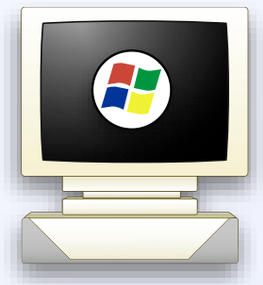
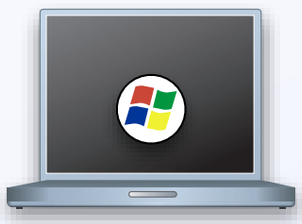
Podstawy bezpieczeństwa w sieciach bezprzewodowych

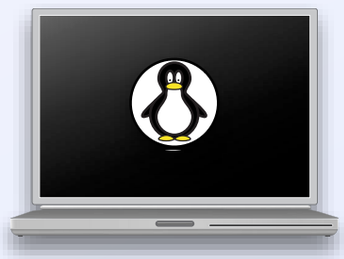
Protokół WEP - sposób działania, możliwe ataki, możliwe usprawnienia, następcy

Filip Piękniewski,
Wydział Matematyki i Informatyki UMK,
członek **IEEE**

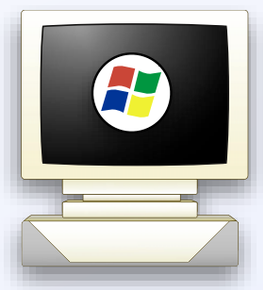
Sieci bezprzewodowe

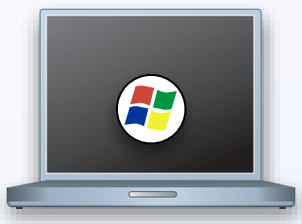


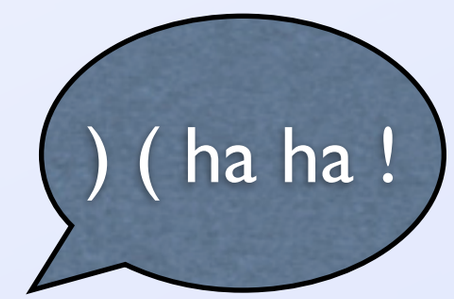


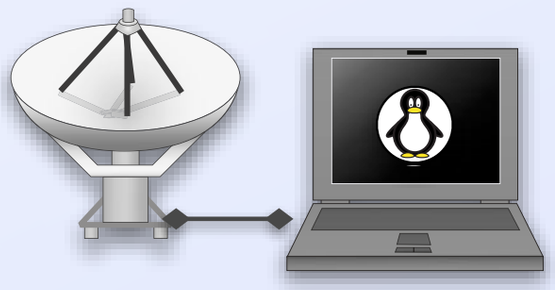


Sieci bezprzewodowe

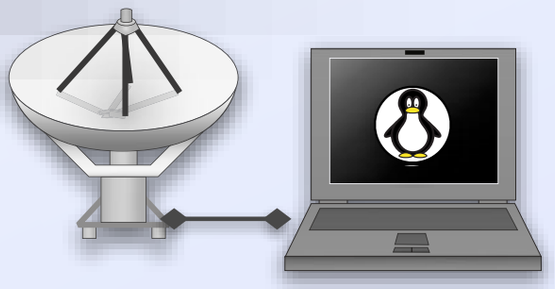


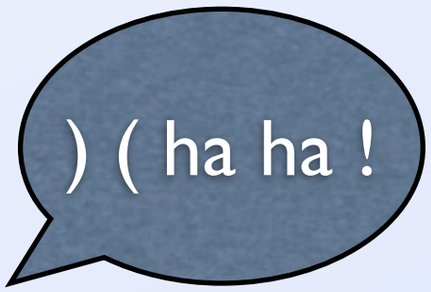






Sieci bezprzewodowe





WEP - historia

- **WEP - Wired Equivalent Privacy -** jest częścią standardu IEEE 802.11

WEP - historia

- **WEP - Wired Equivalent Privacy -** jest częścią standardu IEEE 802.11
- Został ratyfikowany w 1999 roku

WEP - historia

- **WEP - Wired Equivalent Privacy -** jest częścią standardu IEEE 802.11
- Został ratyfikowany w 1999 roku
- W 2001 roku wykazano słabości algorytmu RC4 używanego przez WEP [Scott R. Fluhrer, Itsik Mantin, Adi Shamir, **"Weaknesses in the Key Scheduling Algorithm of RC4"**. Selected Areas in Cryptography 2001: pp1–24.]

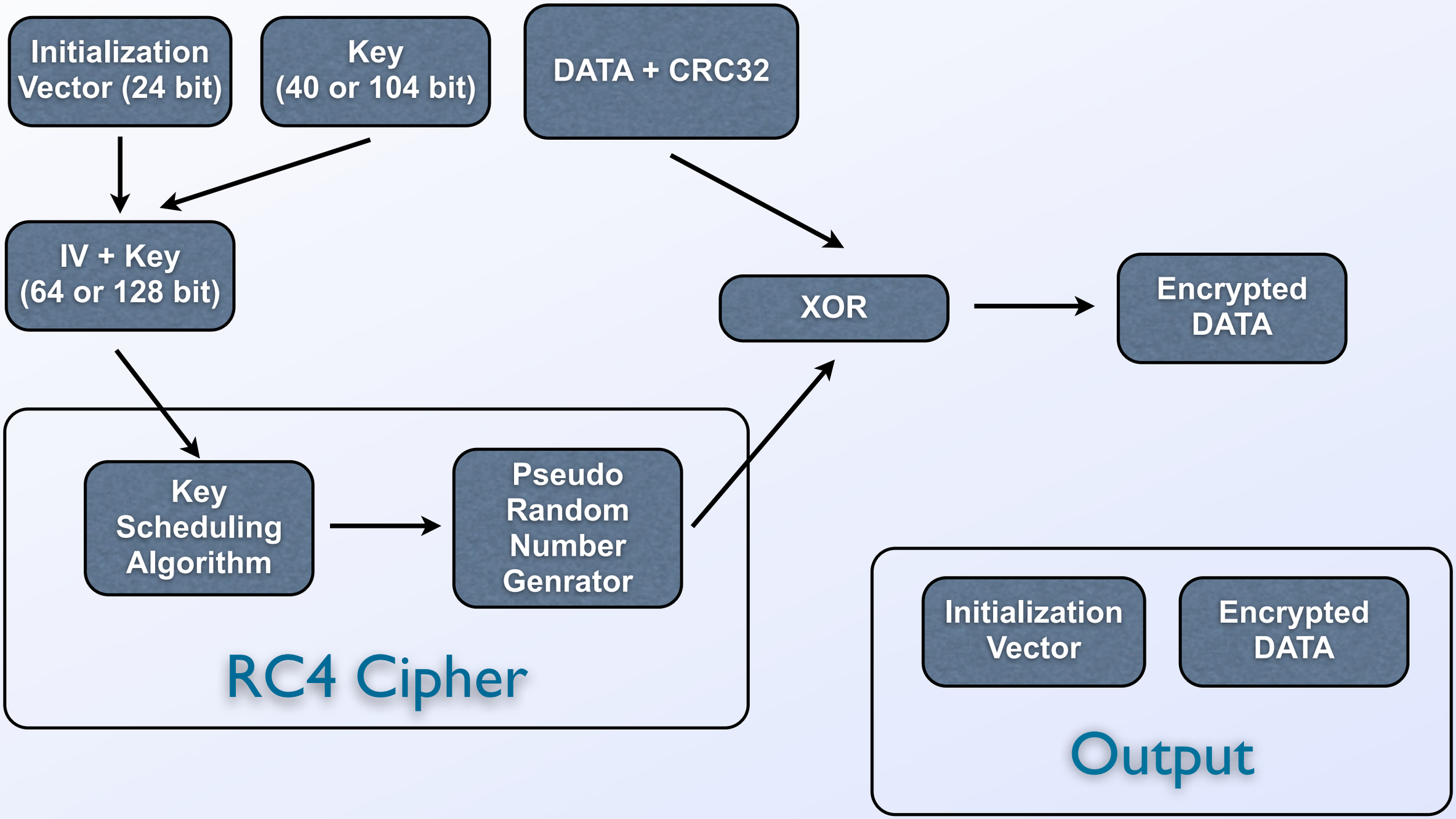
WEP - historia

- **WEP - Wired Equivalent Privacy -** jest częścią standardu IEEE 802.11
- Został ratyfikowany w 1999 roku
- W 2001 roku wykazano słabości algorytmu RC4 używanego przez WEP [Scott R. Fluhrer, Itsik Mantin, Adi Shamir, **"Weaknesses in the Key Scheduling Algorithm of RC4"**. Selected Areas in Cryptography 2001: pp1–24.]
- W 2003 wskazano na liczne słabości samego WEP [Nancy Cam-Winget, Russell Housley, David Wagner, Jesse Walker: **Security flaws in 802.11 data link protocols.** Communications of the ACM 46(5): 35-39 (2003)]

