LUND UNIVERSITY

EITA25 Computer Security (Datasäkerhet)
Mobility

PAUL STANKOVSKI WAGNER, EIT, 2020-03-02

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, 3GPP, LTE
  - WLAN

GSM - Introduction

- European standard, first deployed in 1991, still widely used
- Denoted 2G as it replaced NMT (1G)
- Security goals
  - Provide confidentiality for users – eavesdroppers cannot reconstruct messages
  - Provide anonymity for users – not possible to trace a user
  - Authenticate users – not 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

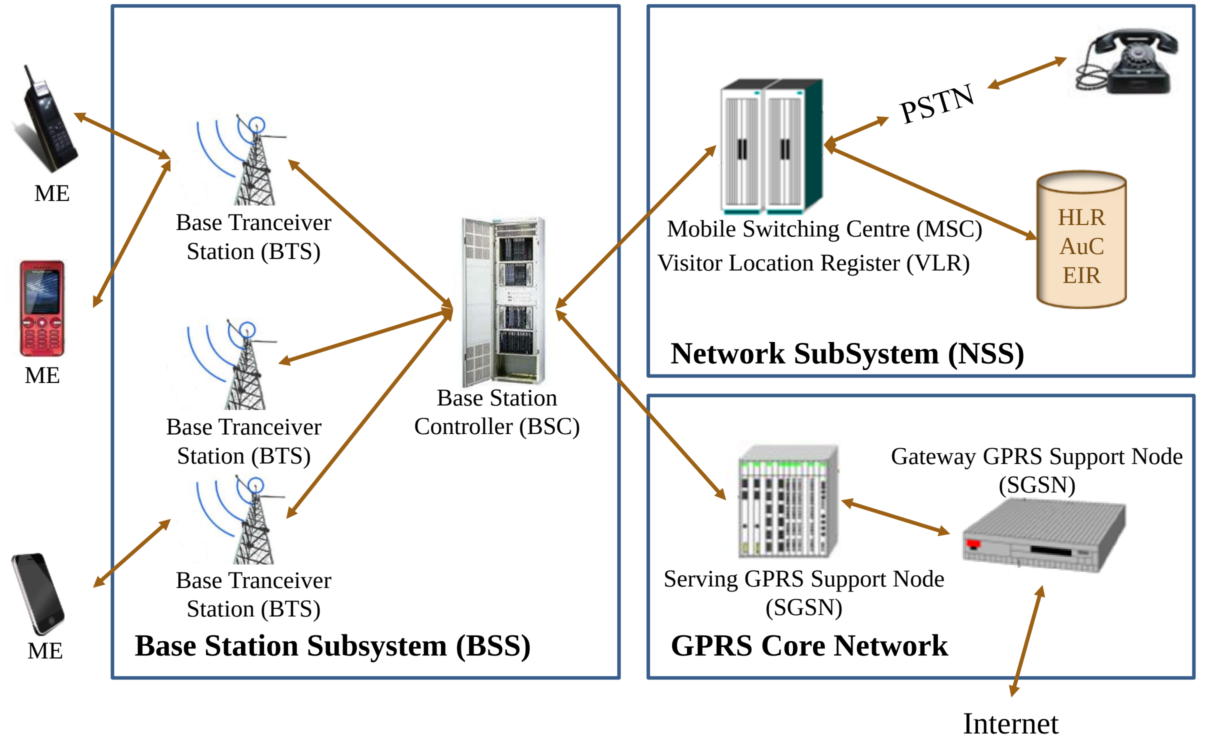
- Consists of mobile equipment (ME)
  - Physical device
  - IMEI – International Mobile Equipment Identity
- SIM card – Subscriber Identity Module, Smart card with identifiers, keys and algorithms
  - K_i – Subscriber Authentication Key (Long term key)
  - IMSI – International Mobile Subscriber Identity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

LUND UNIVERSITY

Some Important Parts of the Network

- 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
- VLR – Visitor Location Register
  - Serves a base station
  - Stores IMSI and TMSI
  - Updates HLR with location
- AuC – Authentication Center
  - Manages authentication data for user
  - Stores K_i and algorithm ID (A3/A8)
  - Issues key for encryption
- EIR – Equipment Identity Register
  - Keeps a list of banned IMEI
  - Used to track stolen phones

