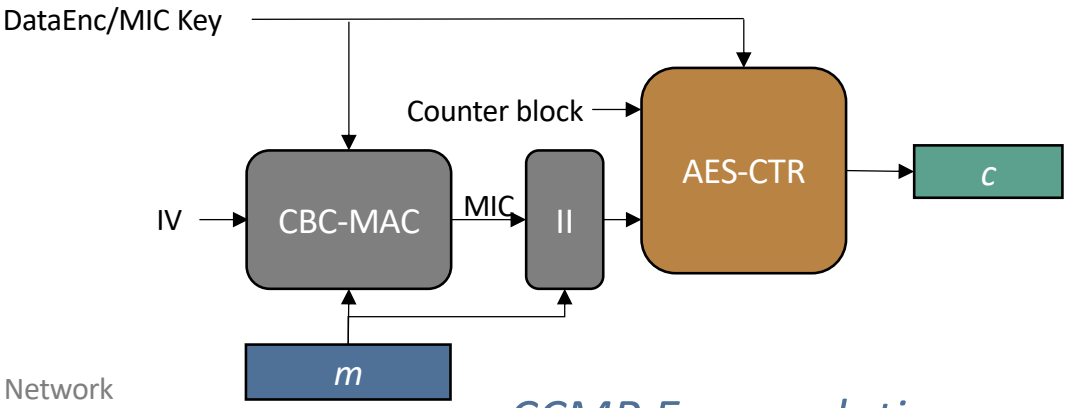
KRACK attack
(2017)

IEEE 802.11i
(2004)



RSN

TKIP

AES

RSN: Robust Security Network
MIC: Message Integrity Check
MAC: Media Access Control
CCMP: CTR mode with CBC-MAC Protocol

CCMP Encapsulation
Advanced Encryption Standard (AES)

+ *Integrity:*
CBC-MAC (AES)

+ *Confidentiality:*
AES-CTR

– *Attacks:*
KRACK, Kr00k, etc.

Backwards compatibility:
WEP, TKIP

Counter block (CB) *(128 bits)*

01011001

Flag	*Priority*	*Source Address*	*Packet No.*	*Counter*	
(8 bits)	(8 bits)	(48 bits)	(48 bits)	(16 bits)	1+

Initialization Vector (IV) *(128 bits)*

01011001

Flag	*Priority*	*Source Address*	*Packet No.*	*Data Length*
(8 bits)	(8 bits)	(48 bits)	(48 bits)	(16 bits)

CCMP Header *(64 bits)*

rrrrr1xy

Packet No.0-1	*Reserved*	*KeyID*	*Packet No.2-5*
(2x8 bits)	(8 bits)	(8 bits)	(4x8 bits)

r:reserved ; xy: KeyID (2 bits)

Pairwise Master Key - PMK (256 bits)

Pairwise Transient Key PTK (384 bits)

EAPOLMICKey (128 bits)	*EAPOLEncKey (128 bits)*	*DataEnc/MIC Key (128 bits)*

AES Pairwise Key Hierarchy

$$PTK = f(PMK, NonceAP, NonceSTA, MAC_{AP}, MAC_{STA})$$

Group Master Key - GMK (128 bits)

Group Transient Key GTK (128 bits)

DataEnc/MIC Key (128 bits)

AES Group Key Hierarchy

$$GTK = f(GMK, NonceAP, MAC_{AP})$$

802.11 frame