Mobility

- Wireless traffic is easy to eavesdrop
- Requires new security solutions
- Mobile phones: Network operator may not be same as service provider
- We will look at
  - GSM
  - UMTS
  - WLAN

GSM - Introduction

- Used by 2 billion people in more than 200 countries
- Security goals
  - Provide confidentiality for users – If the channel is eavesdropped it should not be possible to reconstruct messages.
  - Provide anonymity for users – It should not be possible to trace a user
  - Authenticate users – It should not be possible to spoof an identity
- Security requirements
  - Complexity added by security should be as small as possible
    - Bandwidth
    - Error rate
    - Overhead
  - Must be possible to use other networks in other countries

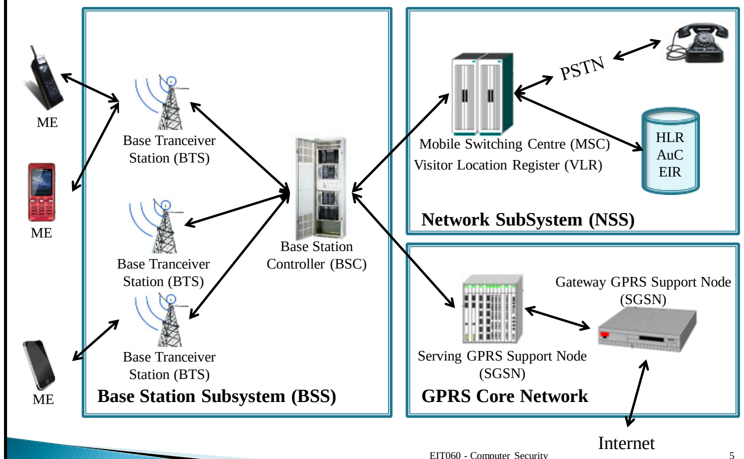
Mobile Station

- Consists of mobile equipment (ME)
  - Physical device
  - IMEI – International Mobile Equipment Identity
- SIM card – Subscriber Identity Module, Smart card with identifiers, keys and algorithms
  - K_i – Subscriber Authentication Key (Long term key)
  - IMSI – International Mobile Subscriber Identity
  - TMSI – Temporary Mobile Subscriber Identity
  - PIN – Personal Identity Number protecting a SIM
  - LAI – Location Area Identity

Some important parts of GSM

- *HLR – home location register*
  - Stores information about every SIM card issued by the operator. SIM identified by IMSI.
  - Stores current location of SIM
  - Sends data to VLR/SGSN when SIM roams
- *AuC – Authentication Center*
  - Manages authentication data for user
  - Stores K_i and algorithm ID (A3/A8)
  - Issues key for encryption
- *VLR – Visitor Location Register*
  - Serves a base station
  - Stores IMSI and TMSI
  - Updates HLR with location
- *EIR – Equipment Identity Register*
  - Keeps a list of banned IMEI
  - Used to track stolen phones

GSM Architecture

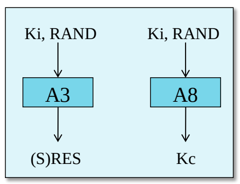


Subscriber Identity Protection

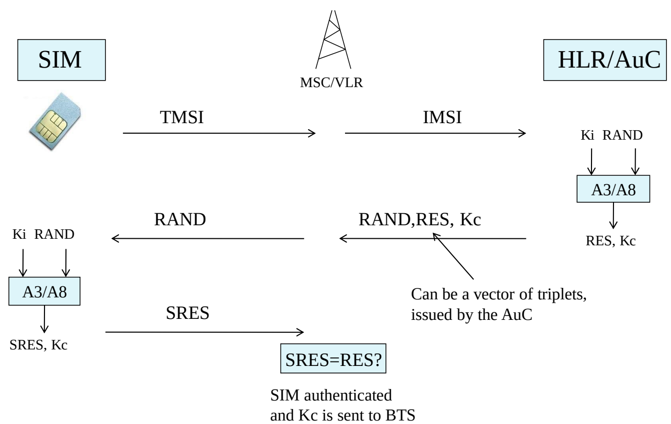
- If IMSI is always used for identification, then it is possible to track subscribers
  - Eavesdropping should not identify users
  - Network must identify users (someone has to pay the call)
- TMSI is used to identify a SIM
- Phone is switched on → IMSI is sent
  - SIM card receives a TMSI
  - All other times → TMSI is used
- VLR maps TMSI → IMSI
- New MSC → new TMSI