GSM Architecture

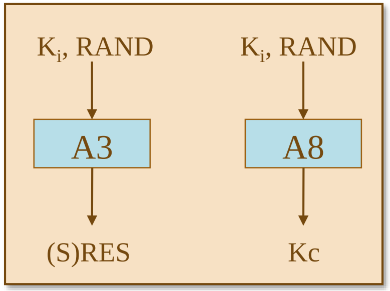


Subscriber Identity Protection

- 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

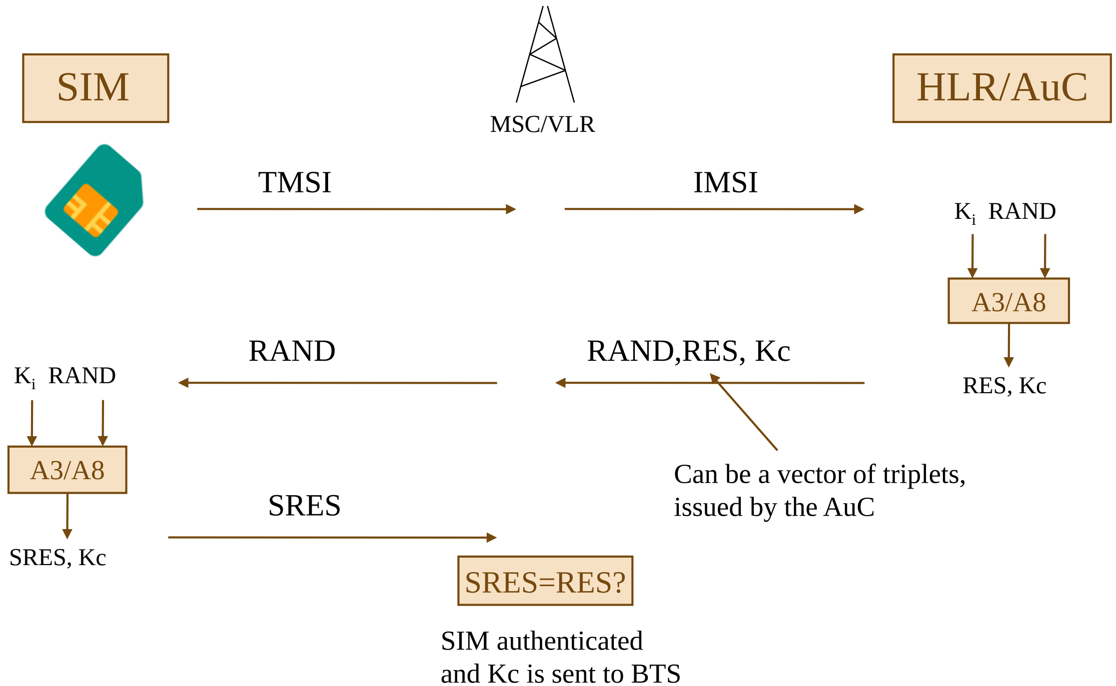
Authentication step

- K_i – subscriber identification key is stored in SIM and HLR/AuC
  - Size is 128 bits
- Goals
  1. Authenticate subscriber to network
  2. Create session key



- Algorithm A3 computes response in authentication step
- Algorithm A8 computes 64-bit session key
- RAND is 128 bits, generated by AuC
- (S)RES is 32 bits

Authentication Step



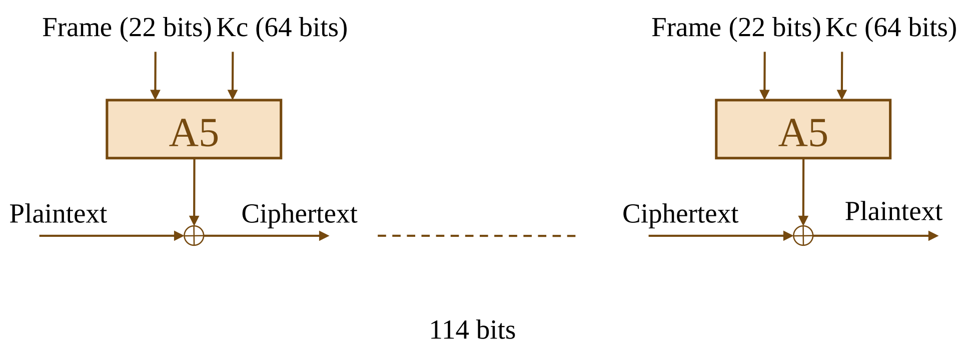
A3/A8

- A3 and A8 are implemented on the SIM
- Can be network specific, but example algorithms were 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)

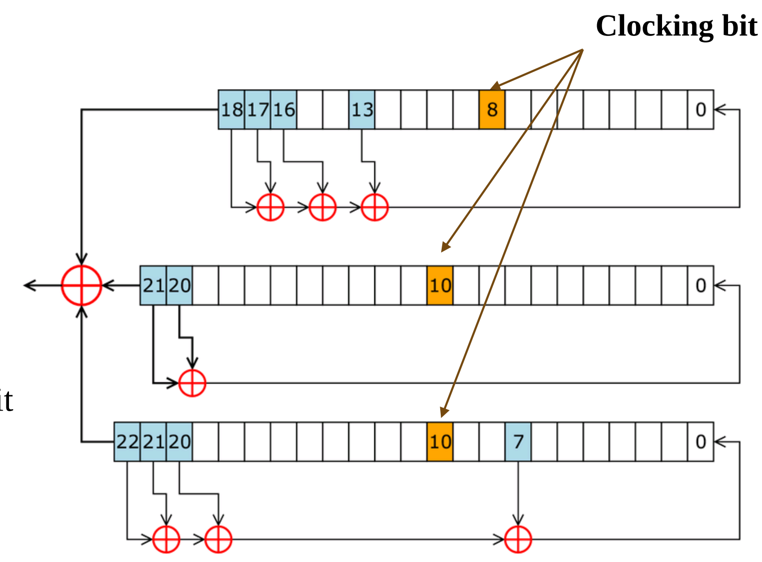
- Traffic only encrypted between mobile station and base station



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 1883 was ignored
- If the algorithm is not investigated by public/researchers before deployment, how can we know it is secure?
  - COMP128 leaked out – got broken
  - A5/1 leaked out – got broken