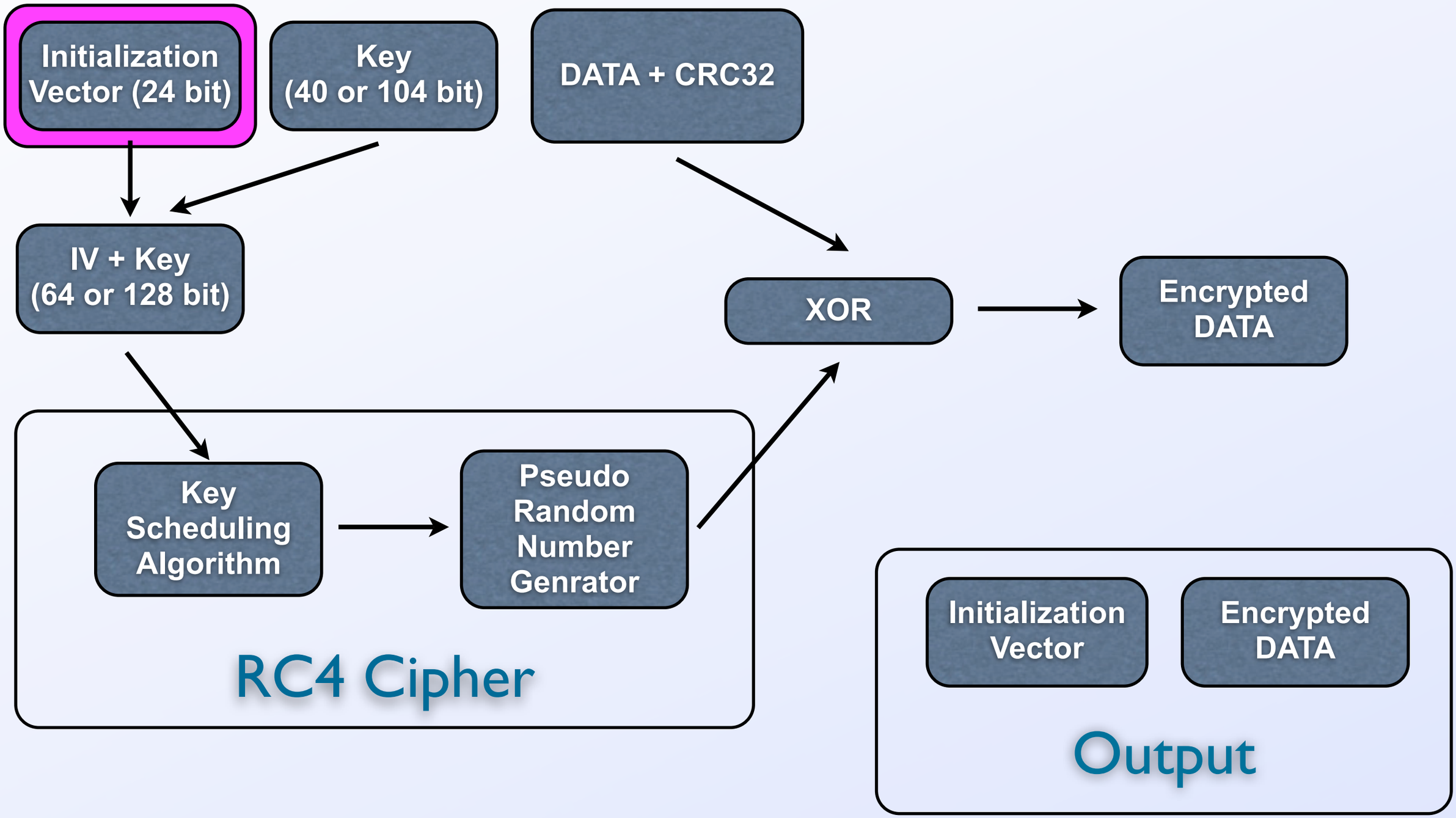
WEP - historia

- **WEP - Wired Equivalent Privacy -** jest częścią standardu IEEE 802.11
- Został ratyfikowany w 1999 roku
- W 2001 roku wykazano słabości algorytmu RC4 używanego przez WEP [Scott R. Fluhrer, Itsik Mantin, Adi Shamir, **"Weaknesses in the Key Scheduling Algorithm of RC4"**. Selected Areas in Cryptography 2001: pp1–24.]
- W 2003 wskazano na liczne słabości samego WEP [Nancy Cam-Winget, Russell Housley, David Wagner, Jesse Walker: **Security flaws in 802.11 data link protocols.** Communications of the ACM 46(5): 35-39 (2003)]
- W 2005 zademonstrowano złamanie klucza WEP publicznie dostępnymi narzędziami