Authentication step

- Ki – subscriber identification key is stored in SIM and HLR/AuC
  - Size is 128 bits
- Goal
  - Authenticate subscriber to network
  - Create a session key
- Algorithm A3 computes response in authentication step
- Algorithm A8 computes 64-bit session key
- RAND is 128 bits
- (S)RES is 32 bits



Authentication Step

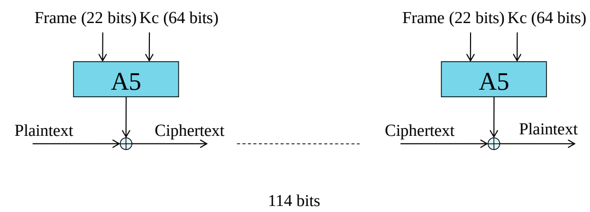


A3/A8

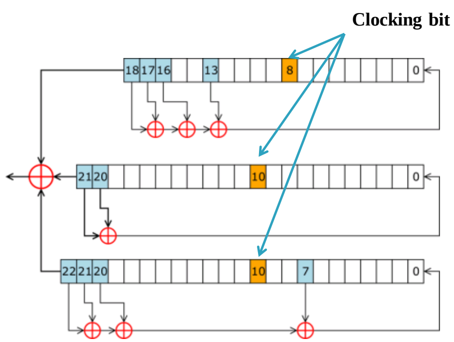
- A3 and A8 are implemented on the SIM
- Can be network specific, but example algorithms are proposed (COMP128)
- Independent of hardware manufacturers
- COMP128 was very weak.
  - Using Smart Card reader it was possible to get K_i
  - Possible to clone SIM cards
  - New versions were proposed

Encryption

- Encryption algorithms
  - **A5/1 – Strong version**
  - A5/2 – Weak version
  - A5/3 – Strong version (introduced later and based on Kasumi used in 3G)
- Traffic only encrypted between mobile station and base station



A5/1



Initialization: Load key and frame number by xoring them with bit 0
Keystream generation: Register is clocked if clocking bit is majority bit.

Note the small state:
Time-memory tradeoff feasible! (Some known plaintext is needed)

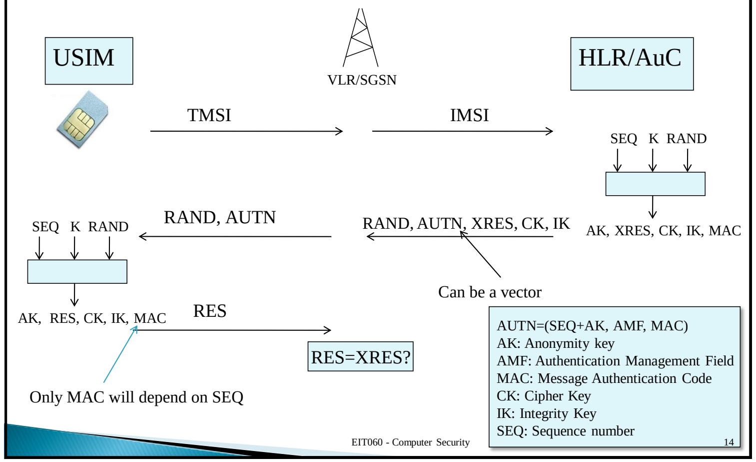
Secrecy of algorithms

- Kerckhoffs' principle – The secrecy of a message should only depend on the secret key!
- This well known principle from the 19th century was ignored
- If the algorithm is not investigated by public/researchers before deployment, how can we know it is secure?
  - COMP128 leaked out – was broken
  - A5/1 leaked out – was broken
- Another problem with GSM: Only users are authenticated, the network is not
  - Fake basestations can trick phones to send IMSI and/or turn off encryption