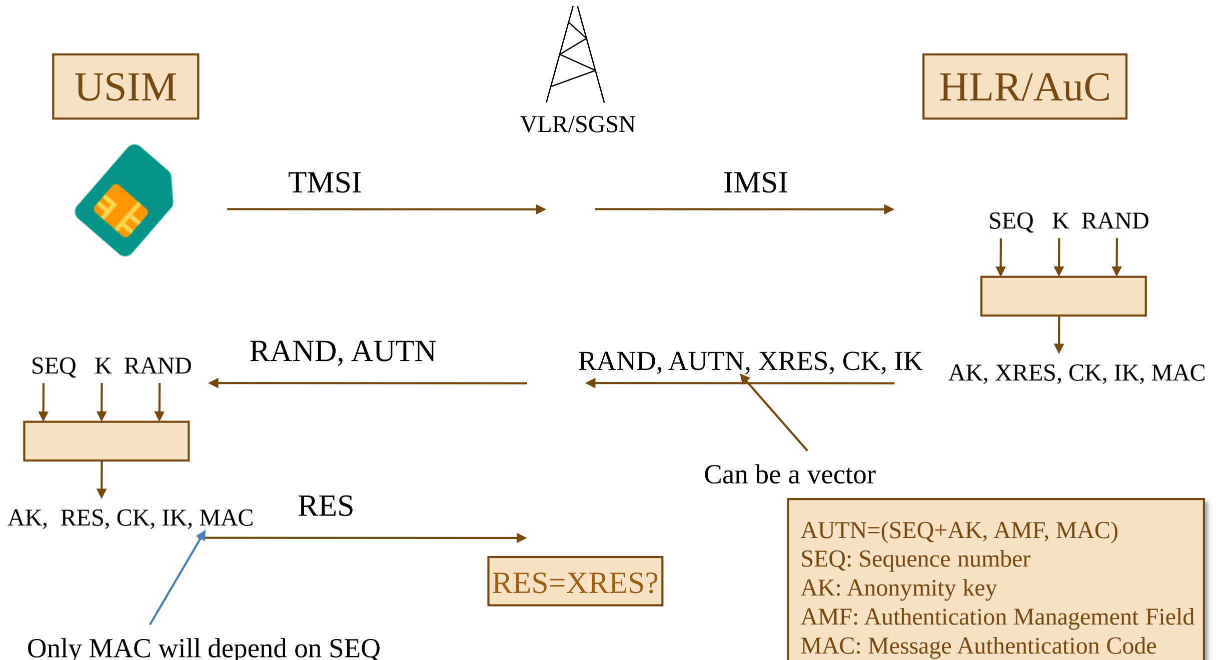
- Another problem with GSM: Only users are authenticated, the network is not
  - Fake basestations can trick phones to send IMSI and/or turn off encryption

UMTS (3G)

- Developed by 3GPP (3rd generation partnership project)
  - Partners from Asia, Europe and North America
- First specification frozen 2000
- 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



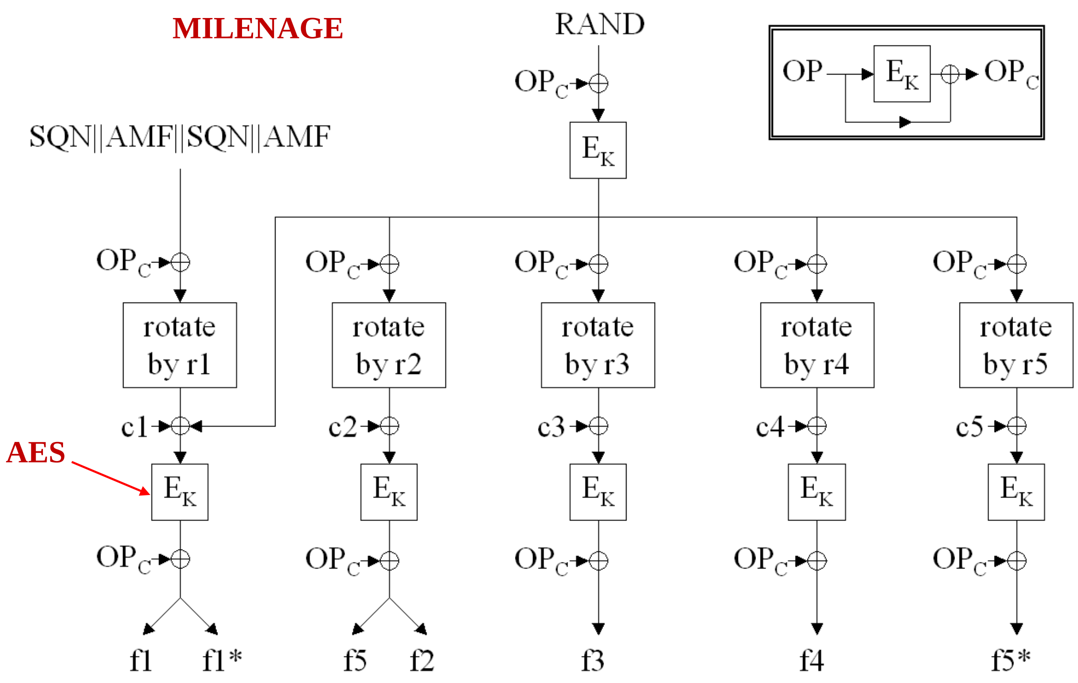
AUTN=(SEQ+AK, AMF, MAC)
SEQ: Sequence number
AK: Anonymity key
AMF: Authentication Management Field
MAC: Message Authentication Code
CK: Cipher Key
IK: Integrity Key