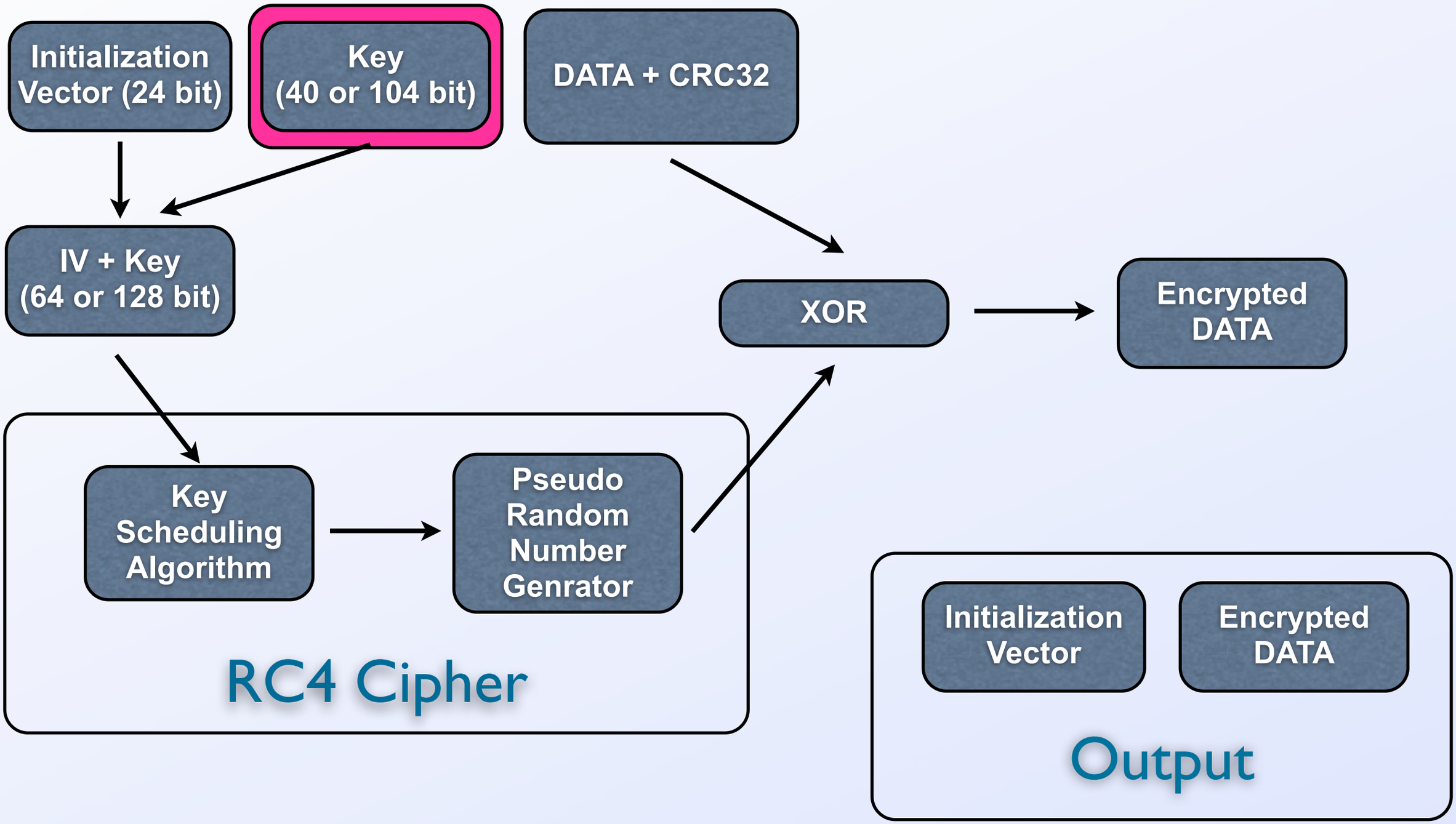
Schemat WEP - szyfrowanie



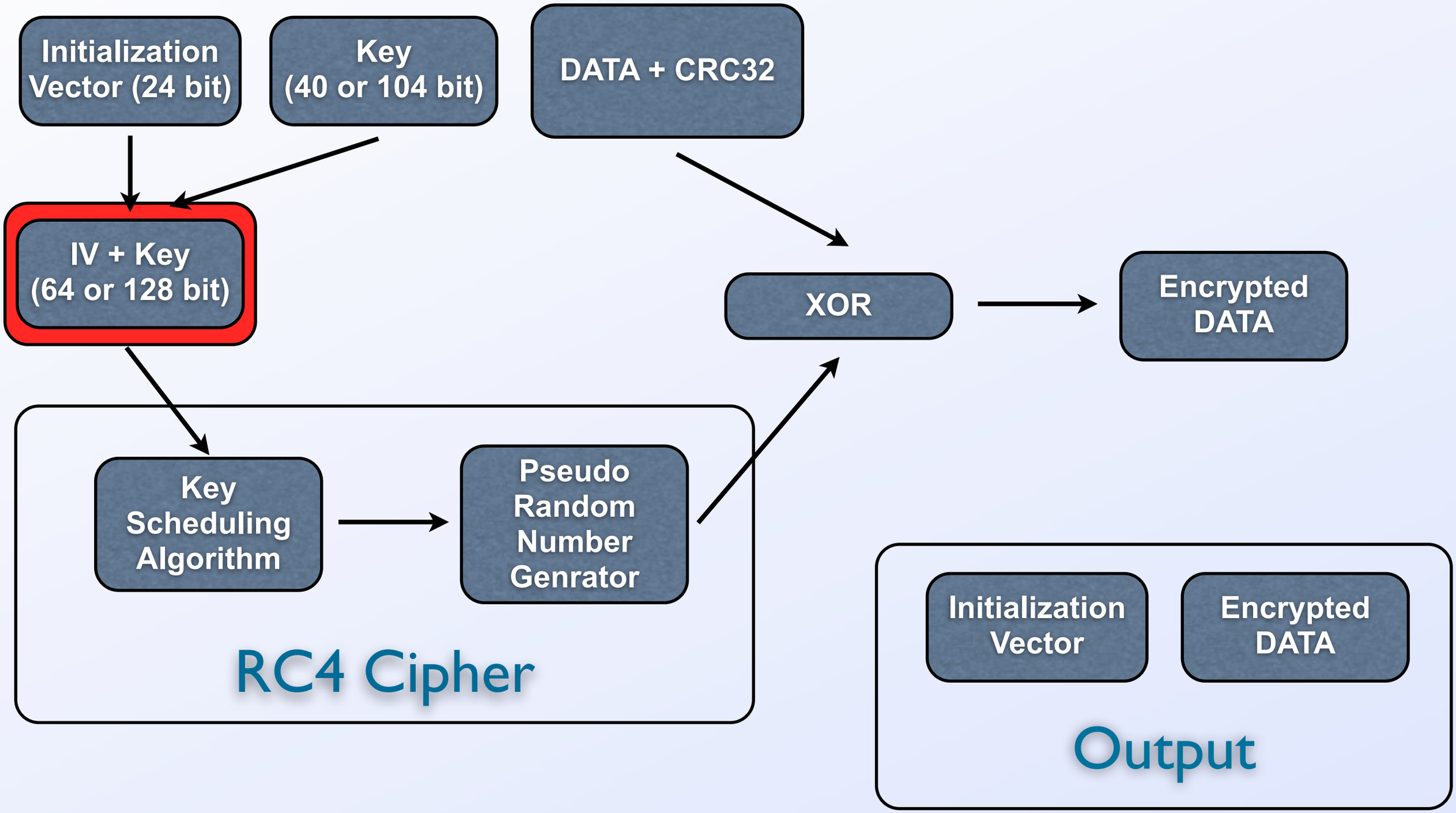
Schemat WEP - szyfrowanie



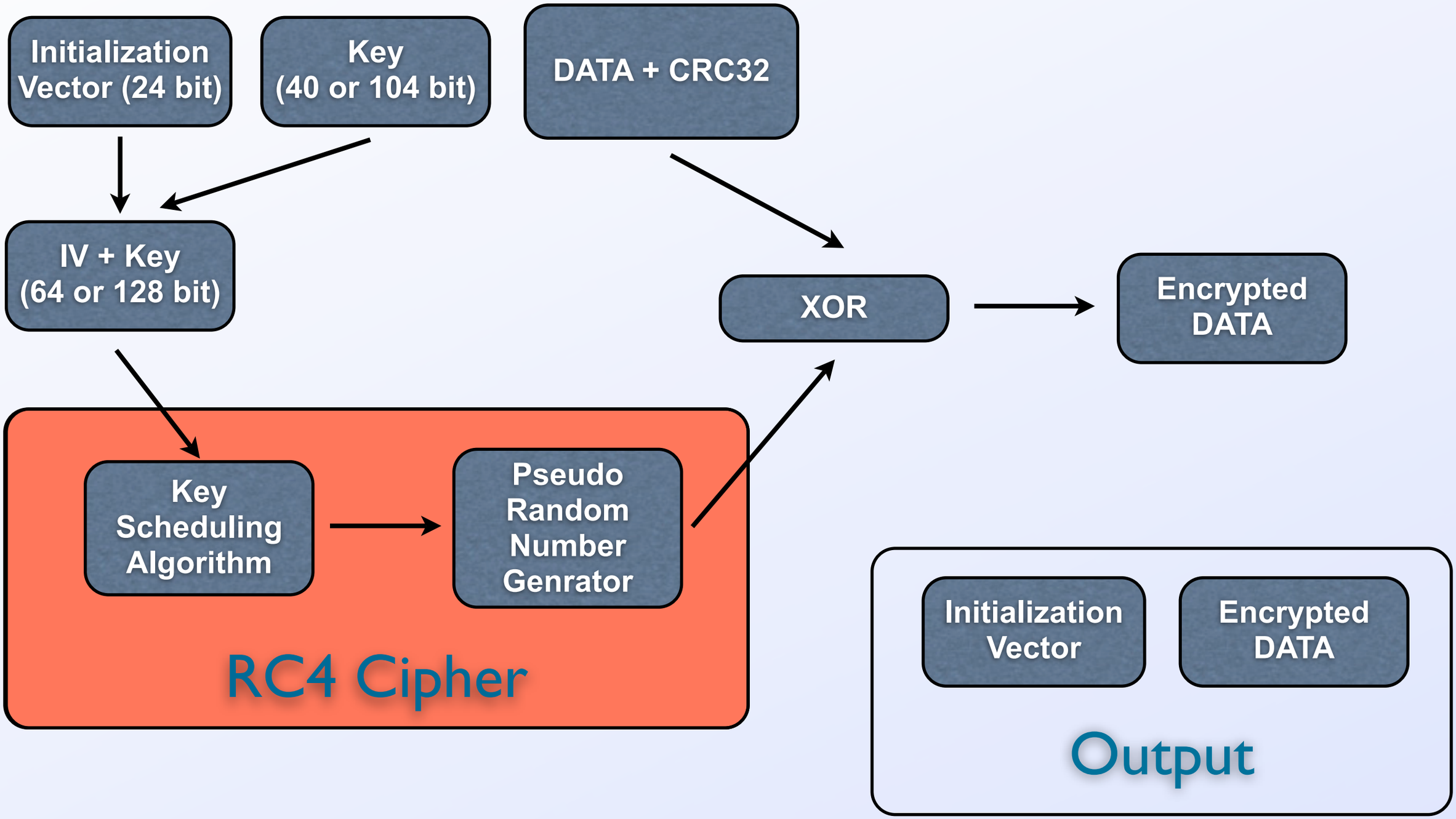
Schemat WEP - szyfrowanie



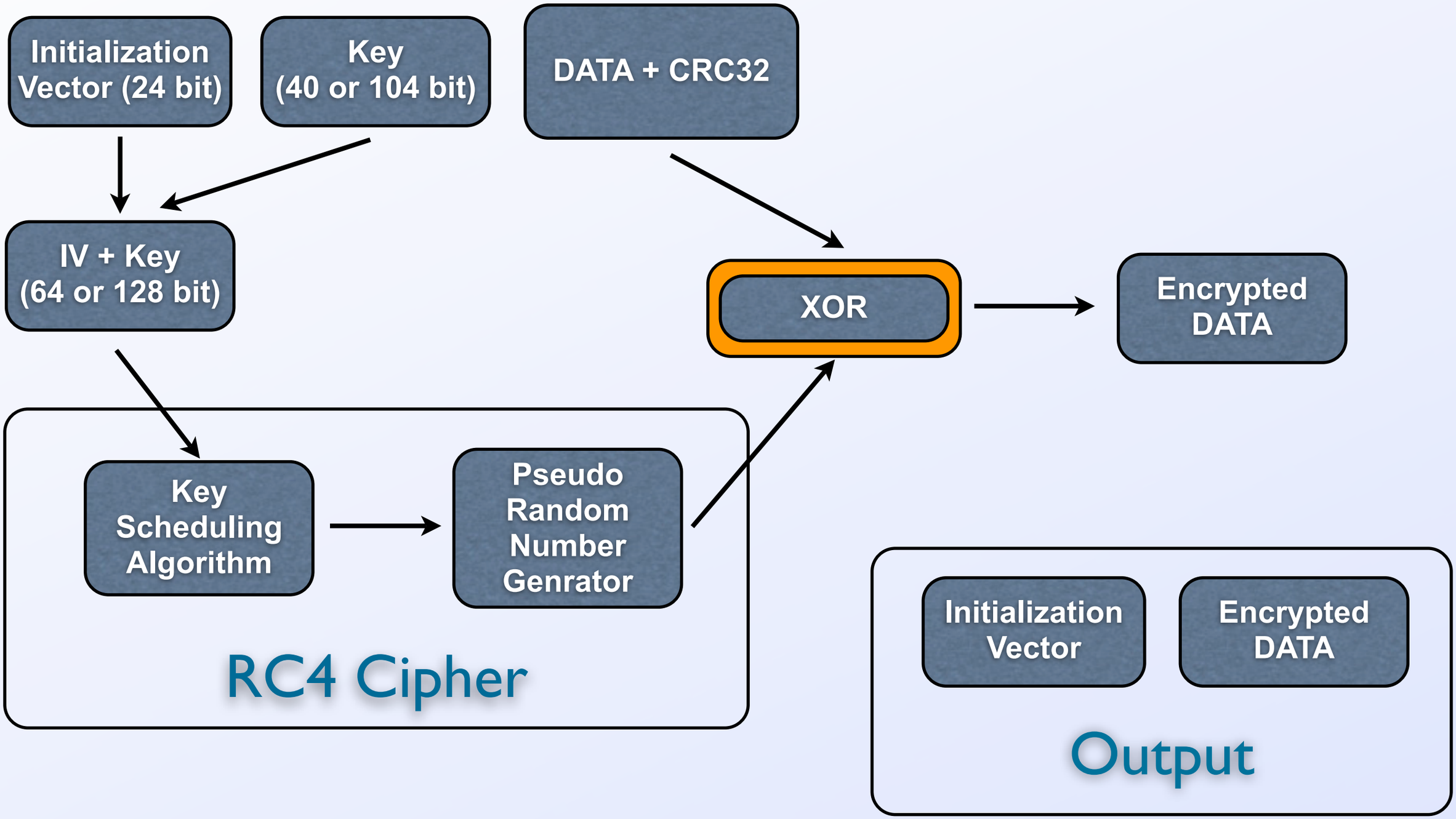
Schemat WEP - szyfrowanie



