

***Conclusion***: it is a very bad idea to encrypt any two bytes of data using the same byte output by a Vernam Cipher PRNG.

***Ever.***

## How to Read WEP Encrypted Traffic (1)

To overcome the keystream reuse attack, IV is introduced!
But how to choose IV?




- By the Birthday Paradox, the probability $P_n$ that two packets will share the same IV after n packets is $P_2 = 1/2^{24}$ after two frames and $P_n = P_{n-1} + (n-1)(1-P_{n-1})/2^{24}$ for n > 2. – IV value is randomly selected!
- 50% chance of a collision exists already after only 4823 packets!!!
- Pattern recognition can disentangle the XOR'd plaintext.
- Recovered ICV can tell you when you've disentangled plaintext correctly.
- After only a few hours of observation, you can recover all $2^{24}$ key streams.

## How to Read WEP Encrypted Traffic (2)

- **Ways to accelerate the process:**
  - Send spam into the network, wait for the victim to check emails over the wireless link – known plaintext attack
  - Get the victim to send e-mail to you
    - The AP creates the plaintext for you! – known plaintext attack
  - Decrypt packets from one Station to another via an Access Point
    - If you know the plaintext on one leg of the journey, you can recover the key stream immediately on the other
  - Etc., etc., etc.

## Key Stream Reuse / IV Reuse

- **Why IV?**
  - The ciphertext of the same plaintext should be different
  - The key stream for each packet/encryption should be different
- **Decryption Dictionaries**
  - A table of key streams indexed by the IV
  - With this dictionary, no key is needed to decrypt message
  - This attack survives even when key length is enlarged
  - Not hard since some network card such as PCMCIA card reset IV to 0 whenever the card is initialized.

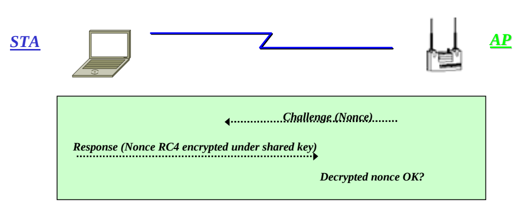
## RC4 Key Generation

- **Key setup**
  - Initialization of S-Box and K-Box for the key
    - S-Box contains 256 bytes of 0—255
    - K-Box contains the key repeated as needed
  - Use K to initially permute S-Box
    - For each byte (the jth byte) in the S-Box, compute j = j+Si + Ki mod 256, then swap Si and Sj. Initially j=0
- **pseudo-random number generation**
  - Generate the byte stream by swapping two elements in the S-box
  - Initialize i=j=0
  - i = (i+1) mod 256;<br>j = (j+Si) mod 256<br>Swap Si and Sj<br>k = (Si+Sj) mod 256<br>output byte Sk.

## RC4 Weak Keys

- **For certain key values, a disproportionate number of bits in the first few bytes of the key stream were determined by a few bits in the key itself [Fluhrer 01]**
  - Some bits of the key have a bigger effect than others
  - These key values are called weak keys, causing direct key attacks
    - The number of effect bits is reduced
    - The first few bytes of the plaintext are easier to be detected, therefore easier to get the first few bytes of the key stream
- **Countermeasures**
  - Discard the first few byes (see 256 bytes) of the RC4 key stream
  - Discussion: can we overcome this problem by not using any weak keys?

## How to Authenticate with the Key




With our background, an easy attack is obvious:

- Record one challenge/response with a sniffer
- Use the challenge to decrypt the response and recover the key stream
- Use the recovered key stream to encrypt any subsequent challenge

## WEP Authentication Fails!

- **Authentication is not a one-time process**
  - Authentication is only useful if you can prove it every time you communicate
  - A common approach is to perform full authentication on first contact and then provide a limited-life "identity badge" – why and how?
- **Authentication keys should be different than encryption keys**
  - The use of derived keys is recommended because master keys should rarely or never be exposed directly to attacker
  - WEP use the same key
- **Lacks mutual authentication**
  - Access point spoofing is easy – Rogue AP is common!
- **User identity spoofing since lack of method of preserving identify over subsequent transactions**
- **Provides plaintext-ciphertext free of charge**
  - Break the WEP encryption key
  - After getting the challenge/response message, an attacker can authenticate itself to the BS even no key is released.
- **Good news: Most systems don't use the futile WEP authentication phase anymore**

## Does WEP Provide Access Control?

- **Authentication does not equal to access control**
  - Authentication authenticates who you are only, no guarantee of access
- **No definition in 802.11**
- **Rely on a list of acceptable MAC addresses**
  - MAC address forging is easy
- **Rely on the shared key**
  - Shared by all users
  - Seldom change
- **Replay attack**
  - Sniffing the messages transmitted by a legitimate user from the very beginning
  - Replay latter after spoofing the MAC address when the legitimate user left
- **How to overcome this problem? – Give a simple countermeasure!**

## Traffic Modification (1)

***Vernam cipher thought experiment 2***: how hard is it to change a genuine packet's data, so ICV won't detect the change?

