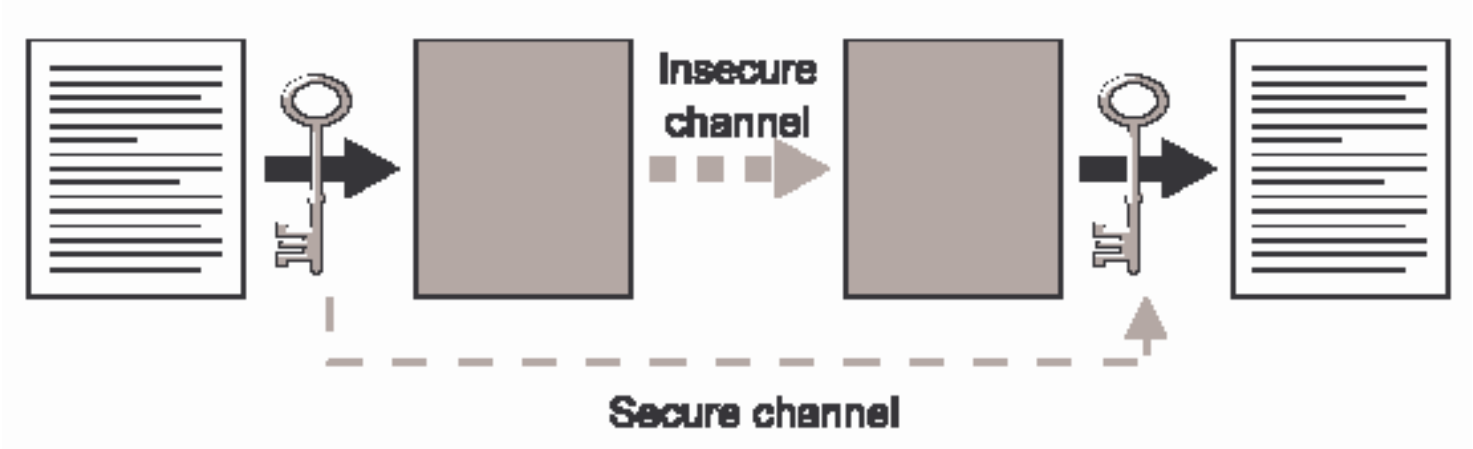
Wi-Fi Security

FEUP>MIEIC>Mobile Communications

Jaime Dias <jaime.dias@fe.up.pt>

Symmetric cryptography

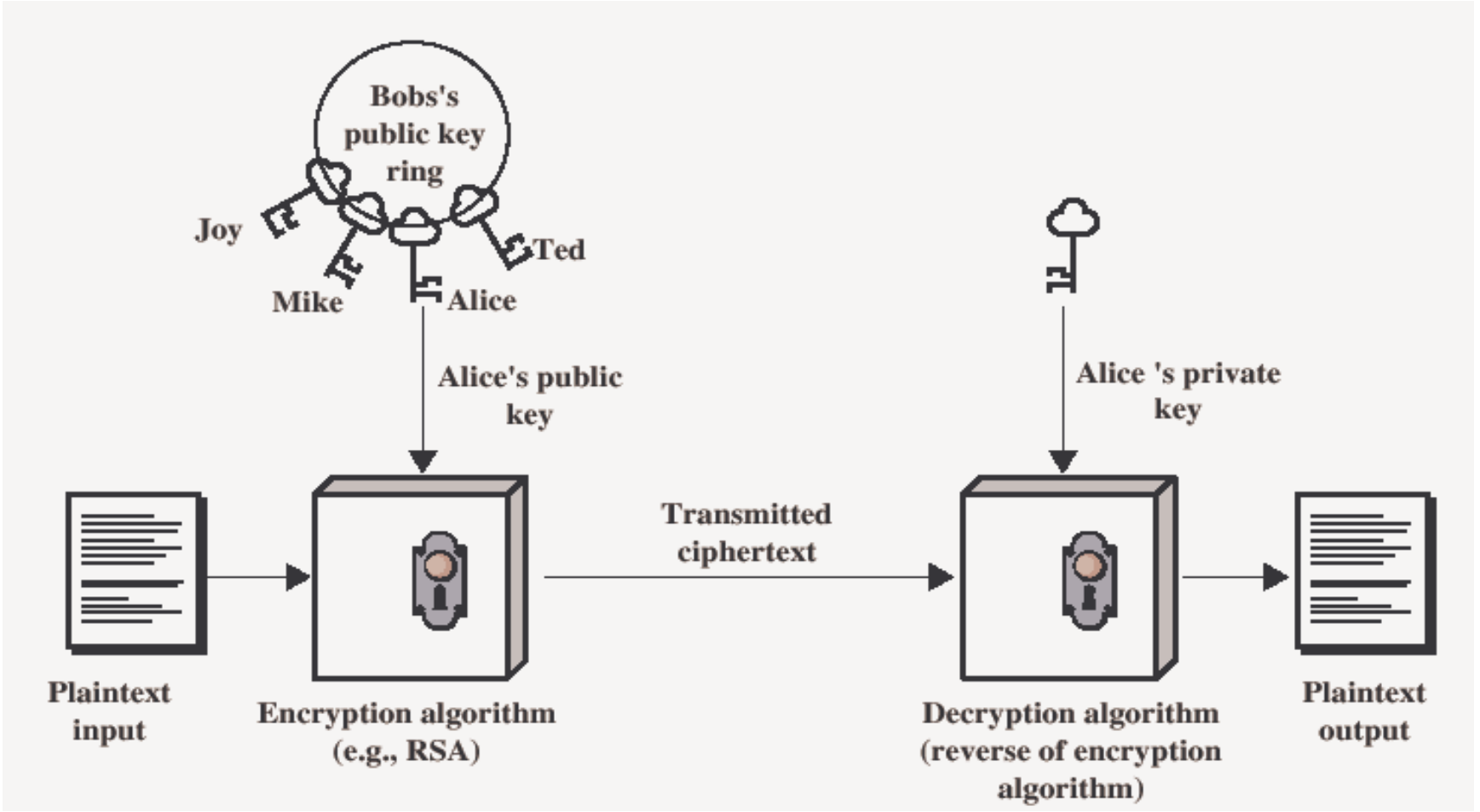
- Ex: RC4, AES



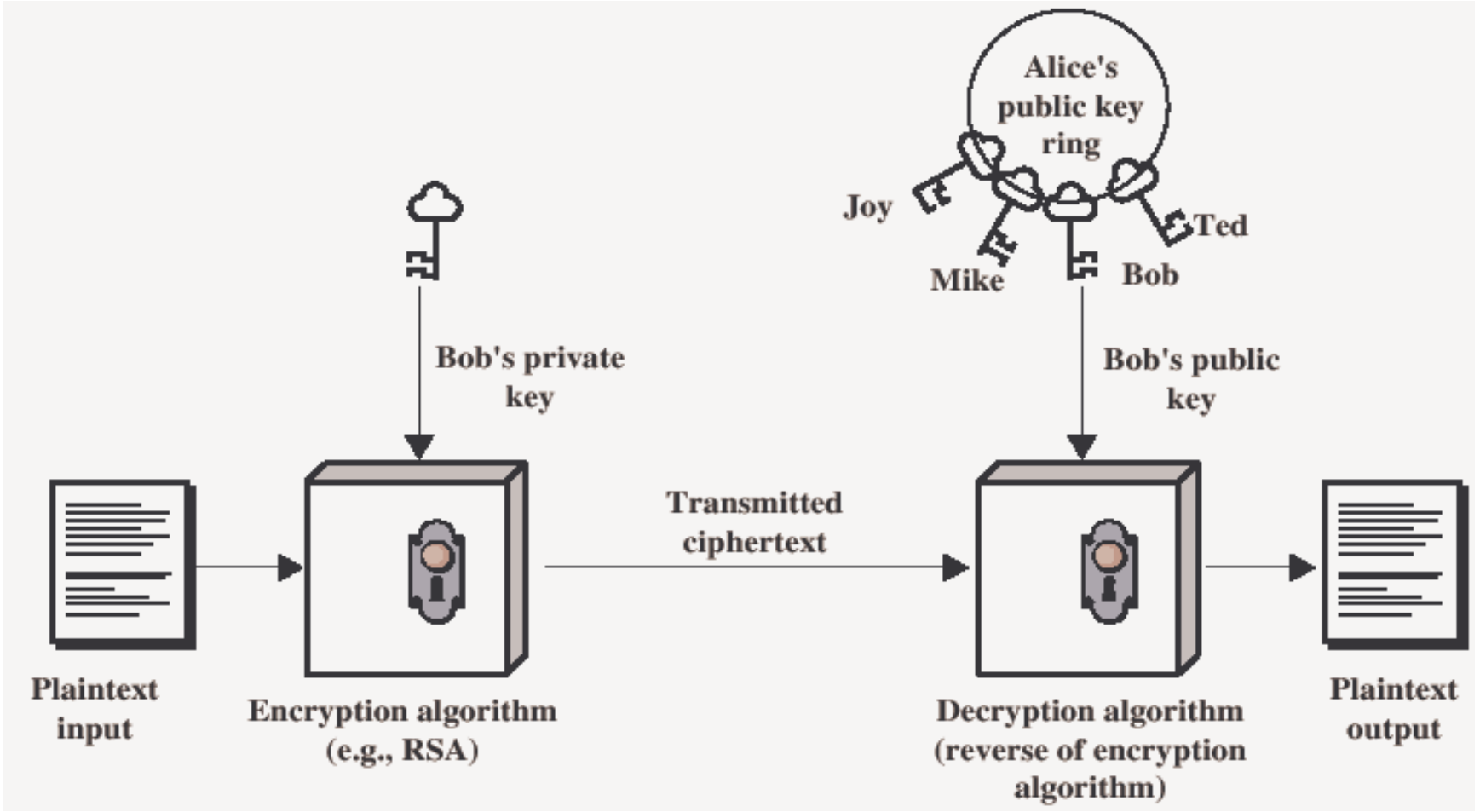
Digest (hash) Cryptography

- Input: variable length message
- Output: a fixed-length bit string