Functions used

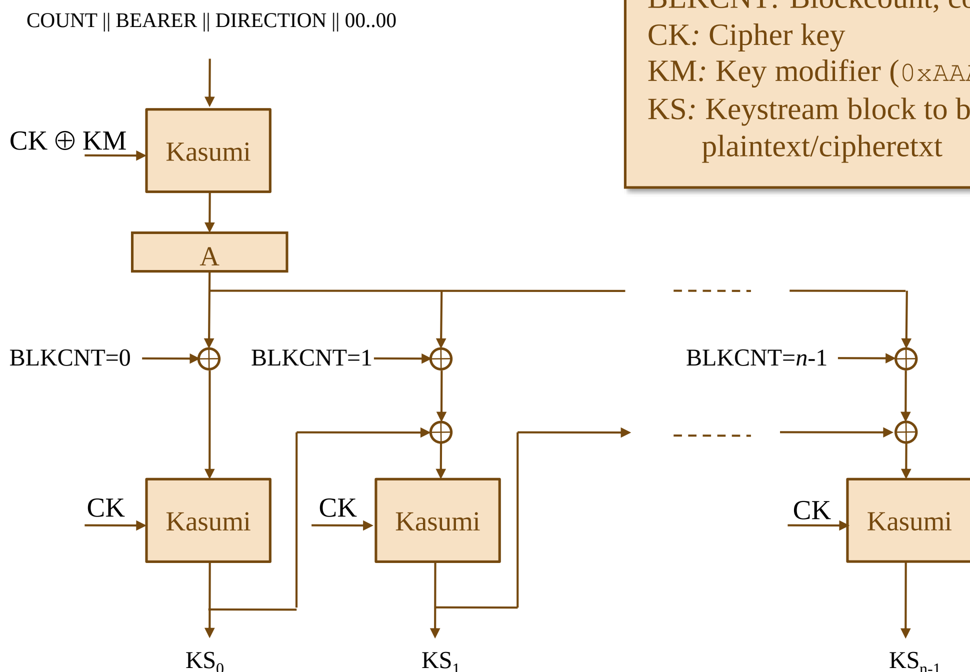
- f0: Random number generator
- f1: Network authentication function. computes a MAC that is part of AUTN
- f2: User authentication function. Computes RES and XRES
- f3: Cipher key derivation function
- f4: Integrity key derivation function
- f5: Anonymity key derivation function. Used to hide sequence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

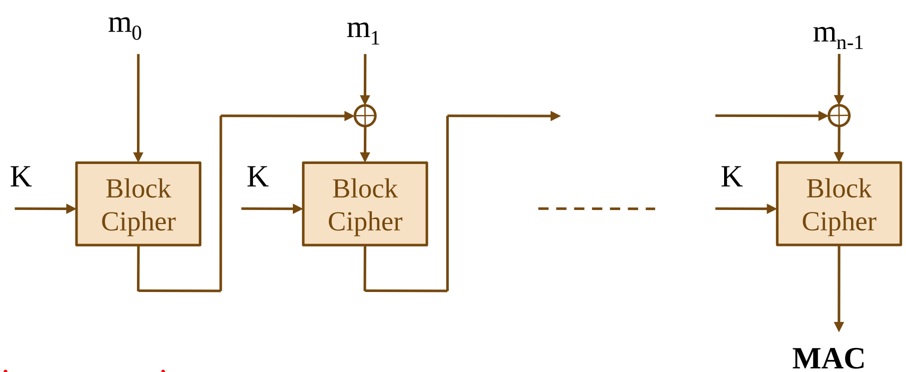
CK: Cipher key

KM: Key modifier (`0xAAAAA`....)

KS: Keystream block to be XORED with plaintext/cipheretxt

Message Authentication, CBC-MAC

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

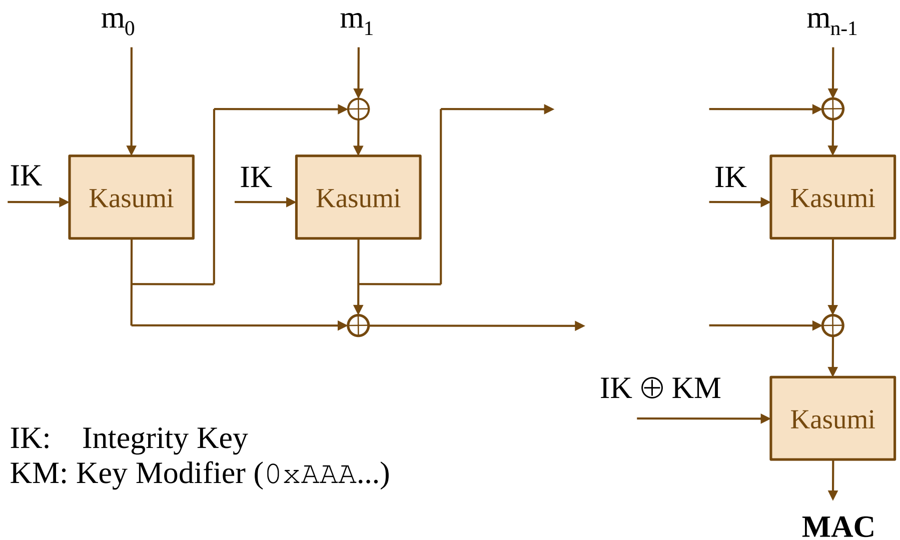


Problem with this construction:
Get message/MAC pair of a one-block message (m,t)

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`...)