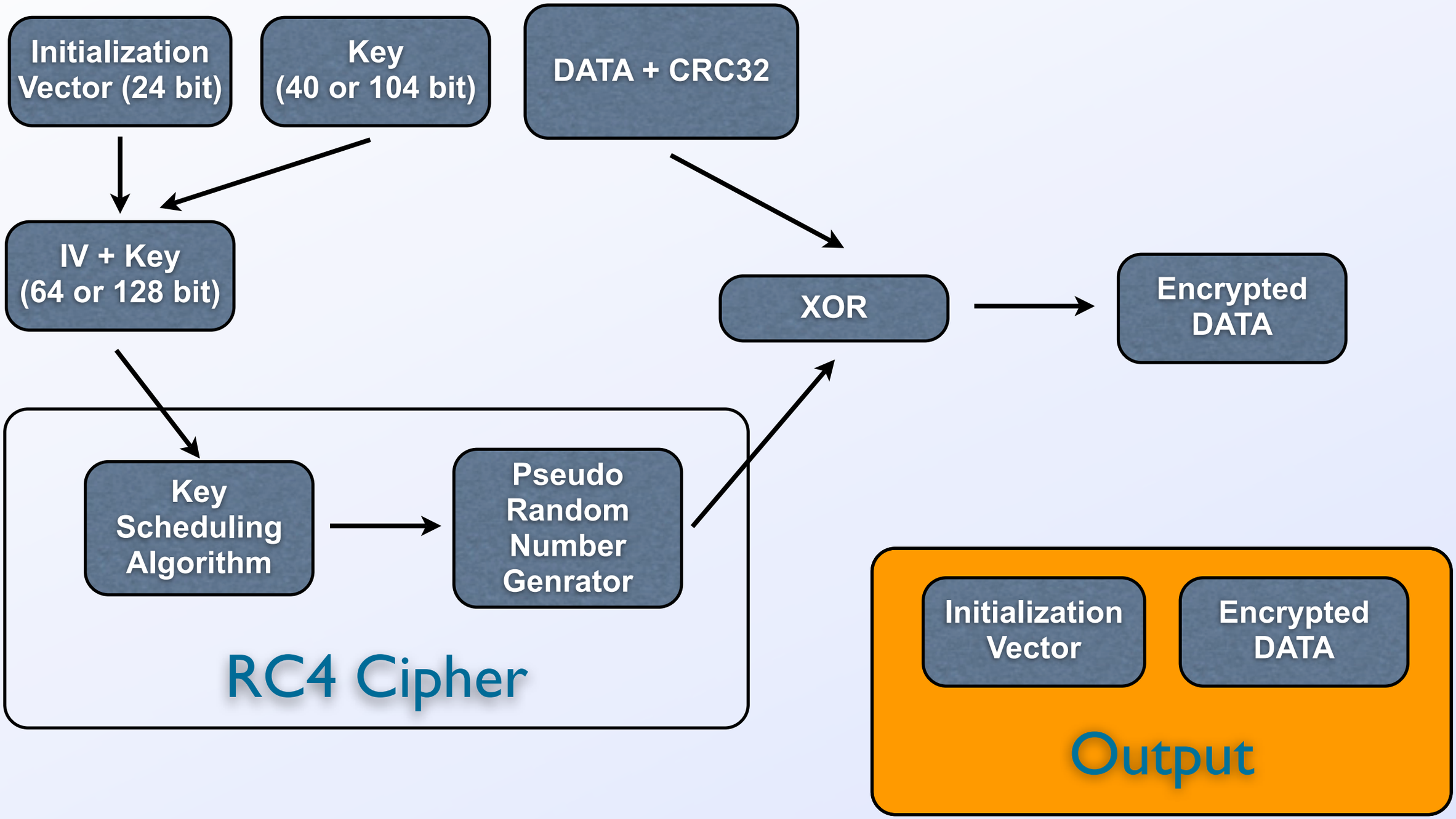
Schemat WEP - szyfrowanie



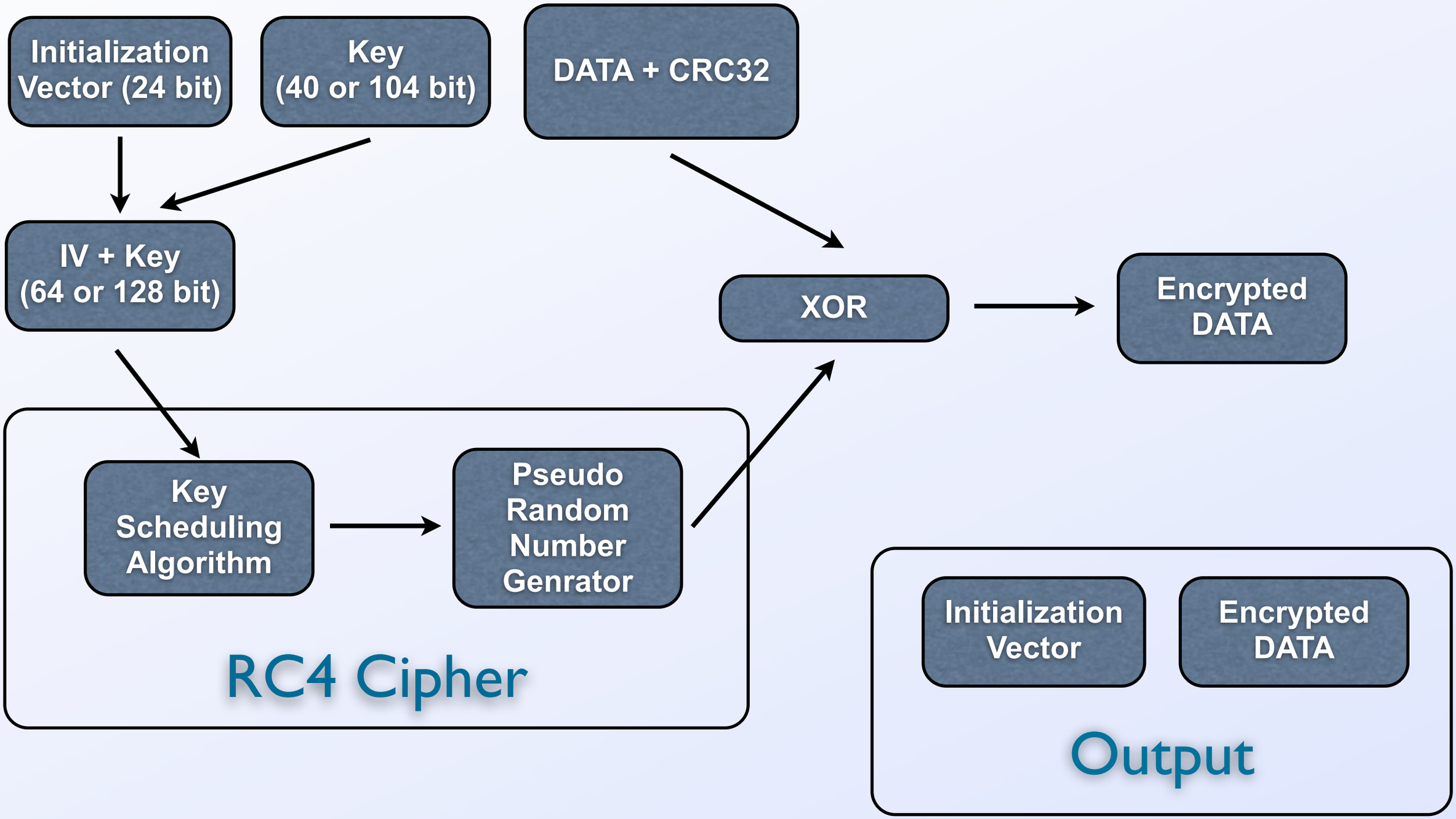
Schemat WEP - szyfrowanie



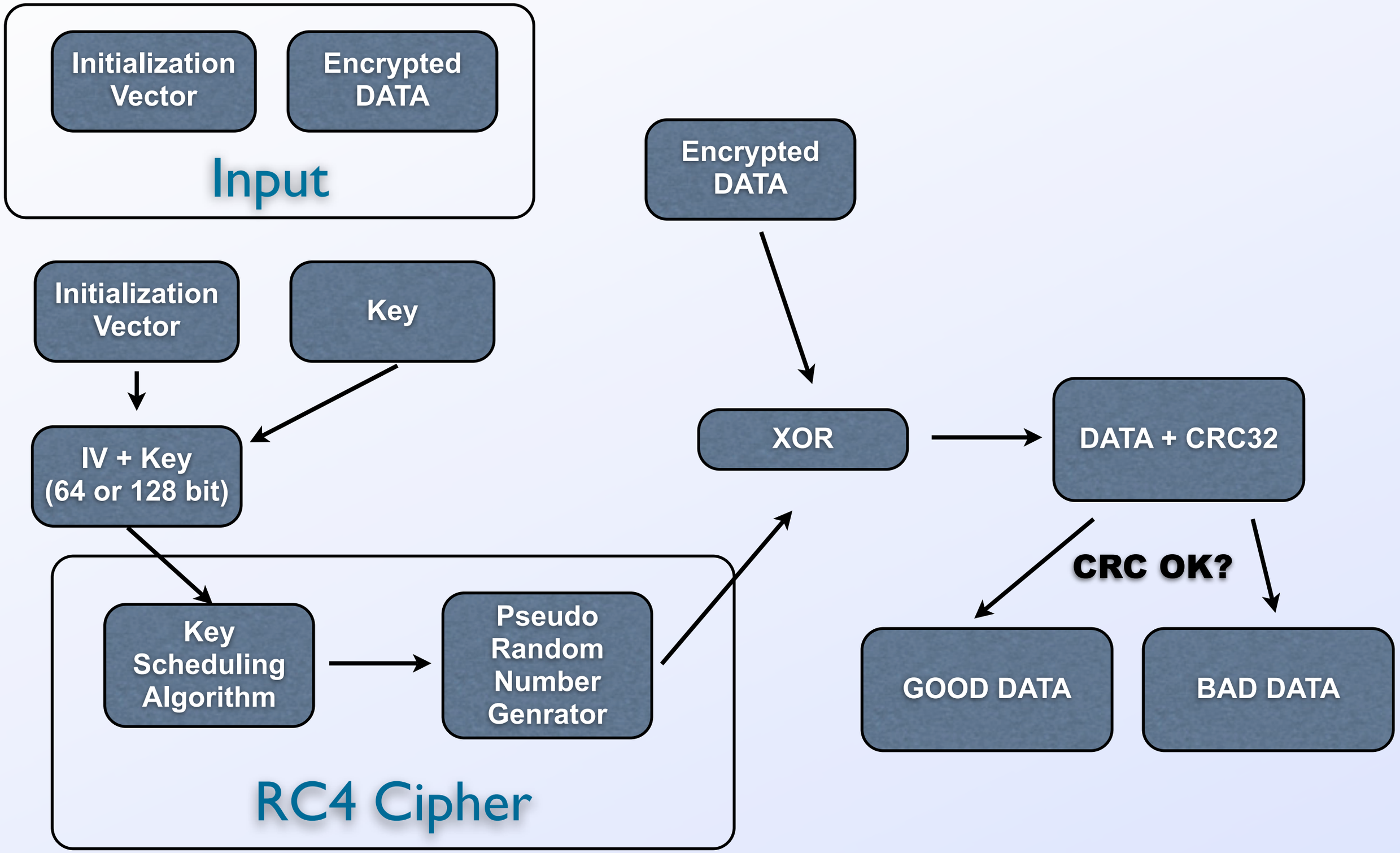
Schemat WEP - szyfrowanie



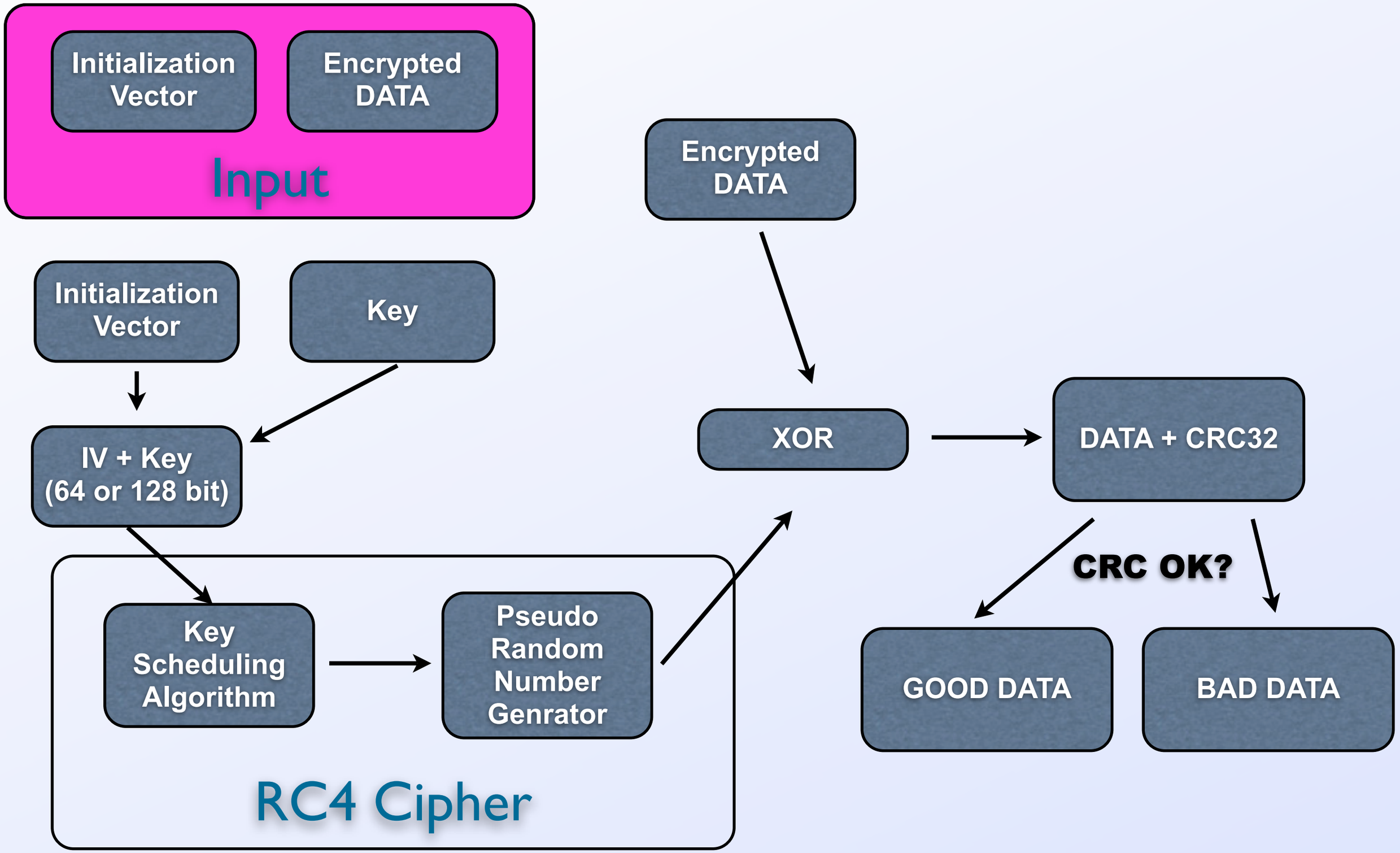
Schemat WEP - szyfrowanie



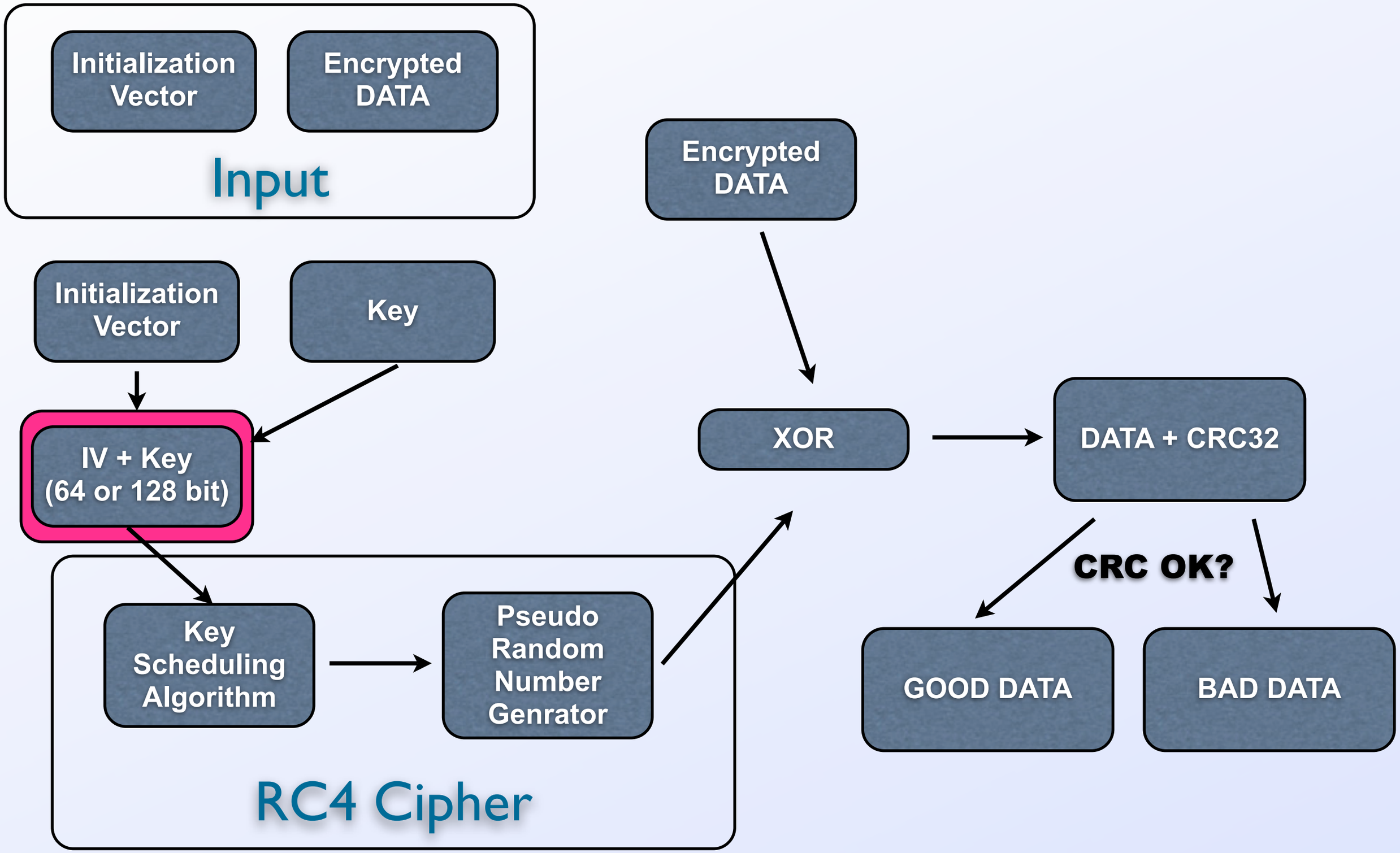