- High performance
- Used for message integrity and identification
- Ideal function
  - One-way: impossible to know the message from the digest
  - Every message has a different digest
- Ex: MD-5, SHA-1

Public Key Cryptography
Confidenciality

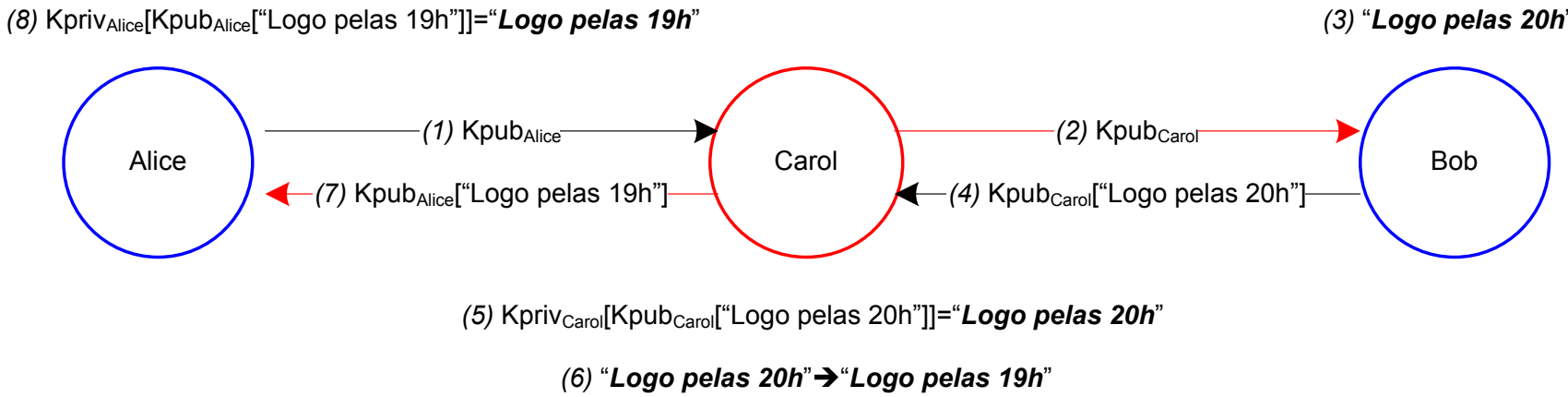


Public Key Cryptography
Authentication (digital signature)