UMTS

- As far as we are concerned the architecture of UMTS is similar to the architecture of GSM
  - USIM – Universal subscriber identity module
  - Secret key K shared between USIM and HLR/AuC
- Goal of authentication step
  - Authenticate user
  - Create session key for encryption
  - **Authenticate network**
  - **Create session key for message authentication**
- **Do not keep algorithms secret**
- **128 bit session key**

Authentication and Key Agreement

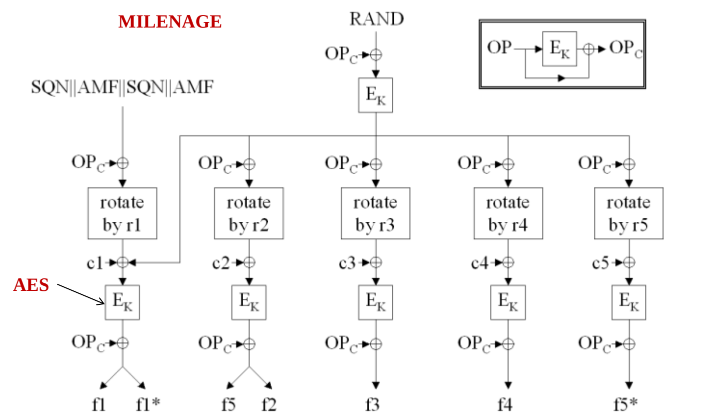


Functions used

- f0: Random number generator
- f1: Network authentication function. computes a MAC that is part of AUTN
- f2: User authentication function. Computes RES and XRES
- f3: Cipher key derivation function
- f4: Integrity key derivation function
- f5: Anonymity key derivation function. Used to hide sequence number
- f8: Stream cipher for session encryption
- f9: MAC for session integrity protection

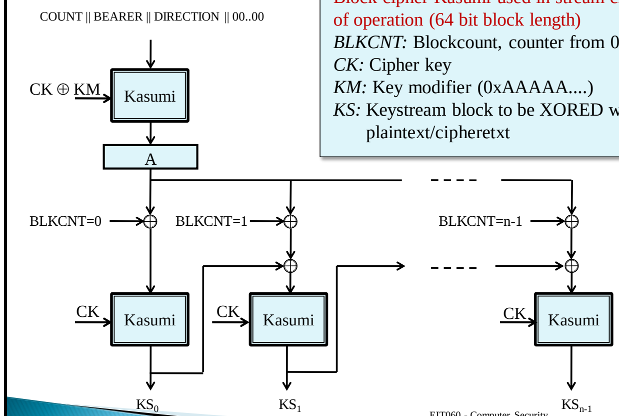
- f0 implemented in AuC
- f1-f5 are operator specific and implemented in USIM
- f8-f9 are mandatory for everyone and implemented in user equipment (phone)

Functions computed in AuC and USIM



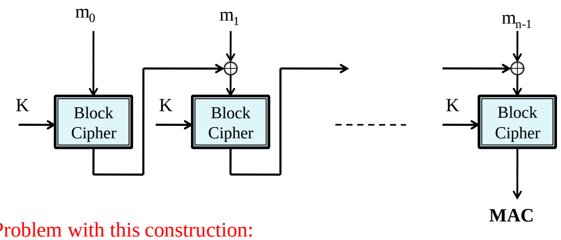
Encryption in UMTS (f8)

Block cipher Kasumi used in stream cipher mode of operation (64 bit block length)
BLKCNT: Blockcount, counter from 0 to n-1
CK: Cipher key
KM: Key modifier (0xAAAAA....)
KS: Keystream block to be XORED with plaintext/ciphertext