LTE (4G)

- New generation, new features
- Quite different network, new names
  - Everything is packet switched
- Developed by 3GPP, constantly evolving with enhancements.
  - LTE is release 8 (2008)
  - LTE advanced is release 10 (2011)
  - LTE Advanced Pro is release 13 and 14 (2016)
  - 5G phases 1 and 2 are releases 15 and 16 (2019+), releases 17 and 18 (2021+)

3GPP Releases

Release Code	Name	Status	Start date	End date
Rel-18	Release 18	Open	2019-09-16	
Rel-17	Release 17	Open	2018-06-15	2021-09-17 (SA#93)
Rel-16	Release 16	Open	2017-03-22	2020-06-19 (SA#88)
Rel-15	Release 15	Frozen	2016-06-01	2019-06-07 (SA#84)
Rel-14	Release 14	Frozen	2014-09-17	2017-06-09 (SA#76)
Rel-13	Release 13	Frozen	2012-09-30	2016-03-11 (SA#71)
Rel-12	Release 12	Frozen	2011-06-26	2015-03-13 (SA#67)
Rel-11	Release 11	Frozen	2010-01-22	2013-03-06 (SA#59)
Rel-10	Release 10	Frozen	2009-01-20	2011-06-08 (SA#52)
Rel-9	Release 9	Frozen	2008-03-06	2010-03-25 (SA#47)
Rel-8	Release 8	Frozen	2006-01-23	2009-03-12 (SA#43)

Security in LTE

- Very similar authentication and key agreement as in UMTS
- AES has replaced Kasumi as confidentiality algorithm.
- New variant of Milenage proposed (based on SHA-3)
- Support for 256-bit symmetric keys

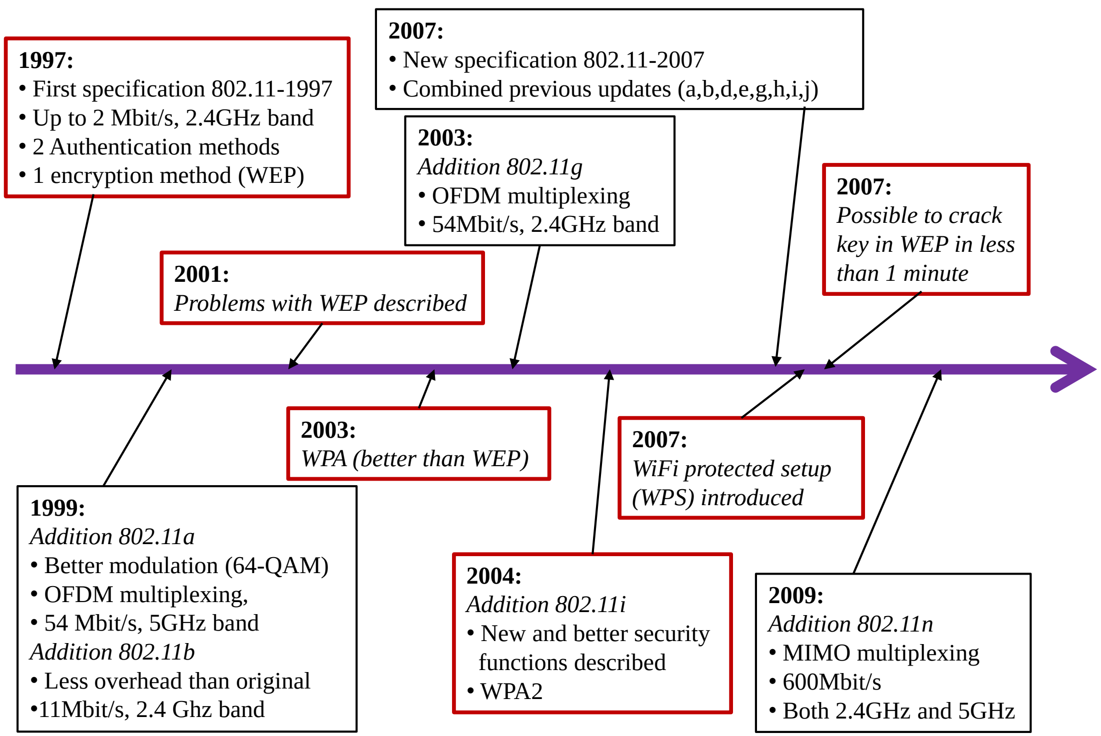
- Ericsson Research Security applied formal verification methods to prove security properties of several LTE methods (2014)

WLAN Security

- IEEE 802.11
- Security Requirements
  1. Integrity
  2. Confidentiality
  3. Authentication
- 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
  - WPA3 introduced 2018
- Specifications are (still) not publically analyzed before they are released!