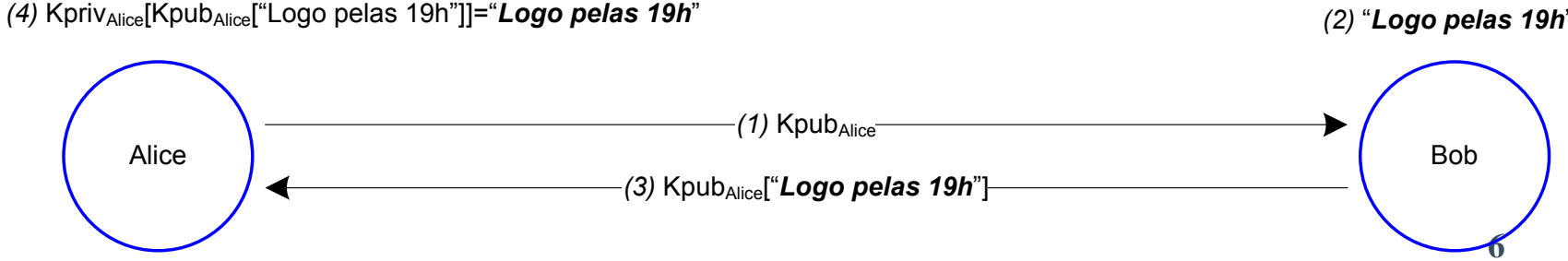


Public Key Distribution Problem

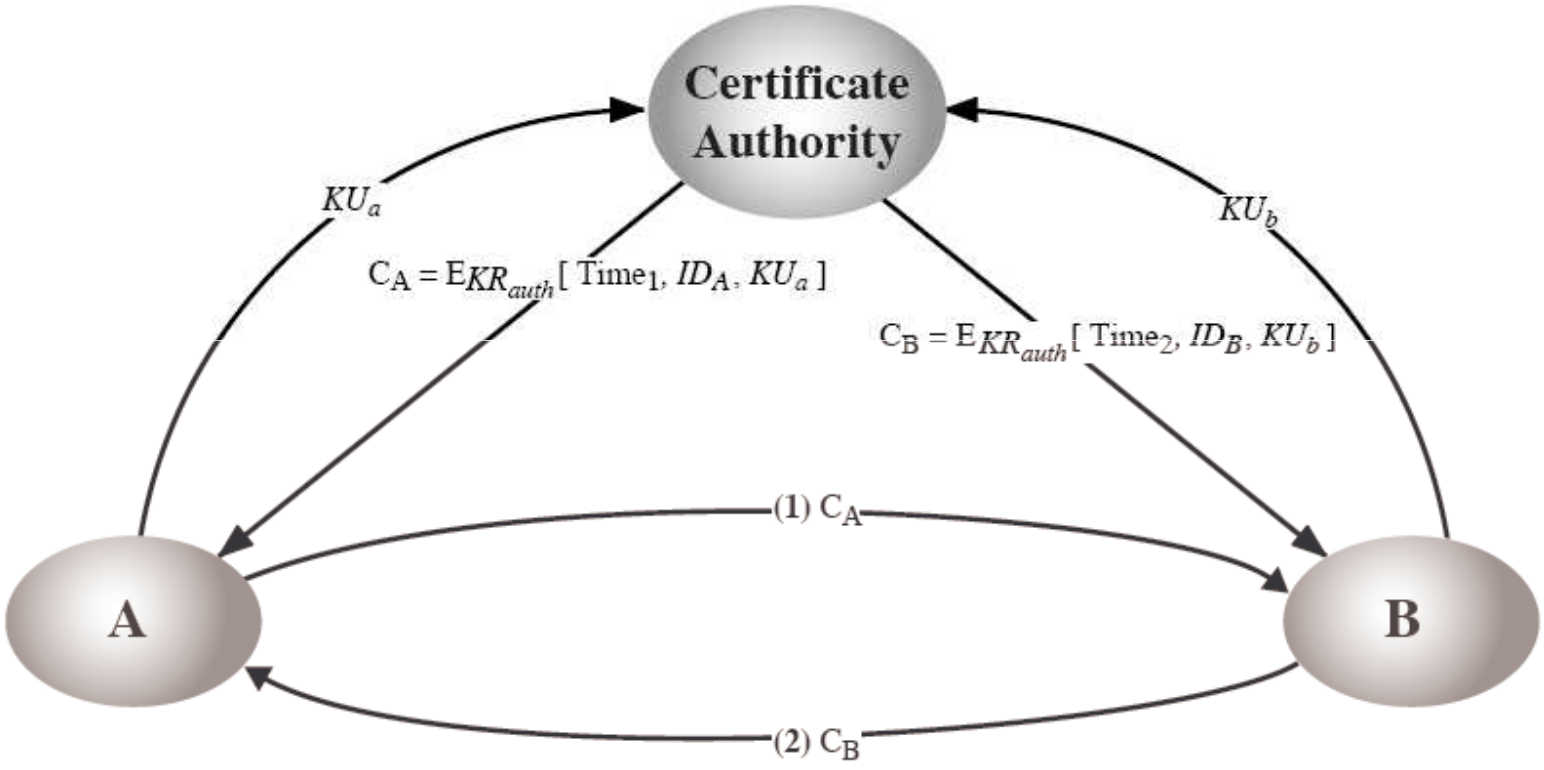
Ataque MIM:



O que a Alice julga ter acontecido:

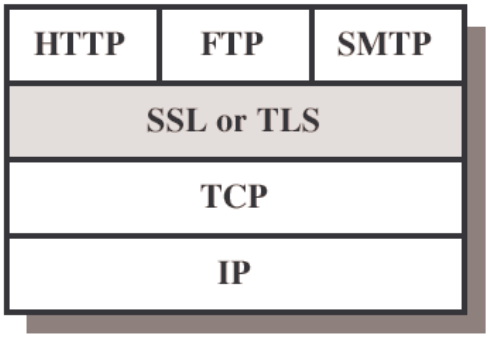


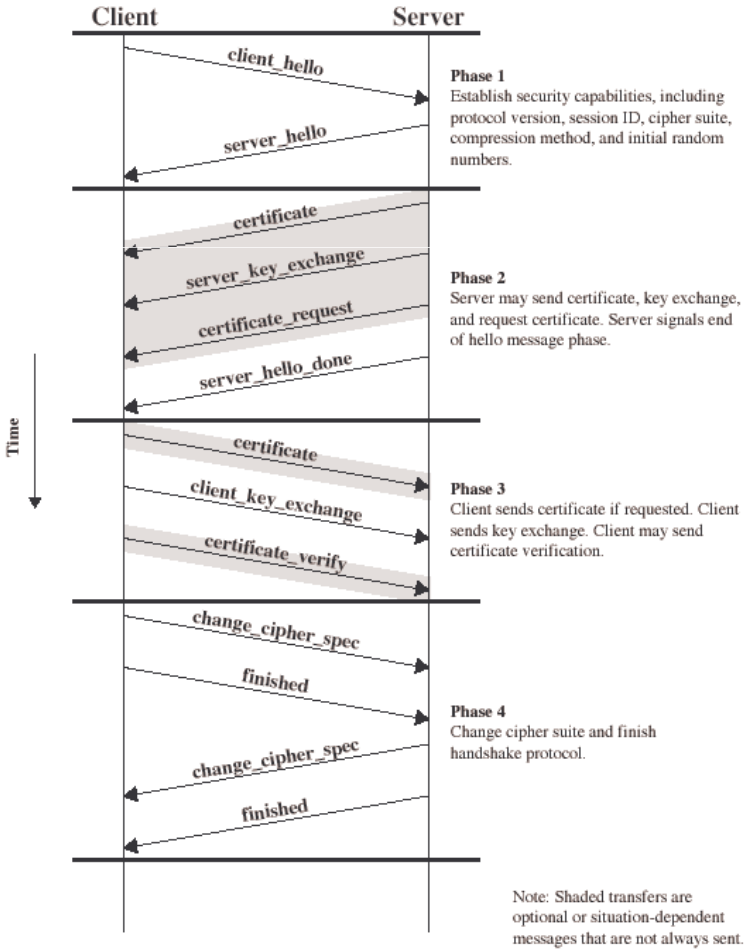
Certification Authority



SSL/TLS

- SSL (Secure Socket Layer)
  - Developed by Netscape
  - Versions 2 e 3
- TLS 1.0 (Transport Layer Security)
  - IETF
- Transparent to application protocols
- Allows both server and client to be authenticated through certificates
- Tipically, due to certificate costs
  - Only servers are authenticated
  - Clients are authenticated at the application layer (ex: passwords)