***Answer***: Easy as pie

Represent an n-bit plaintext as an n-th degree polynomial:

$$\boldsymbol{p} = p_n x^n + p_{n-1} x^{n-1} + \ldots + p_0 x^0 \qquad (\text{each } p_i = 0 \text{ or } 1)$$

Then the plaintext with ICV can be represented as :

$$\boldsymbol{p}x^{32} + \mathrm{ICV}(\boldsymbol{p}) = \boldsymbol{p}_n x^{n+32} + \boldsymbol{p}_{n-1} x^{n-31} + \ldots + \boldsymbol{p}_0 x^{32} + \mathrm{ICV}(\boldsymbol{p})$$

If the $n$+32 bit RC4 key stream used to encrypt the body is represented by the $(n+32)^{nd}$ degree polynomial $\boldsymbol{b}$, then the encrypted message body is

$$\boldsymbol{p}x^{32} + \mathrm{ICV}(\boldsymbol{p}) + \boldsymbol{b}$$

## Traffic Modification (2)

But the ICV is linear, meaning for any polynomials $p$ and $q$

$$\mathbf{IVC}(\boldsymbol{p}+\boldsymbol{q}) = \mathbf{ICV}(\boldsymbol{p}) + \mathbf{ICV}(\boldsymbol{q})$$

This means that if q is an arbitrary nth degree polynomial, i.e., an arbitrary change in the underlying message data:

$$(\boldsymbol{p}+\boldsymbol{q})x^{32} + \mathrm{ICV}(\boldsymbol{p}+\boldsymbol{q}) + \boldsymbol{b} = \boldsymbol{p}x^{32} + \boldsymbol{q}x^{32} + \mathrm{ICV}(\boldsymbol{p}) + \mathrm{ICV}(\boldsymbol{q}) + \boldsymbol{b}$$

$$= ((\boldsymbol{p}x^{32} + \mathrm{ICV}(\boldsymbol{p})) + \boldsymbol{b}) + (\boldsymbol{q}x^{32} + \mathrm{ICV}(\boldsymbol{q}))$$

***Conclusion***: Anyone can alter an WEP encapsulated packet in arbitrary ways without detection!!

## IP Address Redirection

- **Through message modification, is it possible to modify the destination IP address of a IP packet. Discuss how this can be done.**

## WEP Conclusions

- **Attacks on the Wired Equivalent Privacy protocol which defeat each of the security goals of:**
  - Confidentiality: We can read WEP-protected traffic.
  - Access Control: We can inject traffic on WEP-protected networks.
  - Data Integrity: We can modify WEP-protected traffic in transit.

## Definitions (1)

- **Wi-Fi defines a subset of IEEE 802.11 with some extensions**
  - Wi-Fi alliance was formed for interoperability of 802.11 products by different manufacturers
  - Wi-Fi test plan was created for testing in order for the manufacturers to obtain the Wi-Fi certificate
- **802.11i**
  - It is an addendum to the standard for security enhancement
  - Defines a new type of network called a **robust security network (RSN)**
    - Access point supports only RSN-capable product
  - For backward compatibility, a transitional security network (TSN) has been defined to support both WEP and RSN.

## *Definitions (2)*

- **Can't wait! The standardization of RSN takes time**
  - Create **TKIP – Temporal Key Integrity Protocol**
  - TKIP intends to upgrade current Wi-Fi equipments through software instead of throwing away all Wi-Fi equipments
  - TKIP is an option of RSN
- **A subset of RSN that specifies only TKIP has been adopted by the Wi-Fi alliance, called Wi-Fi Protected Access (WPA)**
  - Software upgrades are available for existing equipment to support WPA
  - New products are shipped with WPA

## *What's Next?*

- **Access Control: IEEE 802.1X, EAP**
- **Upper-Layer Authentication**
- **WPA and RSN key Hierarchy**
- **TKIP**
- **AES -- CCMP**