Schemat WEP - deszyfrowanie



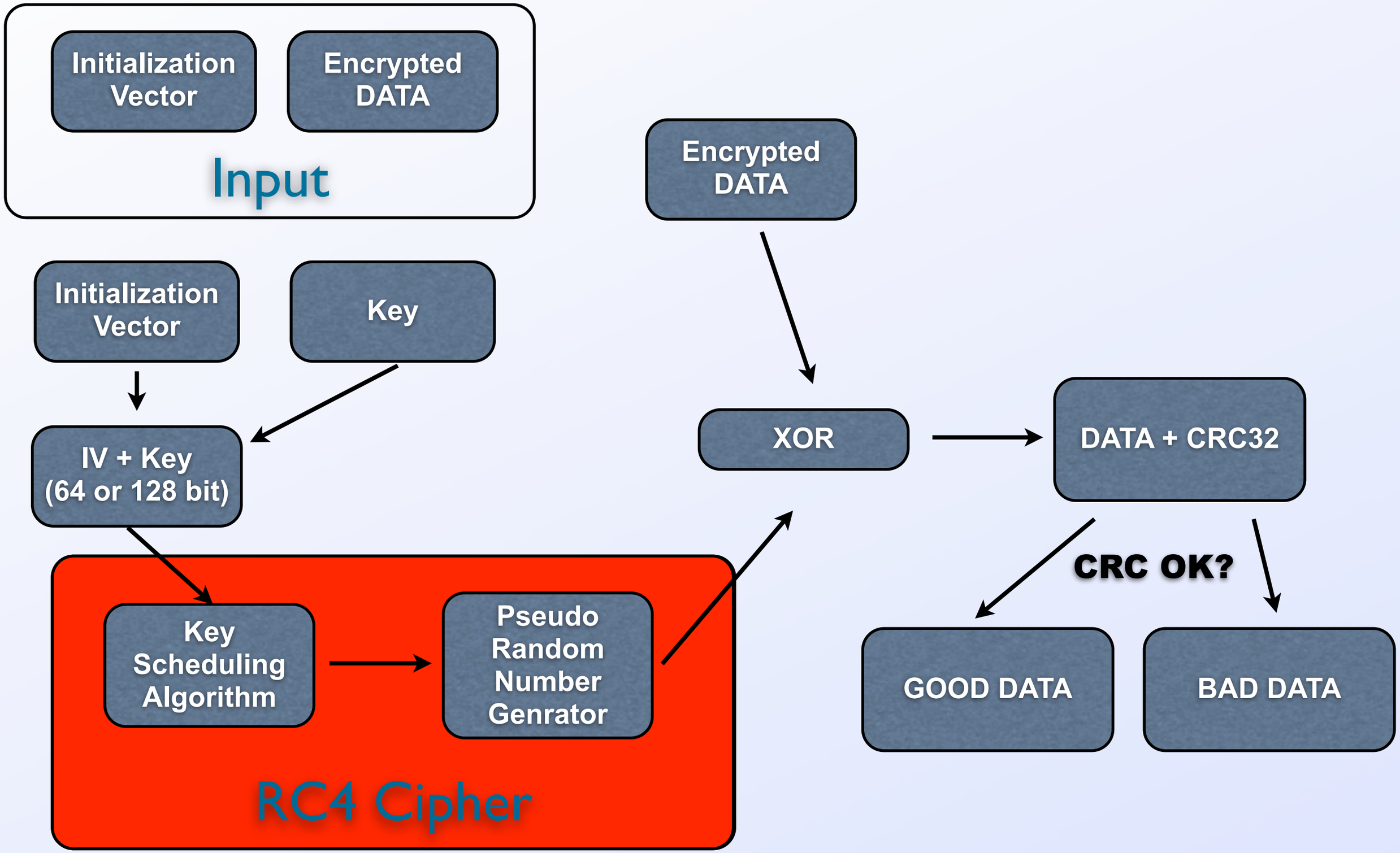
Schemat WEP - deszyfrowanie



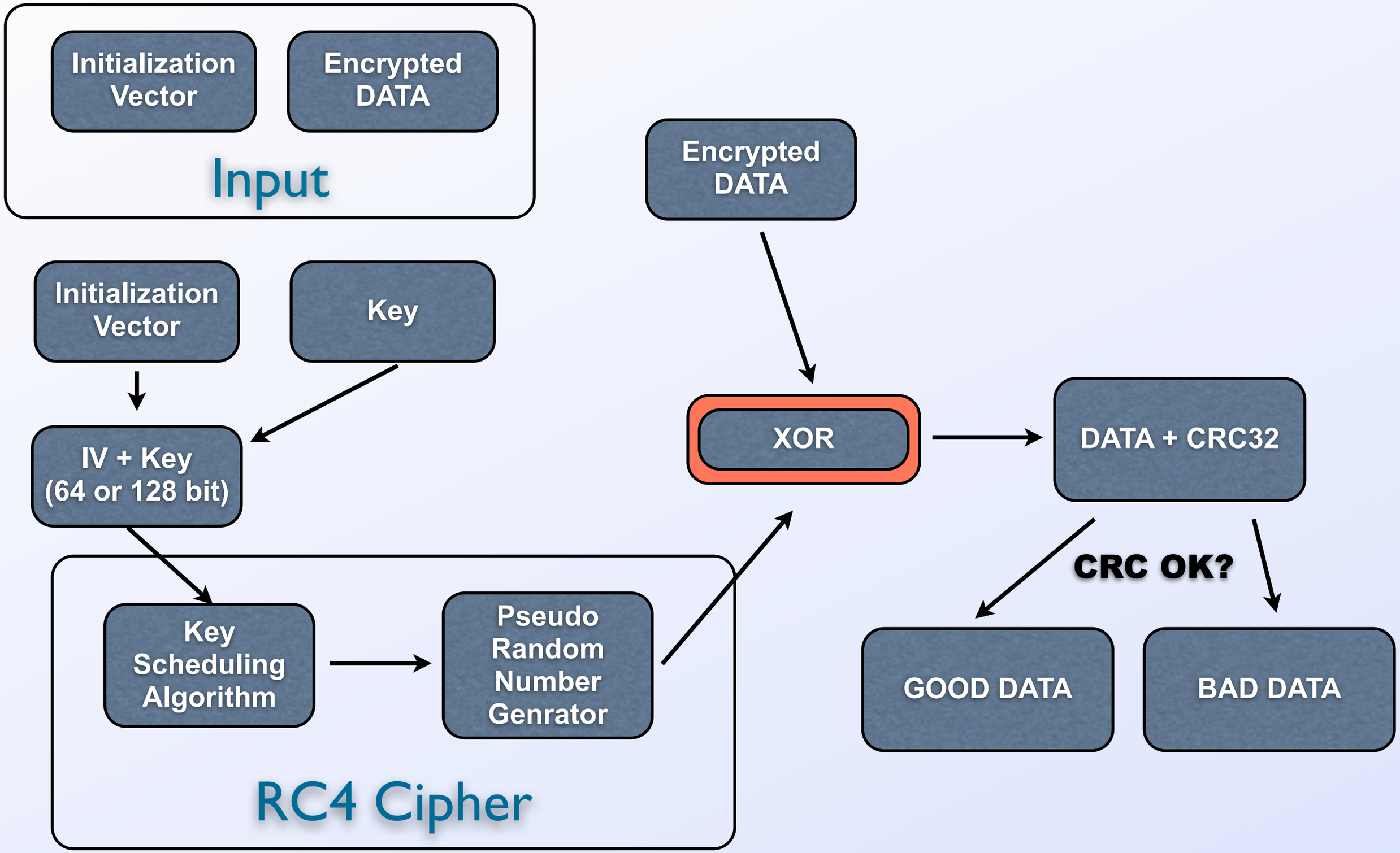
Schemat WEP - deszyfrowanie



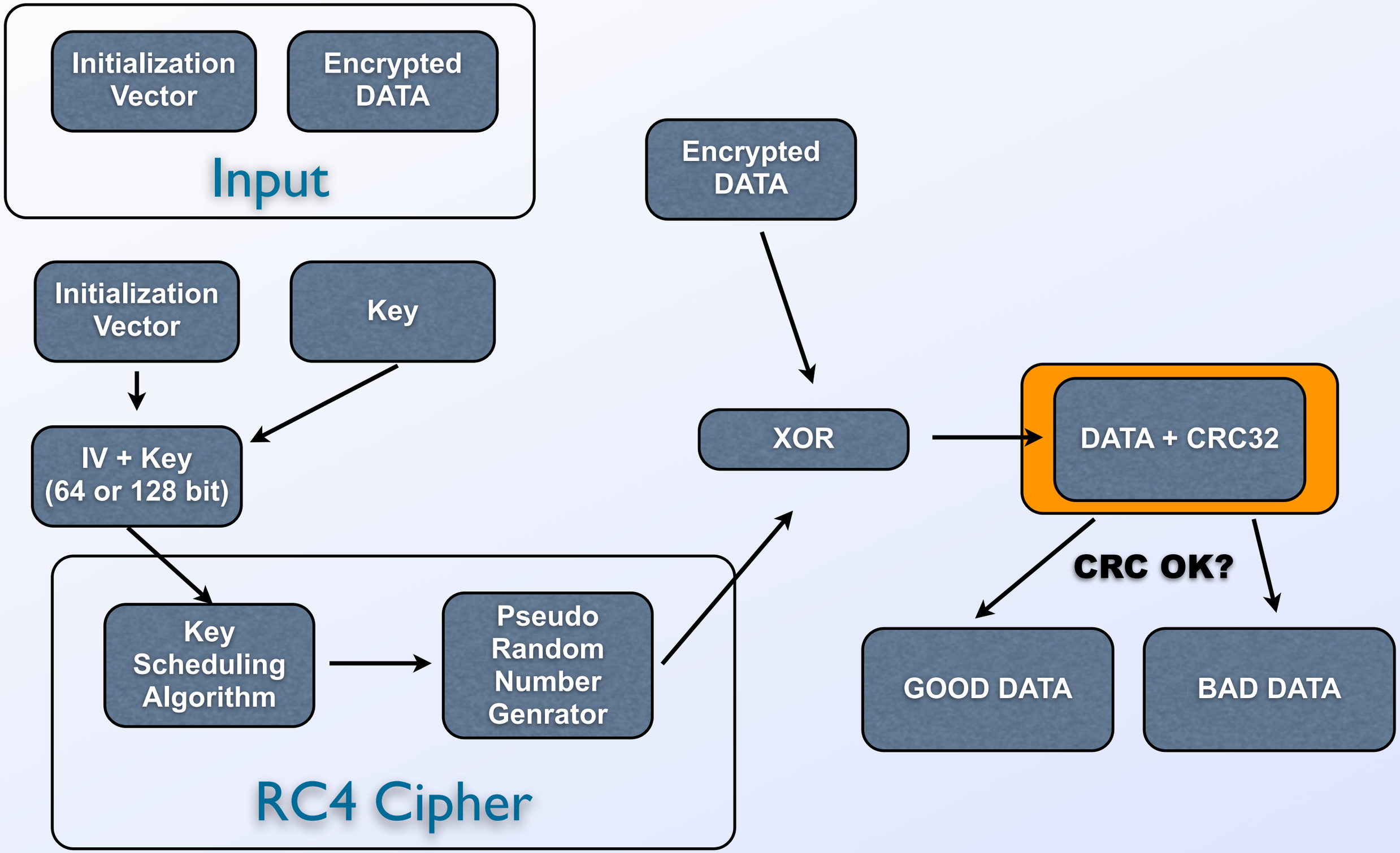
Schemat WEP - deszyfrowanie



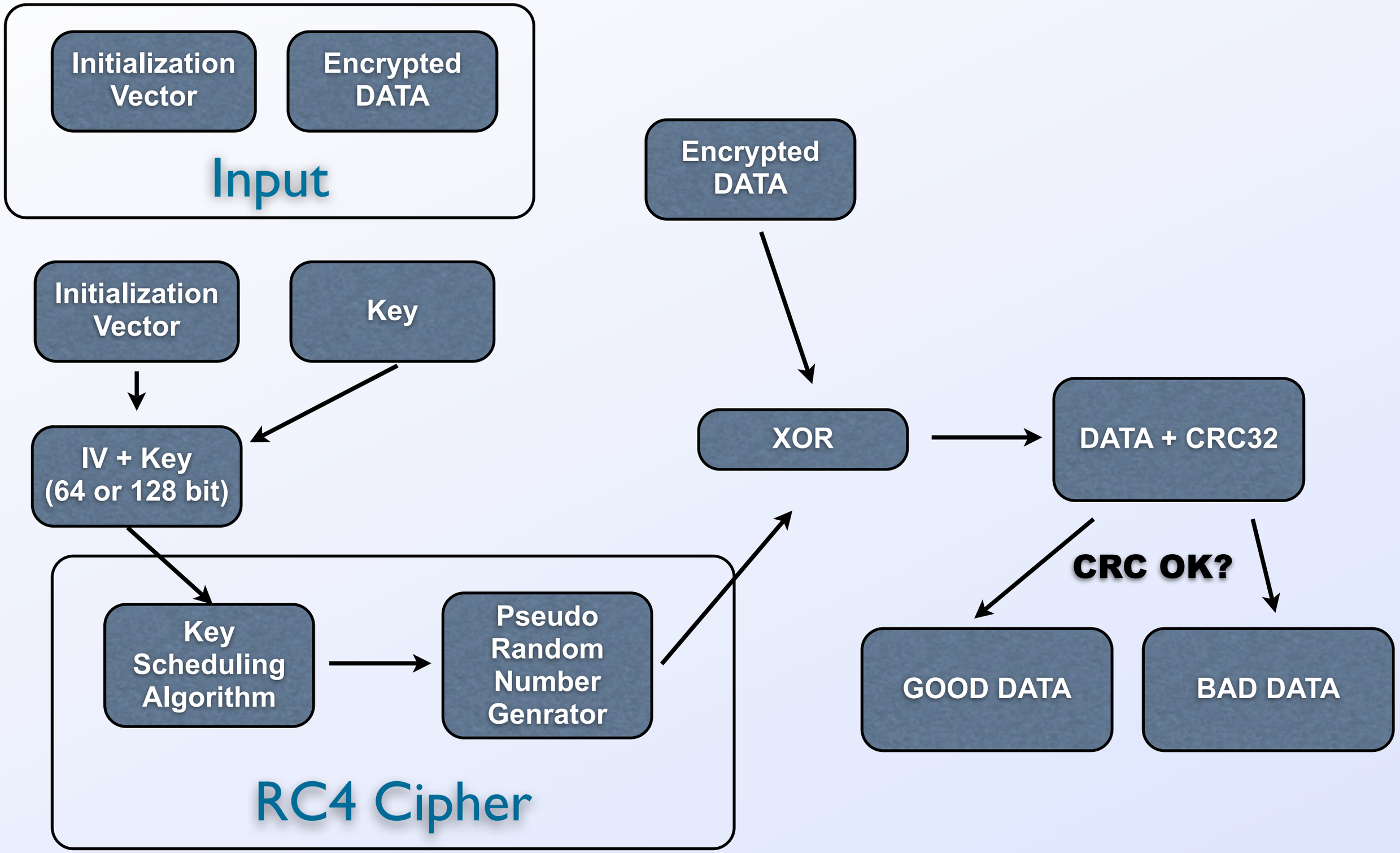