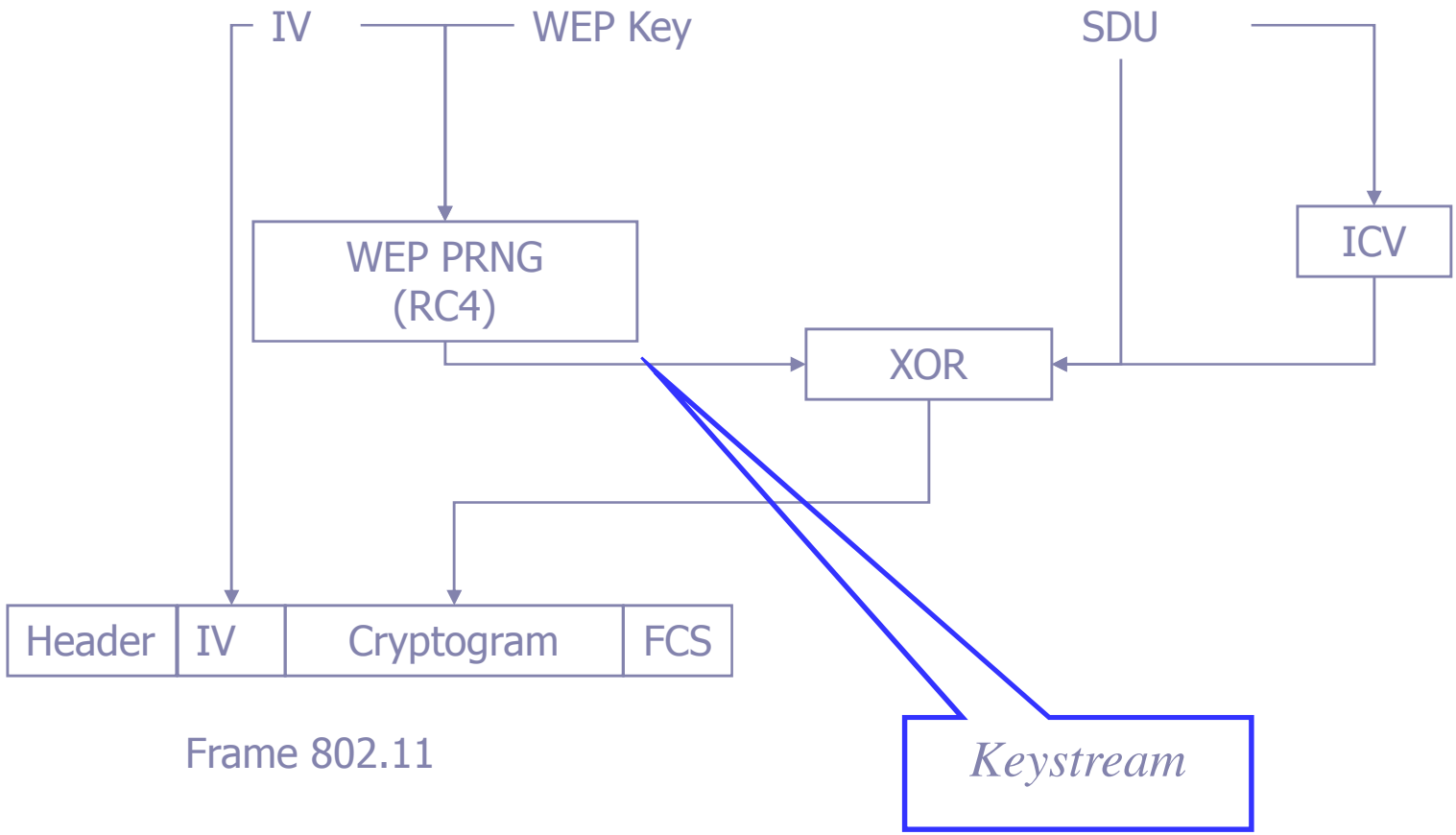




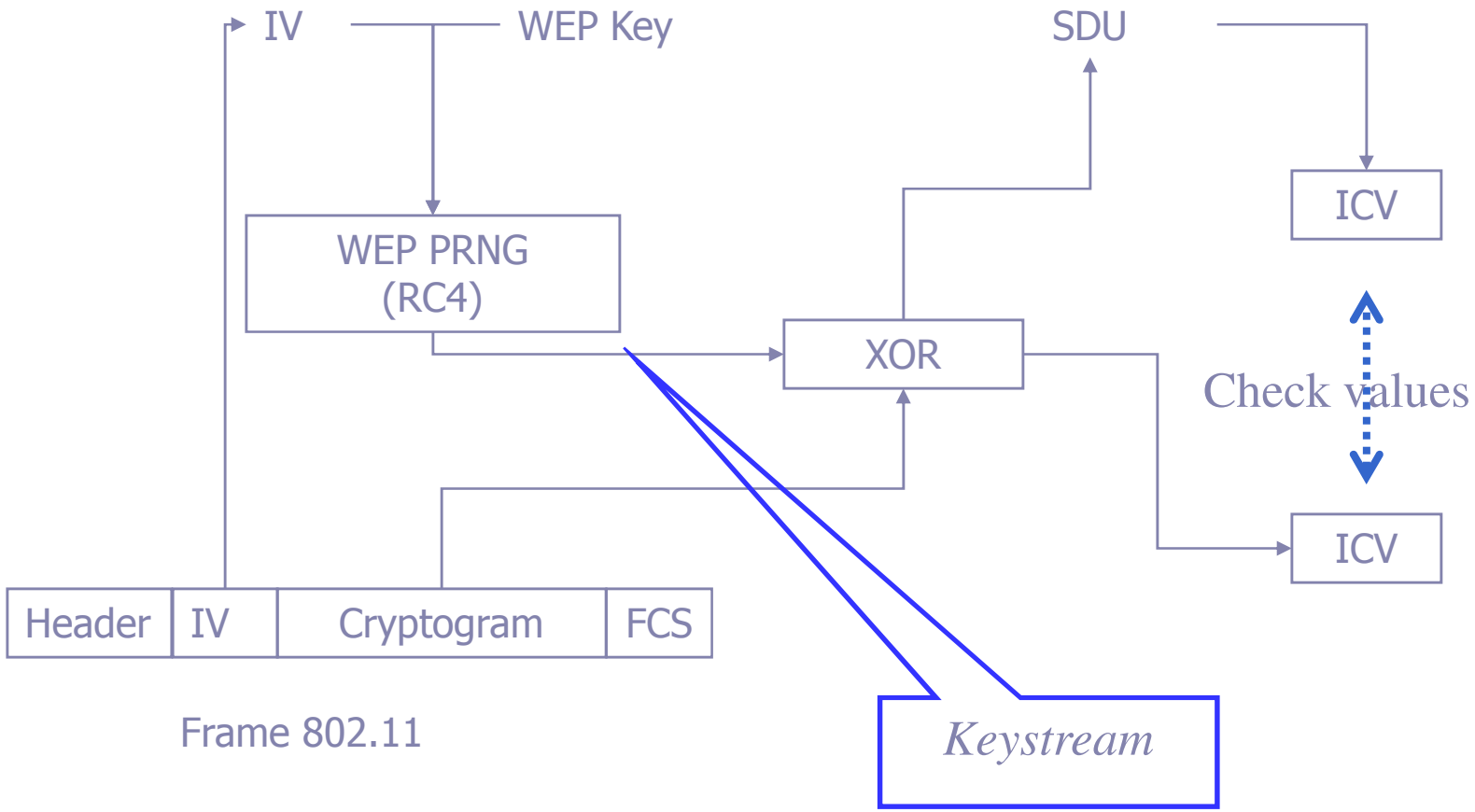
802.11 Security

- “Minimum” security WEP (Wired Equivalent Privacy)
- Station authentication
  - Open mode ← no authentication
  - Shared Mode
    - Challenge: AP sends challenge ← station returns the challenge encrypted with the WEP key
- Confidentiality ← frames are encrypted with RC4
- Integrity ← CRC32

Encryption


IV
WEP Key
SDU
WEP PRNG
(RC4)
ICV
XOR
Header
IV
Cryptogram
FCS
Frame 802.11
Keystream

Decryption


IV
WEP Key
SDU
ICV
WEP PRNG
(RC4)
XOR
Check values
ICV
Header
IV
Cryptogram
FCS
Frame 802.11
Keystream

WEP Vulnerabilities

- Same IV and WEP key same keystream
  - IV too short (24 bits)
  - No mechanism for WEP key update
- Same keystream:
  - **SDU2** ⊕ SDU1 = cryptogram1 ⊕ cryptogram2
  - If SDU1 is known (ICMP, TCP ack, …) then
  - **SDU2** = cryptogram1 ⊕ cryptogram2 ⊕ SDU1

WEP Vulnerabilities (2)

- RC4 key = IV (3 bytes) + WEP key (5 or 13 bytes)
- Weak IVs help breaking the WEP key
  - Weak IVs: i:ff:X
- Ex: Weak IVs for WEP keys of 40 bits
  - 3:ff:X, 4:ff:X, 5:ff:X, 6:ff:X, 7:ff:X

WEP Vulnerabilities (3)

- Integrity Check Value based on CRC32 (linear)
- WEP does not authenticate nor check the integrity of the frame header
  - Station can change the MAC address
- AP is not authenticated
  - Rogue AP
- WEP does not control the frame sequence
  - Replay attacks
- Same key for every station
  - Traffic can be eavesdropped or even changed by any station knowing the WEP key

WEP Vulnerabilities (4)