Message Authentication, CBC-MAC

- CBC-MAC – Block cipher in CBC mode with last ciphertext as MAC value

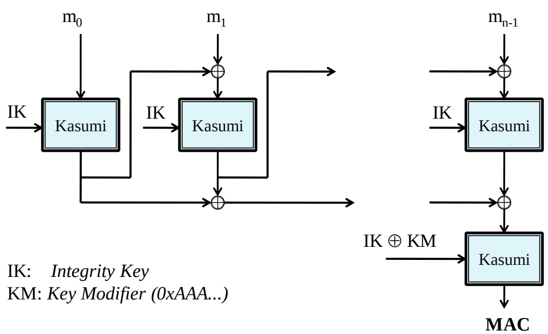


Problem with this construction:
Get message/MAC pair of a one-block message (m,t)

Then m || m+t also has MAC t,
→ (m || m+t, t) is a valid pair

MAC used in UMTS (f9)

- Only signalling data is authenticated
- CBC-MAC with output permutation and extra large state

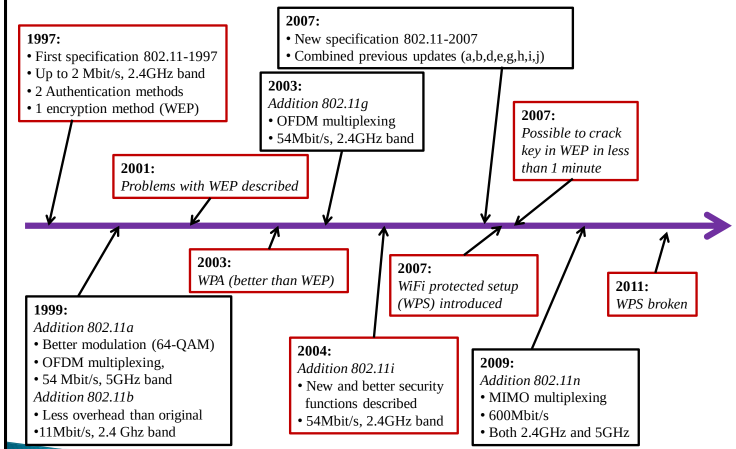


IK: *Integrity Key*
KM: *Key Modifier (0xAAA...)*

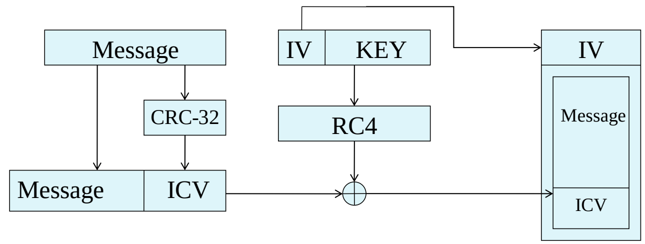
WLAN Security

- IEEE 802.11
- Security Requirements
  - Authentication
  - Confidentiality
  - Integrity
- Non-cryptographic access control
  - Hide SSID – Users will have to know the SSID
  - Restrict access based on MAC address
  - **Both are more or less worthless!**
- Cryptographic protection
  - WEP – Wired Equivalent Privacy
  - WPA – WiFi Protected Access
  - WPA2 – WiFi Protected Access 2

802.11 timeline



WEP encryption



- Integrity Check Value (ICV) based on linear cyclic redundancy check
- Encryption uses stream cipher RC4
- Size of IV is 24 bits
- Size of key is 40 or 104 bits
- Source of confusion: 64-bit WEP uses 40-bit keys and 128-bit WEP uses 104 bit keys