Schemat WEP - deszyfrowanie



Schemat WEP - deszyfrowanie



Schemat WEP - deszyfrowanie



Algorytm RC4

KSA

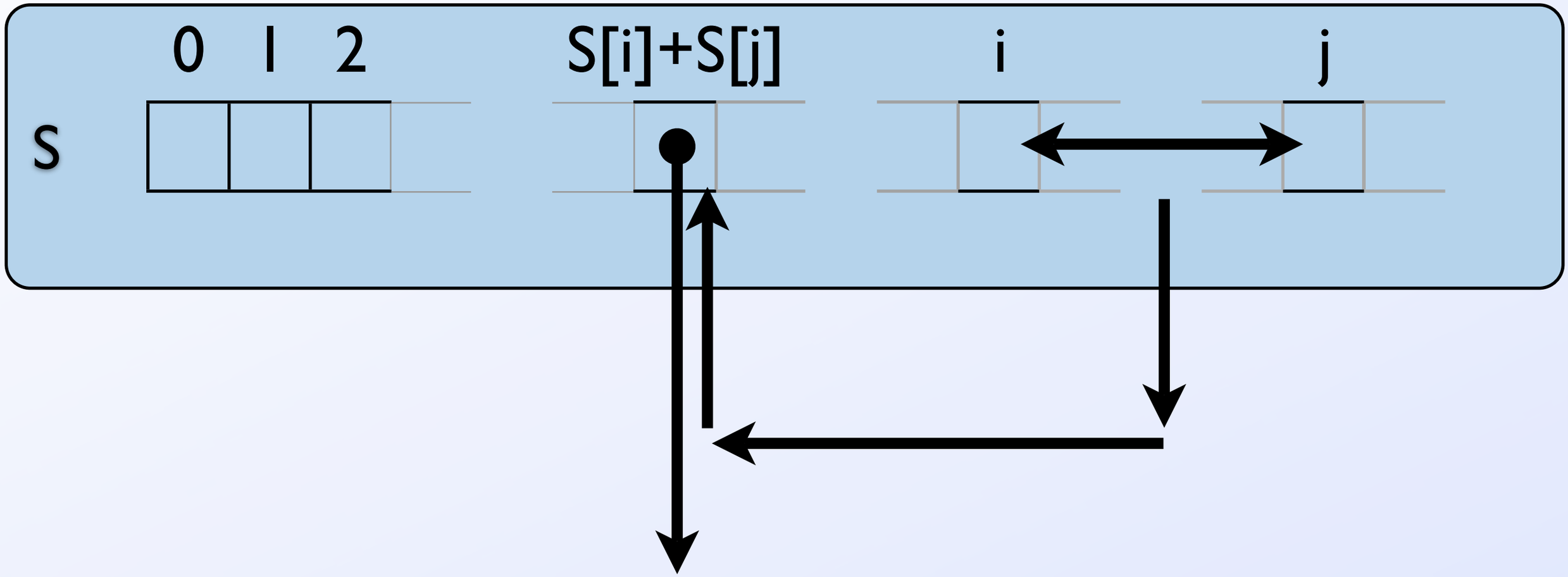
```
for i from 0 to 255
    S[i] := i
j := 0
for i from 0 to 255
    j := (j + S[i] + key[i mod keylength]) mod 256
    swap(S[i],S[j])
```