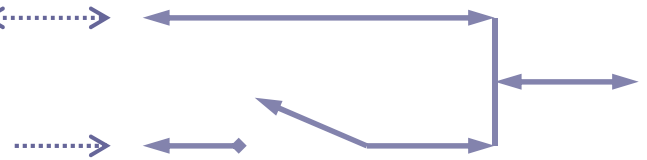
- Manufacturers have put some additional barriers
  - Authentication by SSID
    - Station only need to monitor the medium and wait for another station to associate to see the SSID
  - Access control by MAC address
    - Station only need to see the MAC address of allowed stations and clone their address

802.1X – Access Control

Before the authentication

Traffic 802.1X

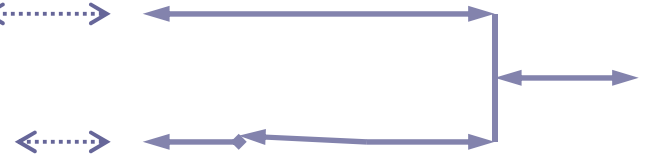
Other traffic (blocked)



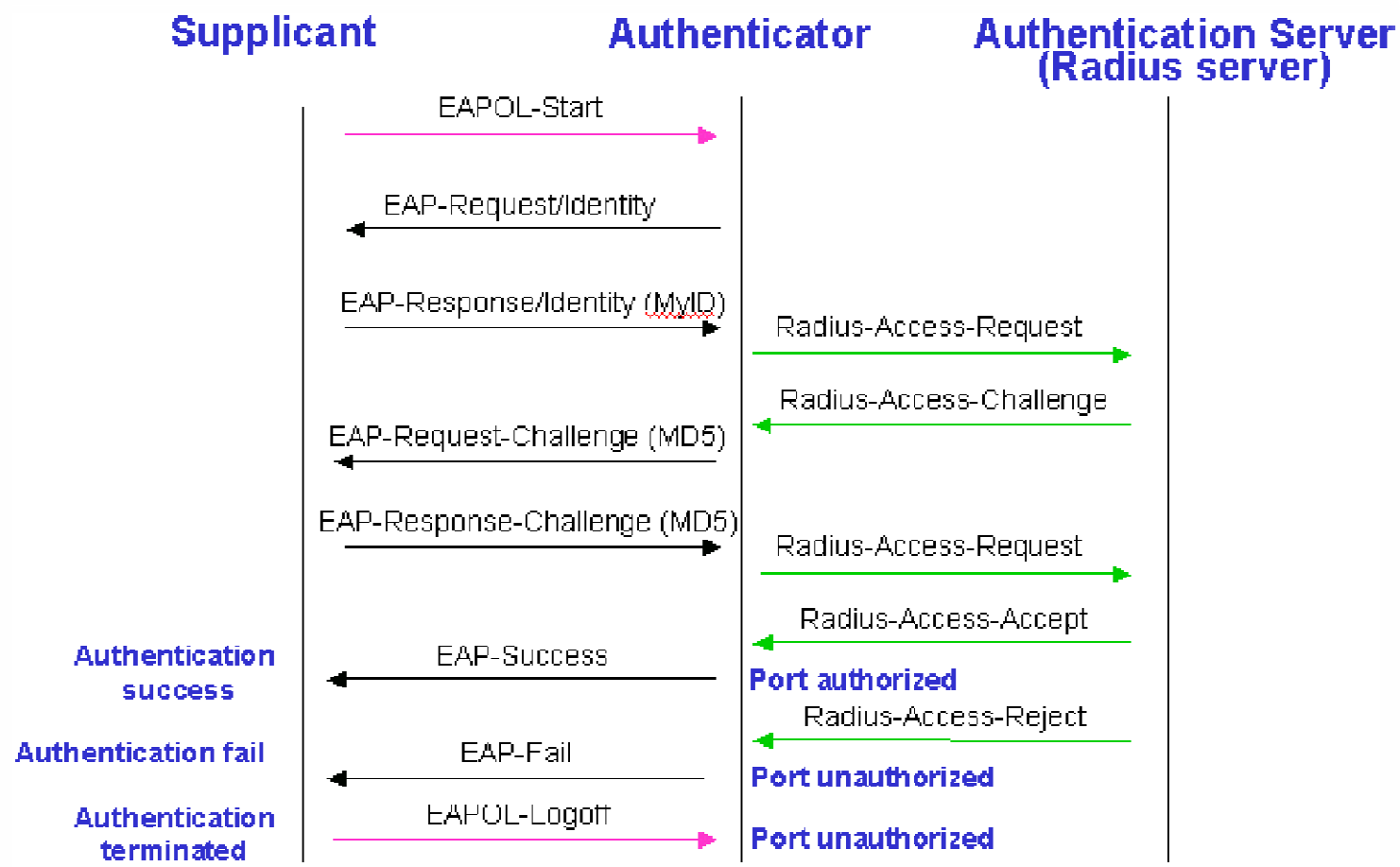
After the authentication

Traffic 802.1X

Other traffic (unblocked)