802.11 timeline



LUND UNIVERSITY

802.11 timeline

2010:
802.11ad
- Introduction of 60GHz
- Not original IEEE
- In products around 2016

2011:
WPS broken

2012:
- New specification 802.11-2012
- Combined previous updates (k,n,p,r,s,u,v,w,y,z)

2013:
Addition 802.11ac:
- Improved 802.11n
- Wider channels, 256-QAM
- Up to 1,3GBit/s

2016:
- New specification 802.11-2016
- Incorporates 60GHz band
- Up to 6,7 Gbit/s

2017:
KRACK attack
- WPA2, reuse of keystream
- install all-zero key in some cases

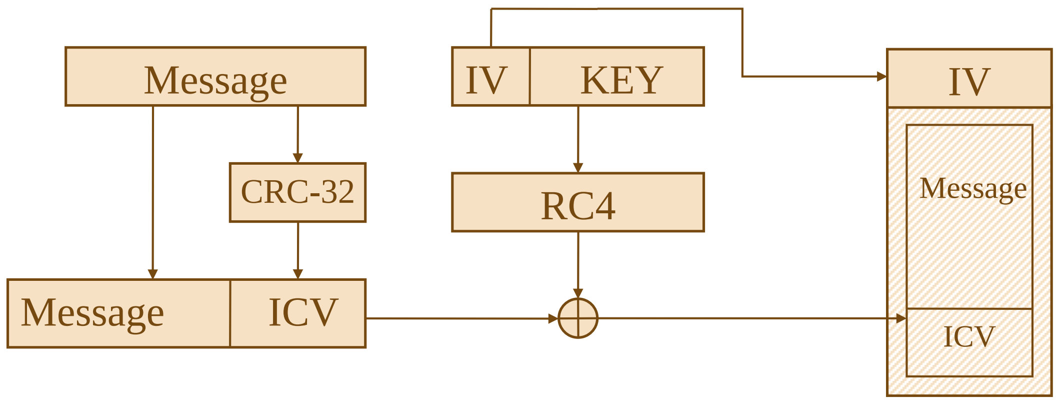
2018:
WPA3
- Longer keys
- Opportunistic encryption

WEP encryption

Three design goals:

- integrity
- confidentiality
- authentication

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 $\delta = \text{CRC-32}(\Delta)$
  - Add $(\Delta \,||\, \delta)$ to ciphertext

$$(M \,||\, \text{CRC-32}(M)) \oplus \text{RC4}(K) \oplus (\Delta \,||\, \delta) = (M \oplus \Delta \,||\, \text{CRC-32}(M) \oplus \delta) \oplus \text{RC4}(K)$$
$$= (M \oplus \Delta \,||\, \text{CRC-32}(M \oplus \Delta)) \oplus \text{RC4}(K)$$

- We still have a valid message → no integrity protection

WEP encryption

Three design goals:

- ~~**integrity**~~
- confidentiality
- authentication

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

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

- 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

WEP encryption

Three design goals:

- ~~**integrity**~~
- ~~**confidentiality**~~
- authentication

RC4

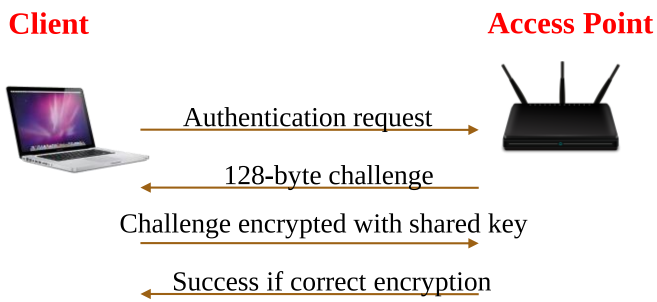
- Probably the most well known (and simplest) stream cipher
- Designed 1987 but kept secret, leaked out 1994
- Also referred to as ARC4 and ARCFOUR since the name RC4 is a trademark
- Many weaknesses have been found
- In SSL/TLS there is no IV in RC4. One stream is used for each key
  - But there are other problems that makes it unsuitable

$\mathrm{KSA}(K[0\ldots\ell-1])$	$\mathrm{PRGA}(K)$

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
  - Prove that you have the key (password)
  - 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.

WEP encryption

Three design goals:

- ~~**integrity**~~
- ~~**confidentiality**~~
- ~~**authentication**~~

LUND UNIVERSITY

WPA, WPA2 and WPA3

- 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
- WPA3 announced in 2018

802.11i Authentication

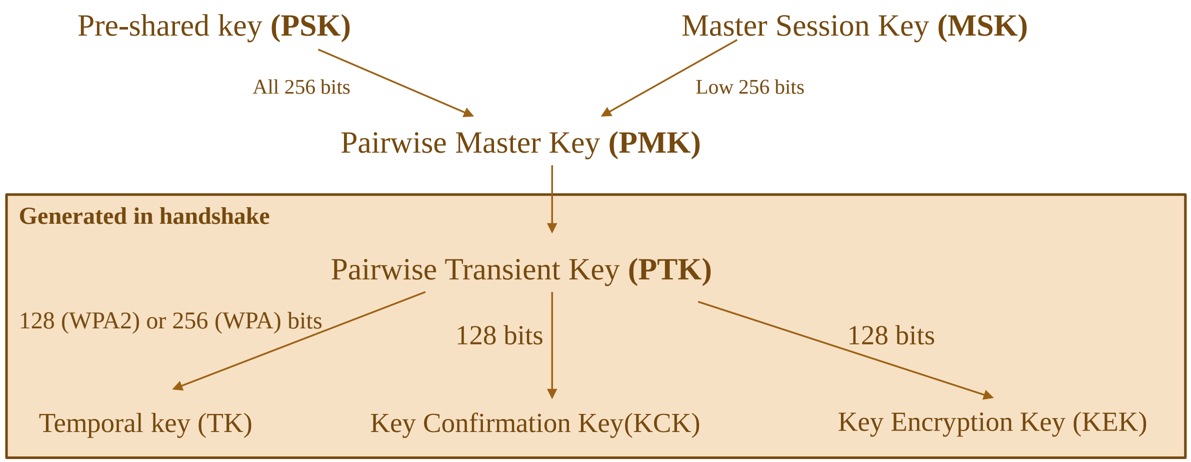
- Can use a specific server for EAP authentication
  - Supports several methods for authentication
  - More on this in the course ”Advanced Computer Security”
  - Authentication server constructs a **Master Session Key (MSK)**
- Can also use a pre-shared key (called WPA-PSK)
  - Still keys are different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

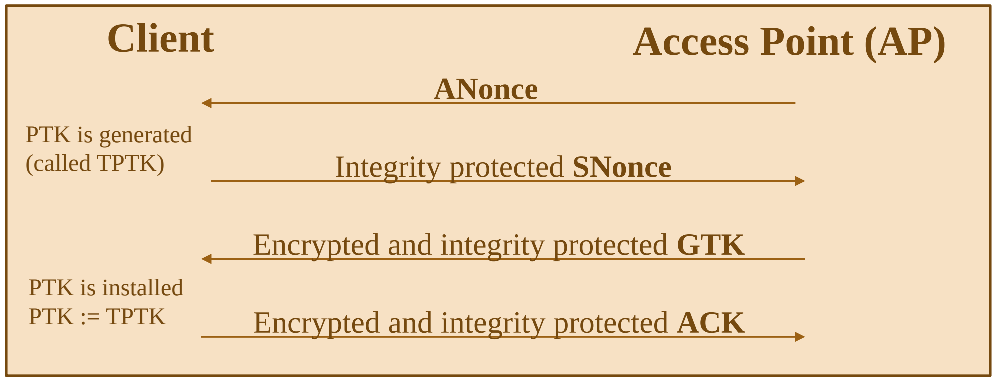
Keys in 802.11i

- A hierarchy of keys



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

4-way handshake

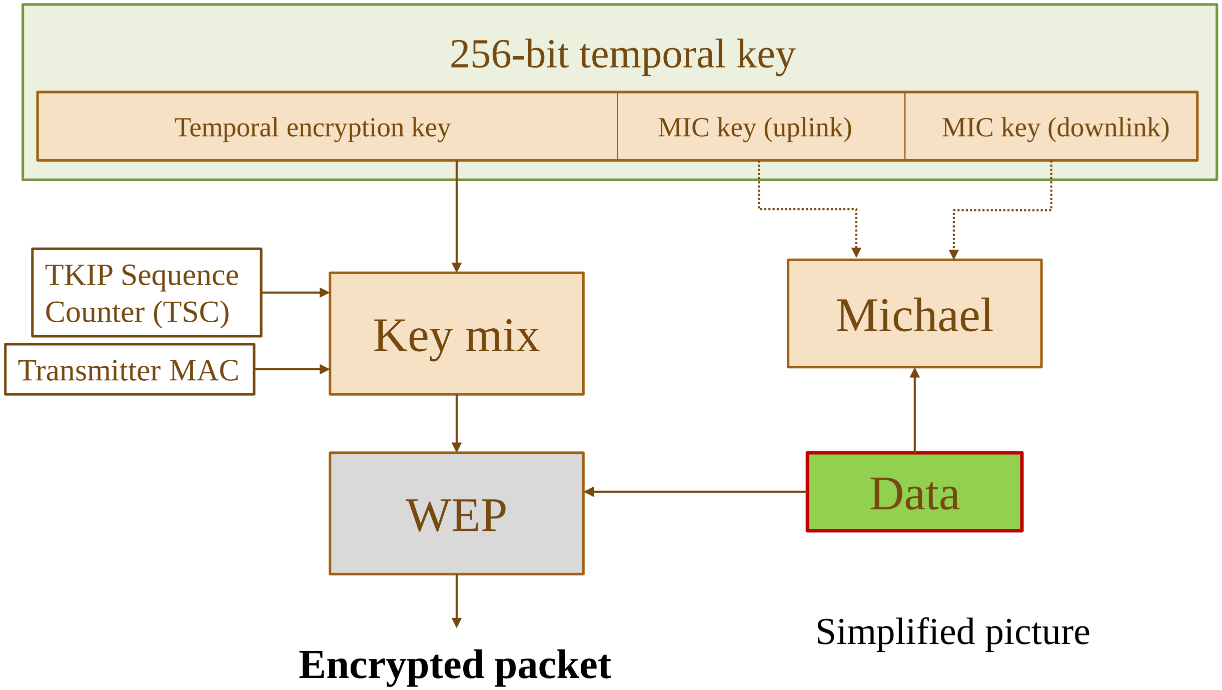


- PTK is hash of (PMK, MAC_{client}, MAC_{AP}, ANonce, SNonce)
  - Iterated SHA-1
  - Note that MAC here is *MAC address*
- Last two messages constructed such that *key confirmation* is provided
- Encryption and integrity protection in handshake uses KCK and KEK
- GTK is derived from GMK and updates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