PRNG

```
i := 0
j := 0
while GeneratingOutput:
    i := (i + 1) mod 256
    j := (j + S[i]) mod 256
    swap(S[i],S[j])
    output S[(S[i] + S[j]) mod 256]
```

Algorytm RC4

i := (i + 1) mod 256 j := (j + S[i]) mod 256



output=S[S[i]+S[j] **mod** 256]

Problemy z WEPem

- Klucz jest jednakowy dla wszystkich użytkowników

Problemy z WEPem

- Klucz jest jednakowy dla wszystkich użytkowników
- Wektor inicjujący powinien być inny dla każdego pakietu, powinien mieć w miarę losowe bity. Wiele urządzeń te zalecenia ignoruje, karty sieciowe często inkrementują wartości wektora zaczynając od zera po każdym zresetowaniu karty

Problemy z WEPem

- Klucz jest jednakowy dla wszystkich użytkowników
- Wektor inicjujący powinien być inny dla każdego pakietu, powinien mieć w miarę losowe bity. Wiele urządzeń te zalecenia ignoruje, karty sieciowe często inkrementują wartości wektora zaczynając od zera po każdym zresetowaniu karty
- Nawet gdyby wektor inicjujący był wyznaczany losowo dla każdego pakietu, to średnio po 5000 pakietów powinien się powtórzyć (paradoks dnia narodzin)

Problemy z WEPem

- Klucz jest jednakowy dla wszystkich użytkowników
- Wektor inicjujący powinien być inny dla każdego pakietu, powinien mieć w miarę losowe bity. Wiele urządzeń te zalecenia ignoruje, karty sieciowe często inkrementują wartości wektora zaczynając od zera po każdym zresetowaniu karty
- Nawet gdyby wektor inicjujący był wyznaczany losowo dla każdego pakietu, to średnio po 5000 pakietów powinien się powtórzyć (paradoks dnia narodzin)
- Posiadanie dwóch pakietów zakodowanych tą samą sekwencją kluczową pozwala poznać ich różnicę symetryczną. Mając kolekcję takich pakietów, można je poddać analizie statystycznej

Problemy z WEPem

- Klucz jest jednakowy dla wszystkich użytkowników
- Wektor inicjujący powinien być inny dla każdego pakietu, powinien mieć w miarę losowe bity. Wiele urządzeń te zalecenia ignoruje, karty sieciowe często inkrementują wartości wektora zaczynając od zera po każdym zresetowaniu karty
- Nawet gdyby wektor inicjujący był wyznaczany losowo dla każdego pakietu, to średnio po 5000 pakietów powinien się powtórzyć (paradoks dnia narodzin)
- Posiadanie dwóch pakietów zakodowanych tą samą sekwencją kluczową pozwala poznać ich różnicę symetryczną. Mając kolekcję takich pakietów, można je poddać analizie statystycznej
- CRC32 jest kodem liniowym. Atakujący może negować bity w zaszyfrowanym tekście, jednocześnie odpowiednio modyfikować zaszyfrowaną sumę kontrolną

Pasywny atak na WEP

- KSA w algorytmie RC4 posiada wiele słabości

Pasywny atak na WEP

- KSA w algorytmie RC4 posiada wiele słabości
- Znając początkowy fragment sekwencji kluczowej można wiele wywnioskować na temat początkowej permutacji

Pasywny atak na WEP

- KSA w algorytmie RC4 posiada wiele słabości
- Znając początkowy fragment sekwencji kluczowej można wiele wywnioskować na temat początkowej permutacji
- Odkrycie początkowej permutacji jest jeszcze łatwiejsze gdy znamy fragment klucza (wektor inicjujący)

Pasywny atak na WEP

- KSA w algorytmie RC4 posiada wiele słabości
- Znając początkowy fragment sekwencji kluczowej można wiele wywnioskować na temat początkowej permutacji
- Odkrycie początkowej permutacji jest jeszcze łatwiejsze gdy znamy fragment klucza (wektor inicjujący)
- Mając zestaw informacji o początkowej permutacji dla kilku znanych fragmentów klucza pozwala wydobyć informację o kolejnych bajtach klucza

Pasywny atak na WEP

- KSA w algorytmie RC4 posiada wiele słabości
- Znając początkowy fragment sekwencji kluczowej można wiele wywnioskować na temat początkowej permutacji
- Odkrycie początkowej permutacji jest jeszcze łatwiejsze gdy znamy fragment klucza (wektor inicjujący)
- Mając zestaw informacji o początkowej permutacji dla kilku znanych fragmentów klucza pozwala wydobyć informację o kolejnych bajtach klucza
- Im więcej bajtów klucza znamy, tym łatwiej wydobyć następne !!!

Pasywny atak na WEP

- Zbieramy dużą ilość pakietów (szczególnie interesujące są kolizje wektorów IV)

Pasywny atak na WEP

- Zbieramy dużą ilość pakietów (szczególnie interesujące są kolizje wektorów IV)
- Poddajemy zebrany materiał analizie statystycznej, wydobywamy początkowe fragmenty strumienia szyfrującego dla różnych IV

Pasywny atak na WEP

- Zbieramy dużą ilość pakietów (szczególnie interesujące są kolizje wektorów IV)

- Poddajemy zebrany materiał analizie statystycznej, wydobywamy początkowe fragmenty strumienia szyfrującego dla różnych IV

- Odtwarzamy kolejne fragmenty klucza WEP na podstawie wczesnych stanów permutacji

Pasywny atak na WEP

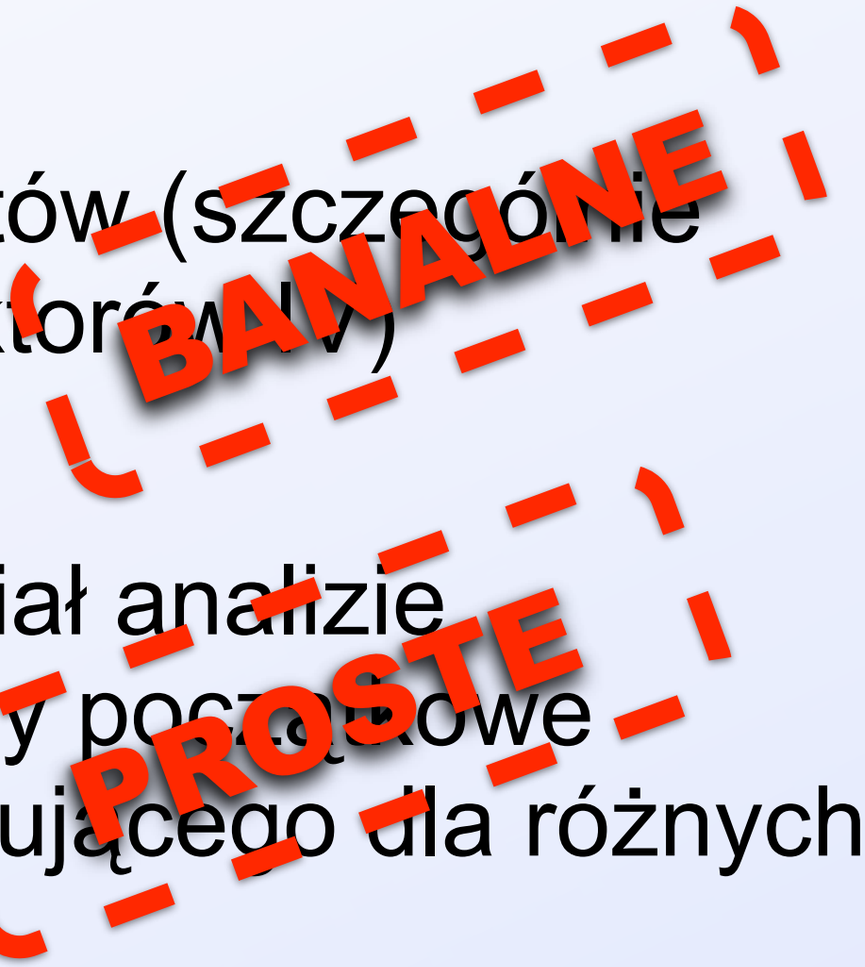
- Zbieramy dużą ilość pakietów (szczególnie interesujące są kolizje wektorów IV)

- Poddajemy zebrany materiał analizie statystycznej, wydobywamy początkowe fragmenty strumienia szyfrującego dla różnych IV

- Odtwarzamy kolejne fragmenty klucza WEP na podstawie wczesnych stanów permutacji

Pasywny atak na WEP

- Zbieramy dużą ilość pakietów (szczególnie interesujące są kolizje wektorów IV)



- Poddajemy zebrany materiał analizie statystycznej, wydobywamy początkowe fragmenty strumienia szyfrującego dla różnych IV