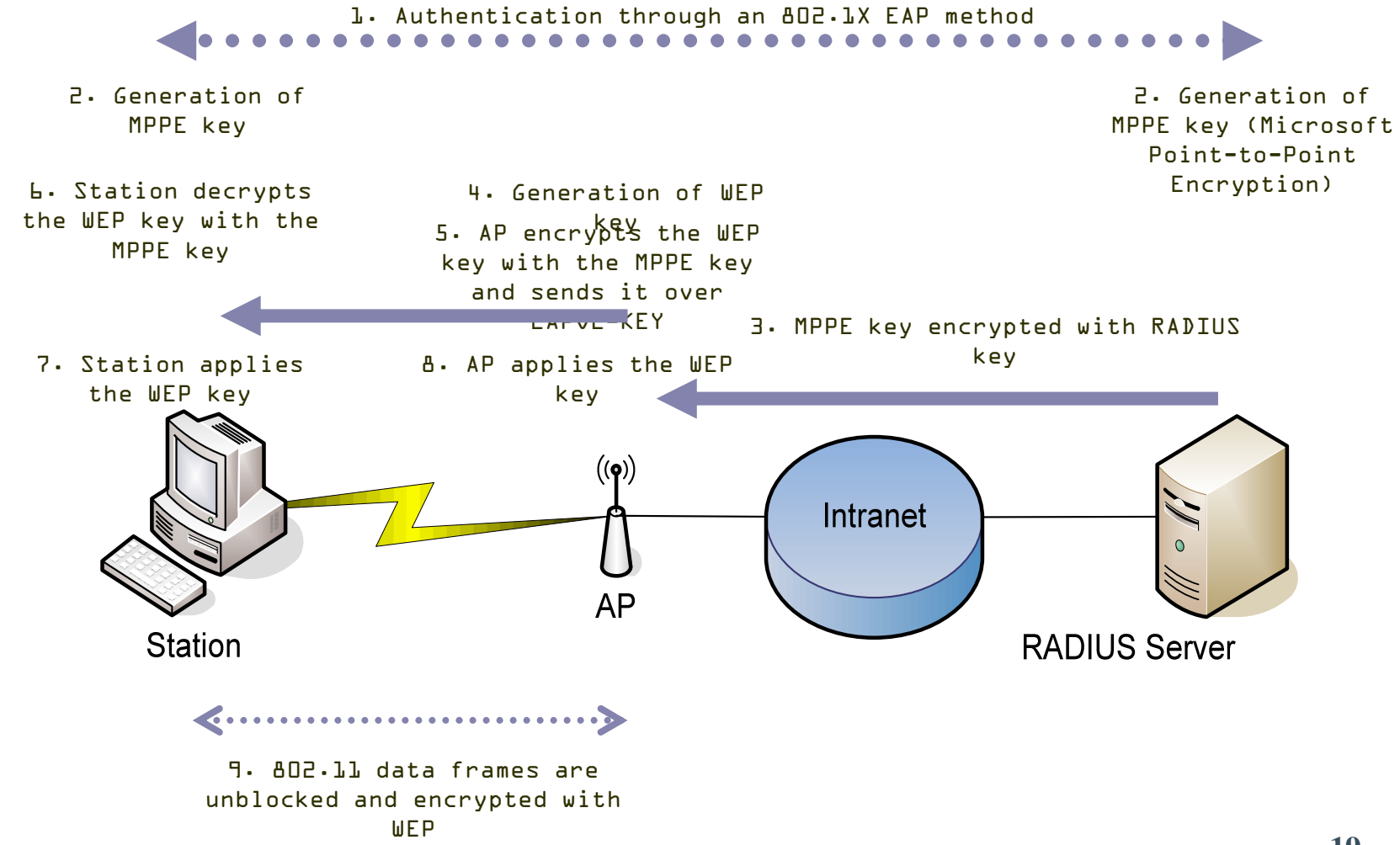
802.1X with Radius



Dynamic WEP

- Uses 802.1X
- User authentication
  - Support of multiple authentication methods
  - Centralized data base with users' credentials, independent of APs
- Authentication of the AP
- Authenticaton keys ≠ encryption keys
- Periodic update of WEP keys

Dynamic WEP (2)



802.11i

- WEP failure IEEE 802.11i
- Uses the 802.1X
- Authentication/Access Control
  - Pre-shared key (PSK)
  - With Authentication Server - 802.1X
- Key Management
  - Temporary Keys
  - Authentication keys ≠ Encryption keys
- Data protection
  - CCMP (Counter mode Cipher block Chaining MAC protocol)
    - Based on the AES cipher algorithm
  - TKIP (Temporal Key Integrity Protocol)
    - Based on the RC4 cipher algorithm (same as WEP)
- Infraestructured and ad-hoc modes

Wi-Fi Protected Access

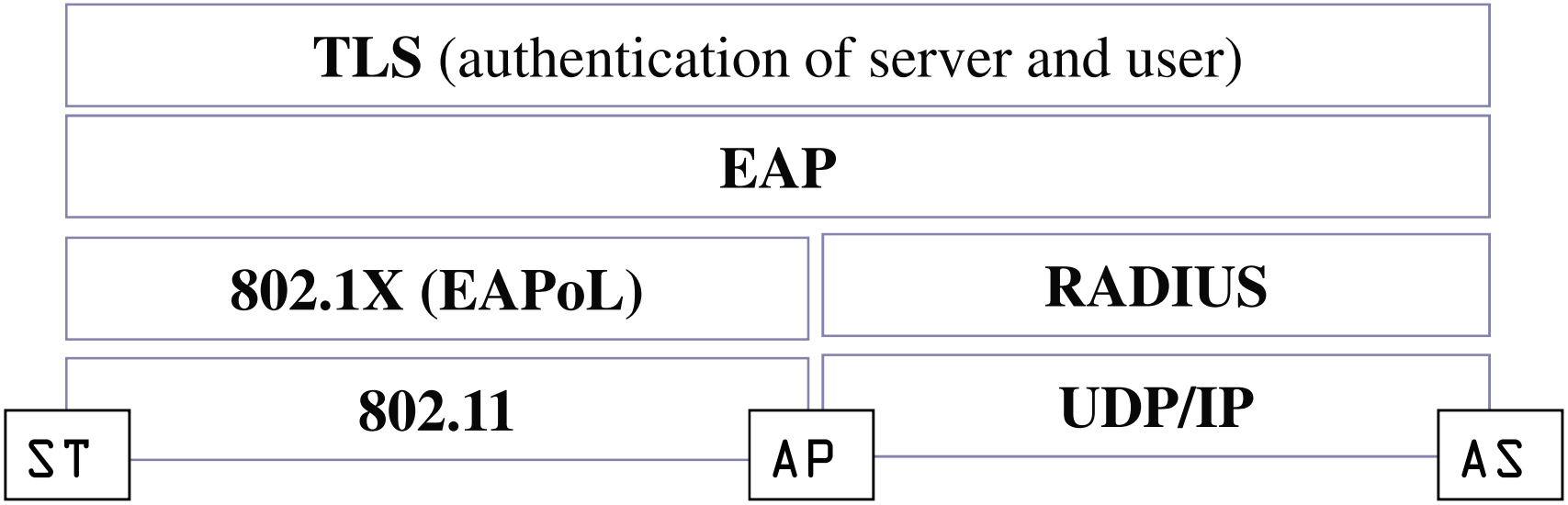
- WPA
  - Based on Draft 3.0 of 802.11i (2002)
  - Short term solution for legacy equipments
  - No support for CCMP nor the ad-hoc mode
  - TKIP reuses the WEP HW (RC4 cipher algorithm)
    - Firmware upgrade
- WPA2
  - Supports 802.11i
  - Long term solution

Authentication methods (802.1X)

- Requires Authentication Server
- Most popular Wi-Fi authentication methods
  - EAP-TLS
  - EAP-TTLS
  - PEAP

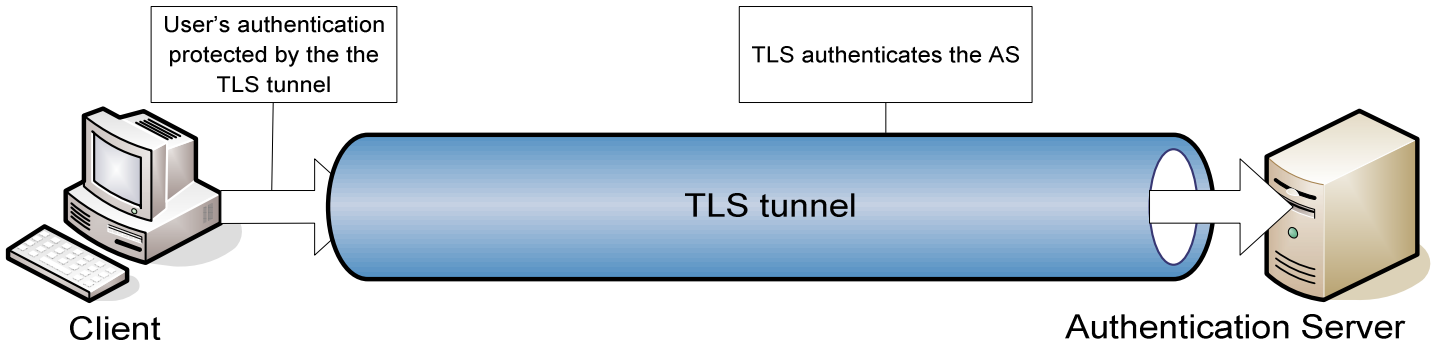
EAP-TLS

- Uses TLS to authenticate both server and user through certificates
- Mandatory in WPA
- Cons:
  - Certificates are expensive
  - User identity goes in clear in the user's certificate