Weakness of CRC-32

- Message is divided by a degree 32 polynomial with coefficients in GF(2)
- Remainder is ICV
- Linear function – protects only against accidental changes if encryption is ”xor plaintext with keystream”
- Assume we want to add (xor) Δ to plaintext.
  - Compute δ = CRC-32(Δ)
  - Add ($\Delta \| \delta$) to ciphertext

$$\begin{aligned}(M \| \text{CRC-32}(M)) \oplus \text{RC4}(K) \oplus (\Delta \| \delta) &= (M \oplus \Delta \| \text{CRC-32}(M) \oplus \delta) \oplus \text{RC4}(K)\\ &= (M \oplus \Delta \| \text{CRC-32}(M \oplus \Delta)) \oplus \text{RC4}(K)\end{aligned}$$

- We still have a valid message

Weakness in encryption

- IV is only 24 bits
- After 2^{24} frames the IV will repeat. If the key is not changed the keystream will repeat.

$$C \oplus C' = \text{RC4}(IV \| K) \oplus P \oplus \text{RC4}(IV \| K) \oplus P' = P \oplus P'$$

- Much worse problem: RC4 does not define how to use IV so it was decided to concatenate the IV with key!
- It is possible to recover the key very fast using this setup
- It does not matter if it is 40 or 108 bit key, it is still easy to break.
- No defense against replay attacks
  - Makes it easy to gather lots of encrypted data

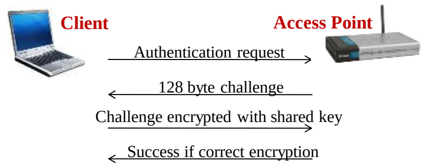
RC4

- Probably the most well known (and simplest) stream cipher
- Designed 1987 but kept secret, leaked out 1994
- Also referred to as ARC4 and ARCFOUR since the name RC4 is a trademark
- Many weaknesses have been found. Still, correctly used, it is not very weak.
- In SSL/TLS there is no IV in RC4. One stream is used for each key.

KSA($K[0\ldots\ell-1]$)	PRGA(K)
Initialization: For $i = 0 \ldots N-1$ $S[i] = i$ $j = 0$ Scrambling: For $i = 0 \ldots N-1$ $j = j + S[i] + K[i \bmod \ell]$ $Swap(S[i], S[j])$	Initialization: $i = 0$ $j = 0$ $S = KSA(K)$ Generation loop: $i = i + 1$ $j = j + S[i]$ Swap($S[i], S[j]$) Output $z = S[S[i] + S[j]]$

Authentication in WEP

- Open system authentication
  - Same as no authentication
  - Client sends identity to authenticator
  - Authenticator sends association message back
- Shared key authentication
  - Challenge response protocol using shared WEP key



Attack: Save *keystream* = *challenge* ⊕ *response* for an IV. Use same keystream for any new challenge and use same IV.

WPA and WPA2

- Wi-Fi protected Access
- First version (WPA) started to appear in APs around 2003
  - Designed to quickly fix the problems in WEP
  - Important that the same hardware could be used – only a software update was necessary
  - Based on 802.11i, but only a draft of it
  - Much stronger than WEP
    - Better authentication
    - Avoiding confidentiality and integrity problems in WEP
- Full implementation of 802.11i, using AES is called WPA2

802.11i Authentication

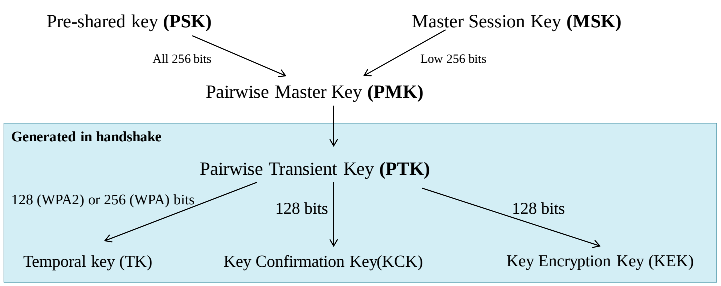
- Can use a specific server for EAP authentication
  - Supports several methods for authentication
  - More on this in the course ”Advanced Computer Security”
  - Authentication server constructs a **Master Session Key (MSK)**
- Can also use a pre-shared key (often called WPA-PSK)
  - Still keys are different for each user and each handshake
  - The **pre-shared key (PSK)** is derived from the password
  - Function used is called Password-Based Key Derivation Function 2 (PBKDF2)
  - Slow function → Key strengthening