TKIP

- Temporal Key Integrity Protocol
- 256 bit temporal key divided into 128-bit encryption key and 2x64 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)



Simplified picture

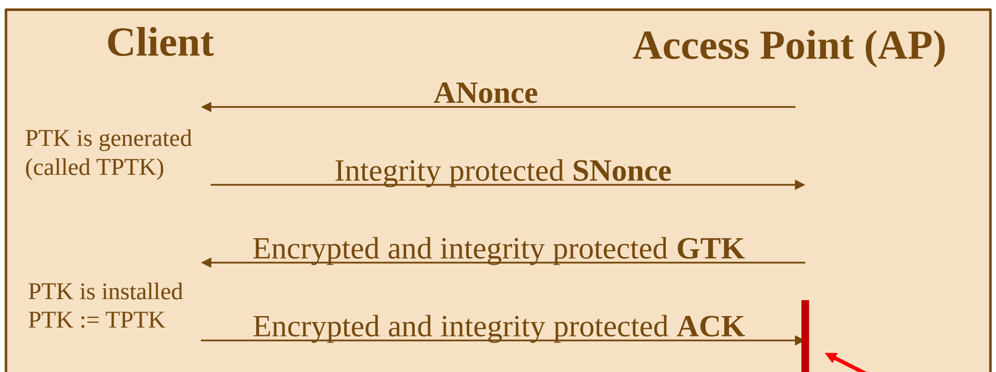
CCMP (WPA2)

- 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
- Requires new hardware since completely new encryption algorithm is used

KRACK Attack

- October 2017
- Third step in 4-way handshake will install key in devices
- Force authenticator (AP) to replay message 3 → supplicant (client) reinstalls same key
  - Nonce is reset
  - Replay counter is reset
- Android 6.0: Zero key is installed

Details are very implementation dependent



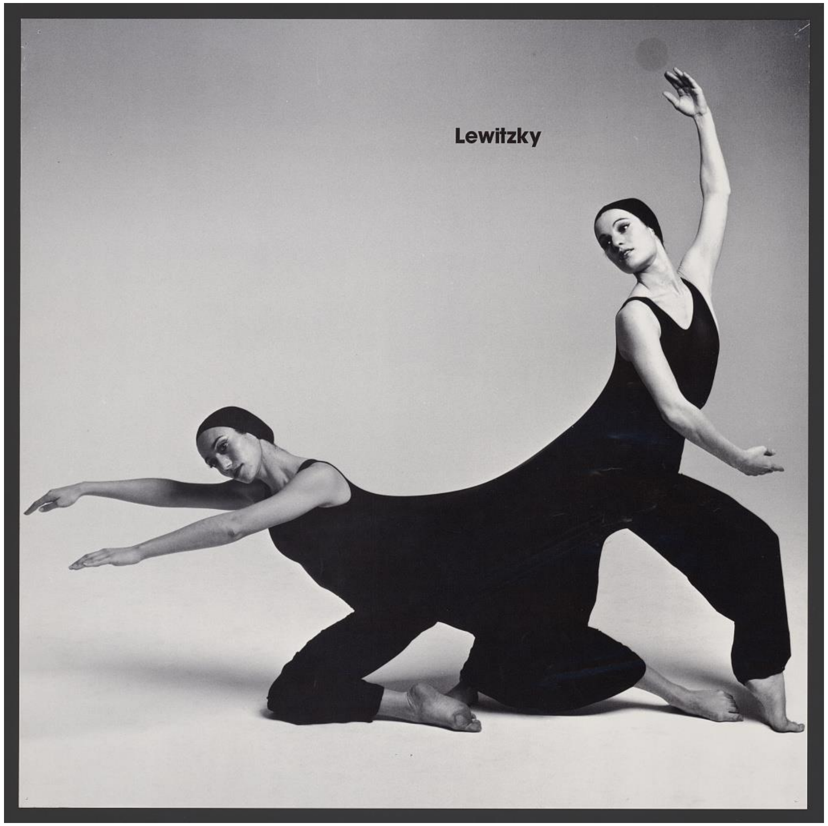
(Wired) KRACK Attack!

Library of Congress, no known restrictions on publication.

Dragonblood Attack

- April 2019
- Serious design flaw in WPA3
- Allows attacker to perform
  - downgrade attacks
  - side-channel attacks
- Problems:
  - enables brute-forcing passphrase
  - DoS attacks on Wi-Fi base stations

Is wireless better?



Library of Congress, no known restrictions on publication.

Stay connected

What's next?

- Optional Exam Friday 20/3, 14-19, MA:10F-H
  - For grade 4-5

- If you want more security courses
  - Web security HT1, 4 hp,
  - Advanced computer security, HT1, 7.5 hp
  - Advanced web security, HT2, 7.5 hp
  - Cryptology, HT2, 7.5 hp
  - Secure Systems Engineering, VT1, 7.5 hp