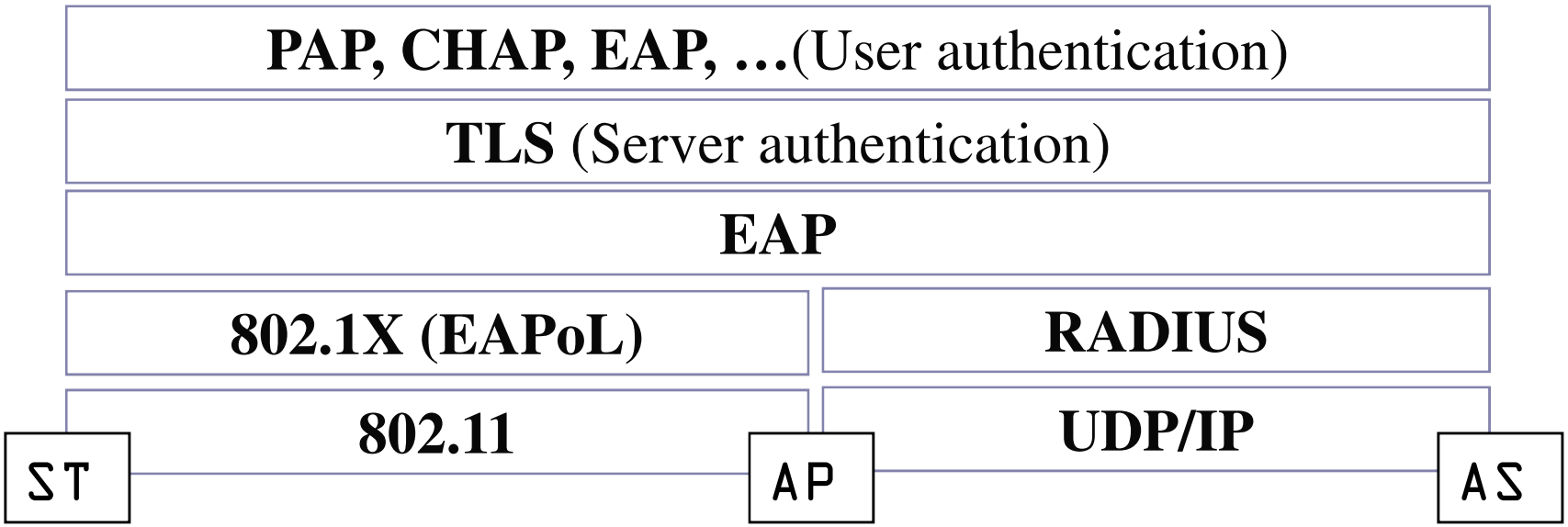
Tunneled authentication

- Two phase authentication
  - TLS tunnel authenticates the Authentication Server
  - User autenticated over the TLS tunel
    - Support of weaker methods for user's authentication
    - Certificates are optional
    - User's identity goes encrypted
- EAP-TTLS, PEAP



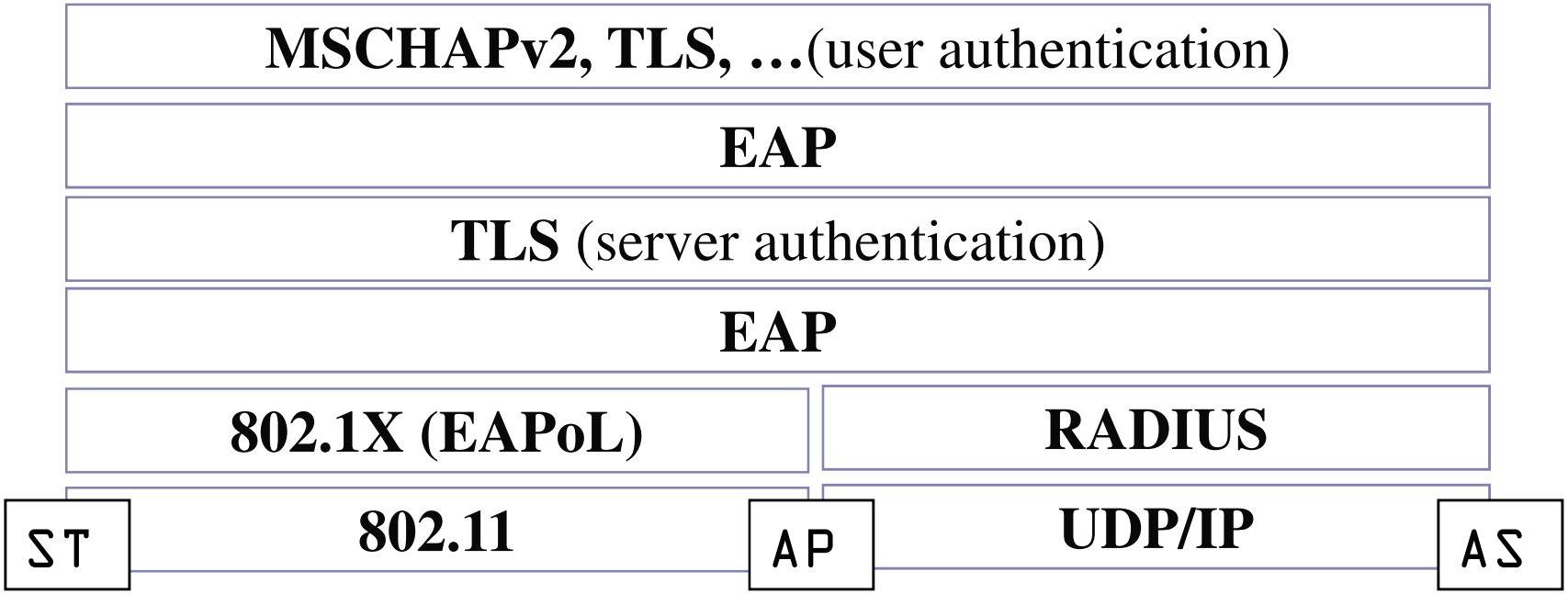
EAP-TTLS

- EAP- Tunneled TLS



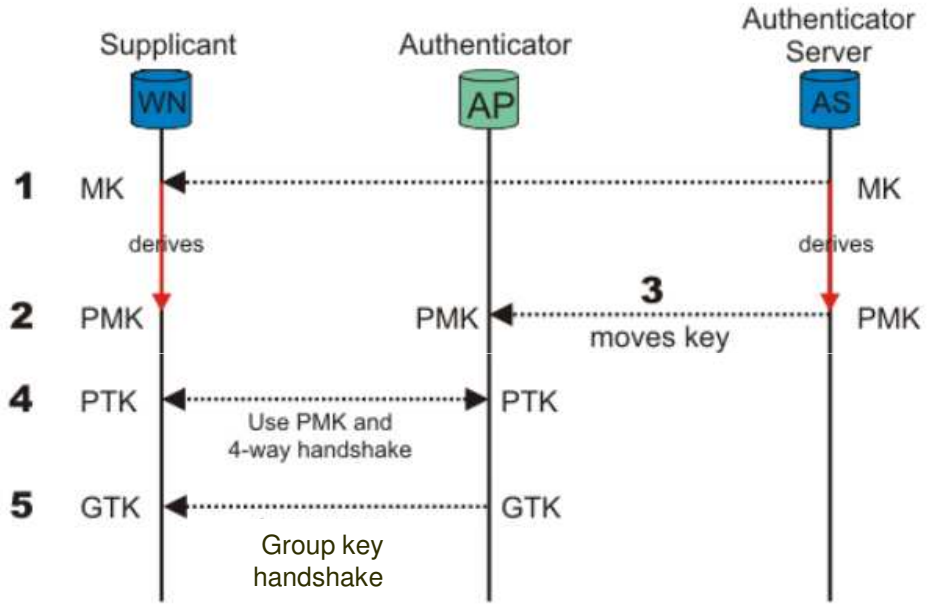
PEAP

- Protected Extensible Authentication Protocol
- v0 Microsoft, v1 Cisco
- PEAPv0/EAP-MSCHAPv2 – the most popular