PSK=PBKDF2(PRF,password,salt,iterations,output size)

- WPA uses PBKDF2(HMAC-SHA1, password, ssid, 4096, 256)

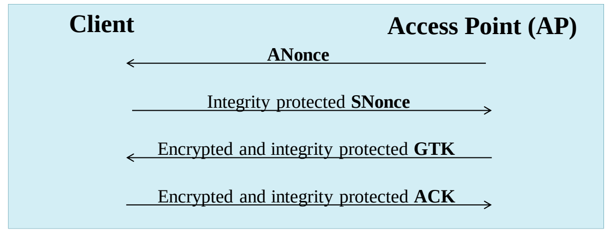
Keys in 802.11i

- A hierarchy of keys



AP also has a Group Master Key (GMK) used for broadcast messages

4-way handshake

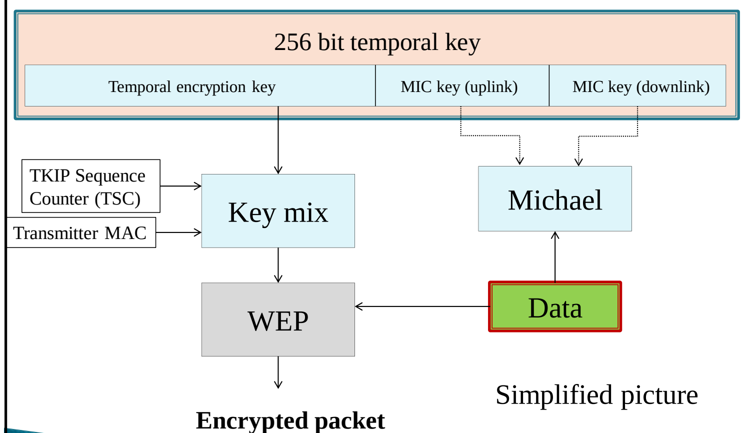


- PTK is hash of (PMK, MAC_{client}, MAC_{AP}, Anonce, SNonce)
  - Iterated SHA-1
  - Note that MAC here is *MAC address*
- Last two messages constructed such that *key confirmation* is provided
- Encryption and integrity protection in handshake uses KCK and KEK
- GTK is derived from GMK and updates every time someone leaves or enters the network

TKIP

- Temporal Key Integrity Protocol
- 256 bit temporal key divided into 128 bit encryption key and 2*64 bit integrity key (one for each direction)
- Message Integrity Code (MIC), Michael, is used
  - ”MIC” removes ”MAC” confusion in this context
- IV is increased to 48 bits and used as counter to prevent replay attacks
- New encryption key for every frame
  - Encryption key is mixed with counter
- WEP is still used
- Attacks on WEP are no longer possible

TKIP (WPA)



CCMP (WPA2)

- Fully implementing 802.11i
- RC4 is replaced by AES in CCMP mode
  - AES used in counter mode
  - CBC-MAC based on AES instead of MIC
- Same 128-bit temporal key used for both encryption and MAC
  - Authenticated encryption
- Require new hardware since completely new encryption algorithm is used

What's next?

- Exam 17/3, 14-19, Sparta A-D
- CEQ will be sent out the day after the exam (18/3)
  - Exam will be corrected immediately (about 4 days)
  - Results will be posted when CEQ response rate has reached 75% or at latest on Tuesday April 7.
- If you want more security courses
  - Web security HT1, 4hp,
  - Advanced computer security, HT1, 7.5hp
  - Advanced web security, HT2, 7.5hp
  - Cryptology, HT2, 7.5hp