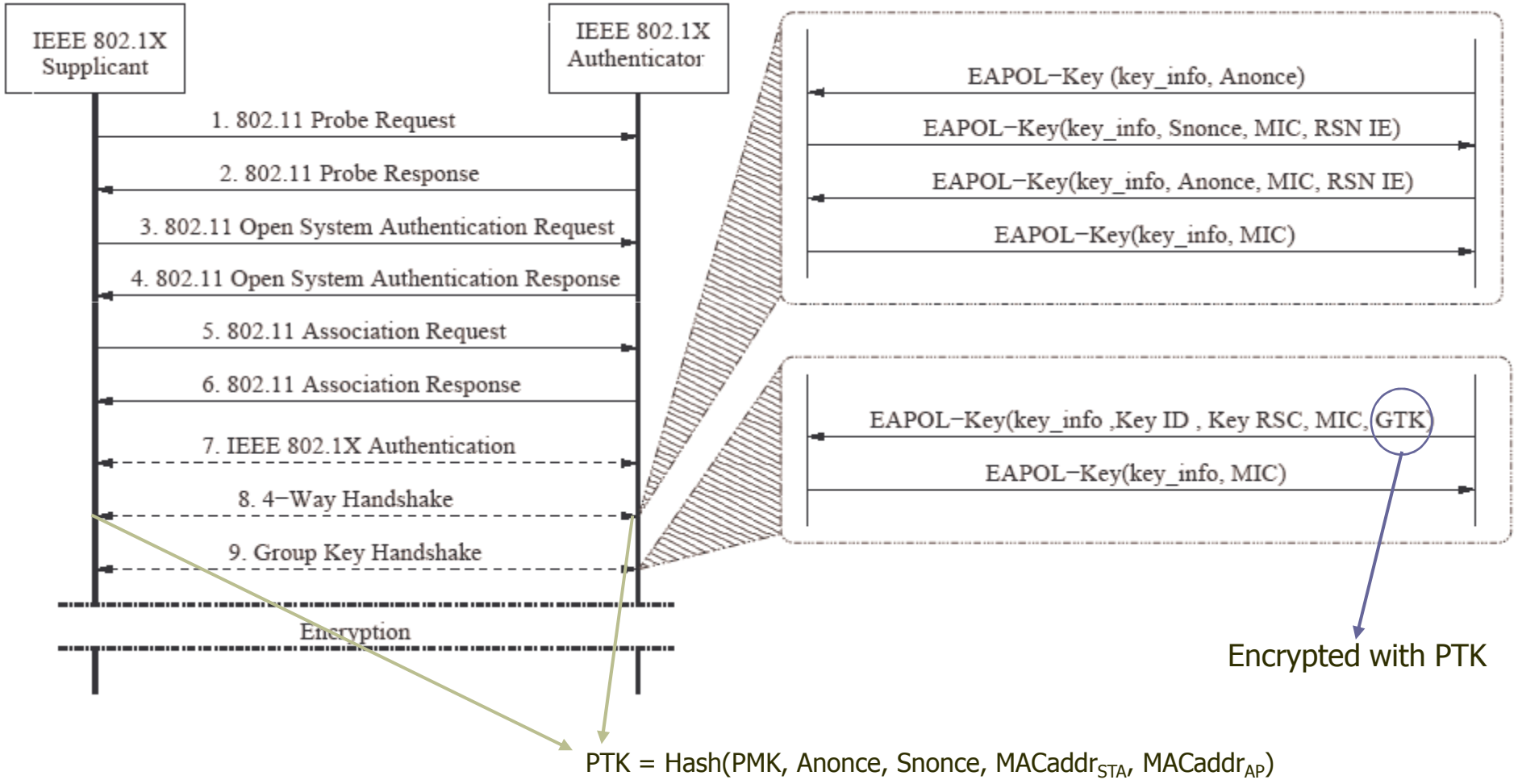


Key Management

1. Master Key (MK) generated from the authentication
2. Pairwise Master Key (PMK) generated from the MK
3. PMK sent to the AP through the AAA protocol (RADIUS)
4. Generation of the Pairwise Transient Key (PTK) through the 4-way handshake
5. Group key handshake (GTK) generated by the AP and sent though the Group key handshake



Key Management (2)



TKIP Key Encryption generation

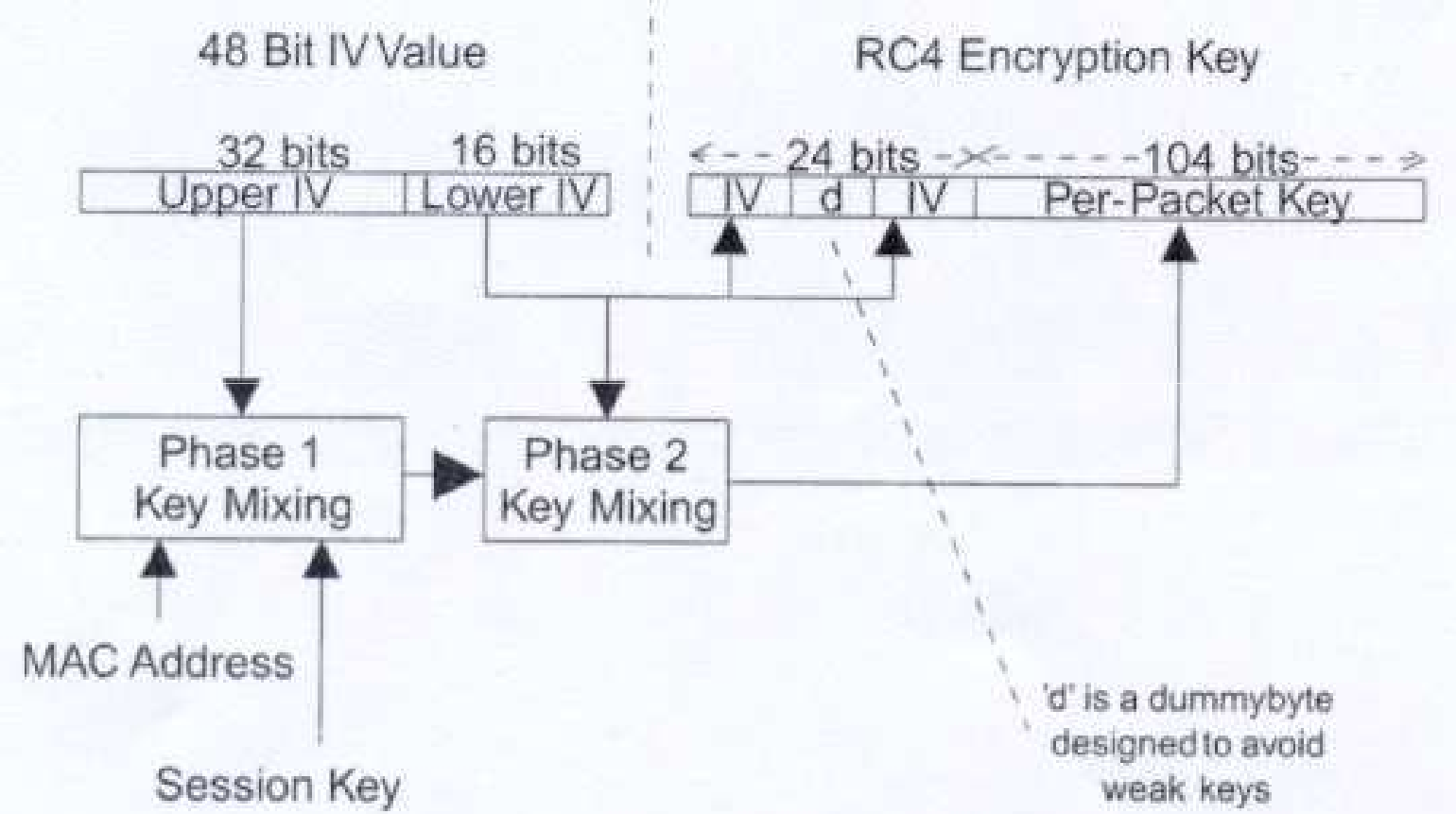


Figure 11.3 Creating the RC4 Encryption Key

Data frames – WEP, TKIP, and CCMP