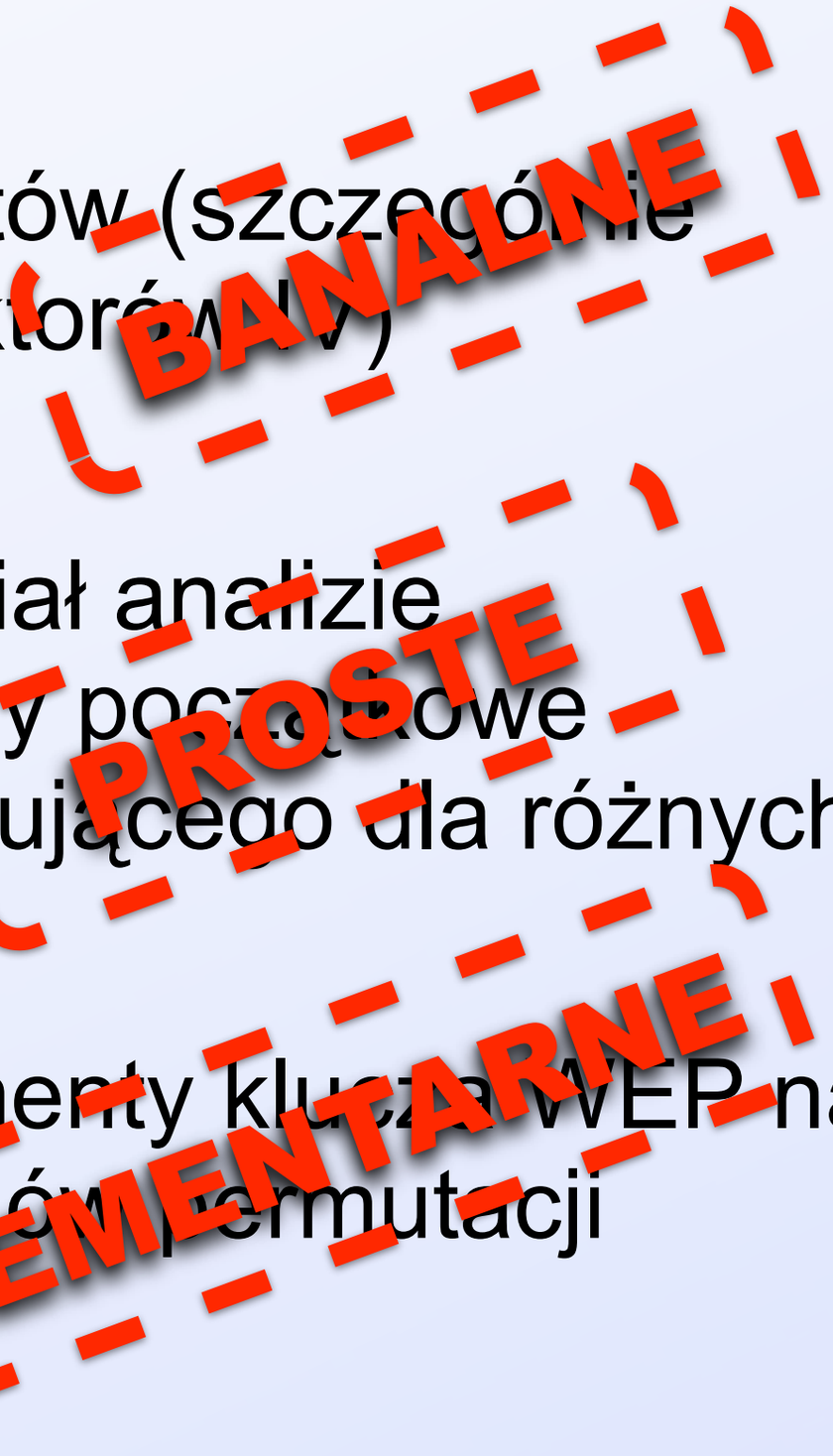
- Odtwarzamy kolejne fragmenty klucza WEP na podstawie wczesnych stanów permutacji

Pasywny atak na WEP

- Zbieramy dużą ilość pakietów (szczególnie interesujące są kolizje wektorów IV)

- Poddajemy zebrany materiał analizie statystycznej, wydobywamy początkowe fragmenty strumienia szyfrującego dla różnych IV

- Odtwarzamy kolejne fragmenty klucza WEP na podstawie wczesnych stanów permutacji



Pasywny atak na WEP

- Wymaga zdobycia średnio rzędu **kilku milionów** pakietów (co odpowiada zaledwie **parunastu minutom** nasłuchiwania obciążonego AP)

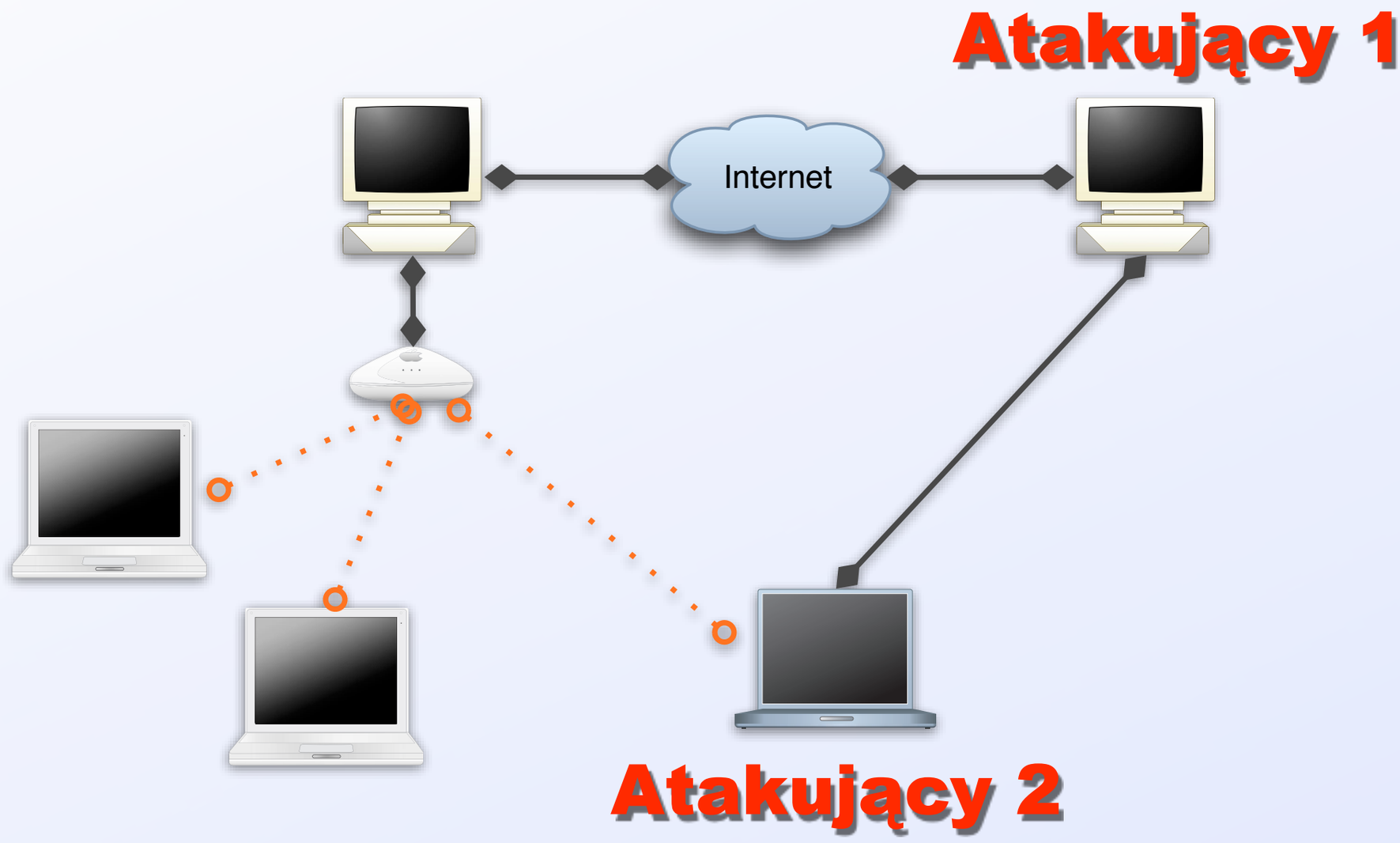
Pasywny atak na WEP

- Wymaga zdobycia średnio rzędu **kilku milionów** pakietów (co odpowiada zaledwie **parunastu minutom** nasłuchiwania obciążonego AP)
- Często klucz można odkryć znacznie wcześniej jeśli jest on jednym ze **słabych kluczy**, które inicjują zbyt prostą permutację początkową

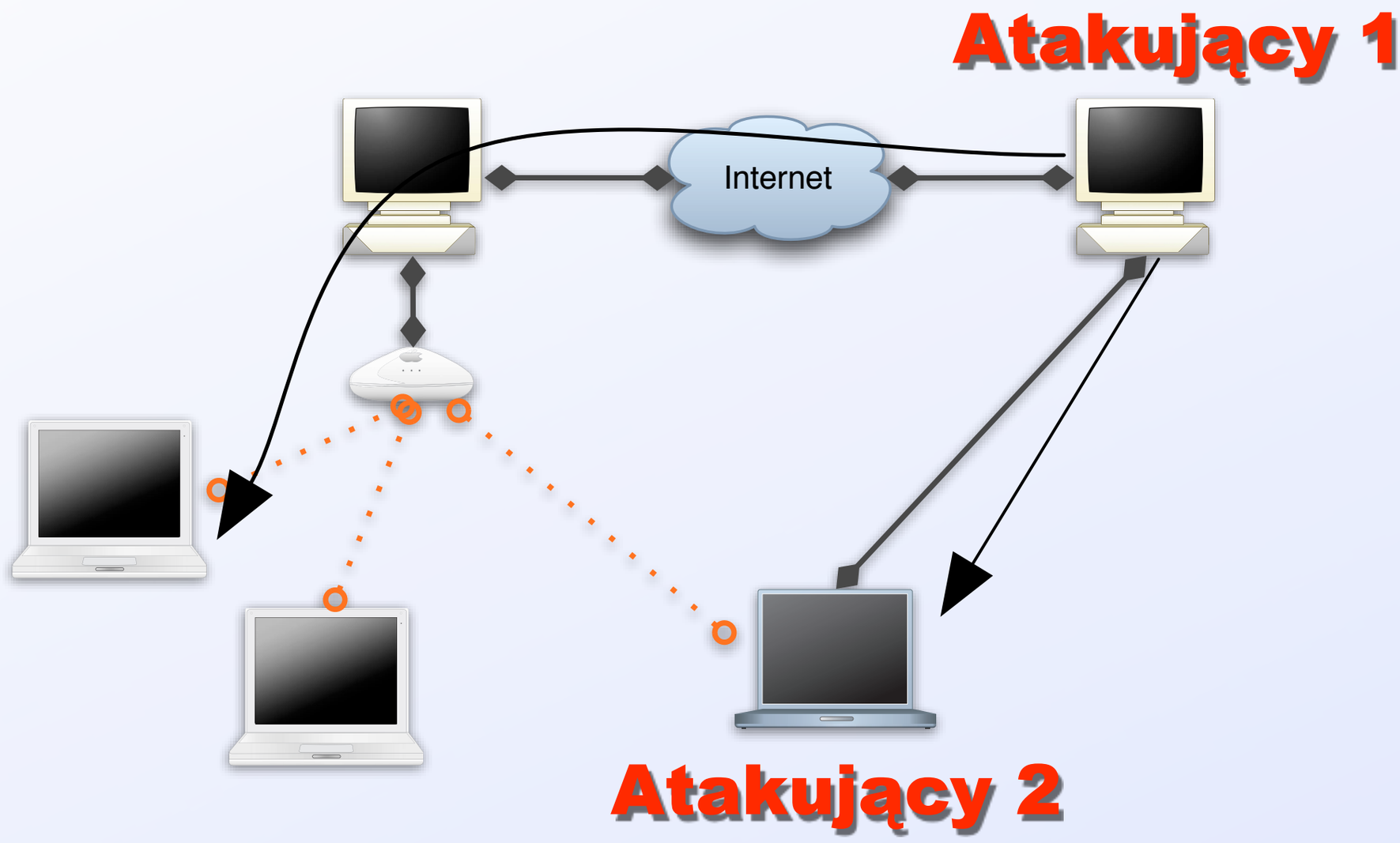
Pasywny atak na WEP

- Wymaga zdobycia średnio rzędu **kilku milionów** pakietów (co odpowiada zaledwie **parunastu minutom** nasłuchiwania obciążonego AP)
- Często klucz można odkryć znacznie wcześniej jeśli jest on jednym ze **słabych kluczy**, które inicjują zbyt prostą permutację początkową
- Złożoność algorytmu odtwarzania klucza jest **liniowa** ze względu na jego długość, zatem zwiększanie długości klucza nie wpływa jakościowo na bezpieczeństwo

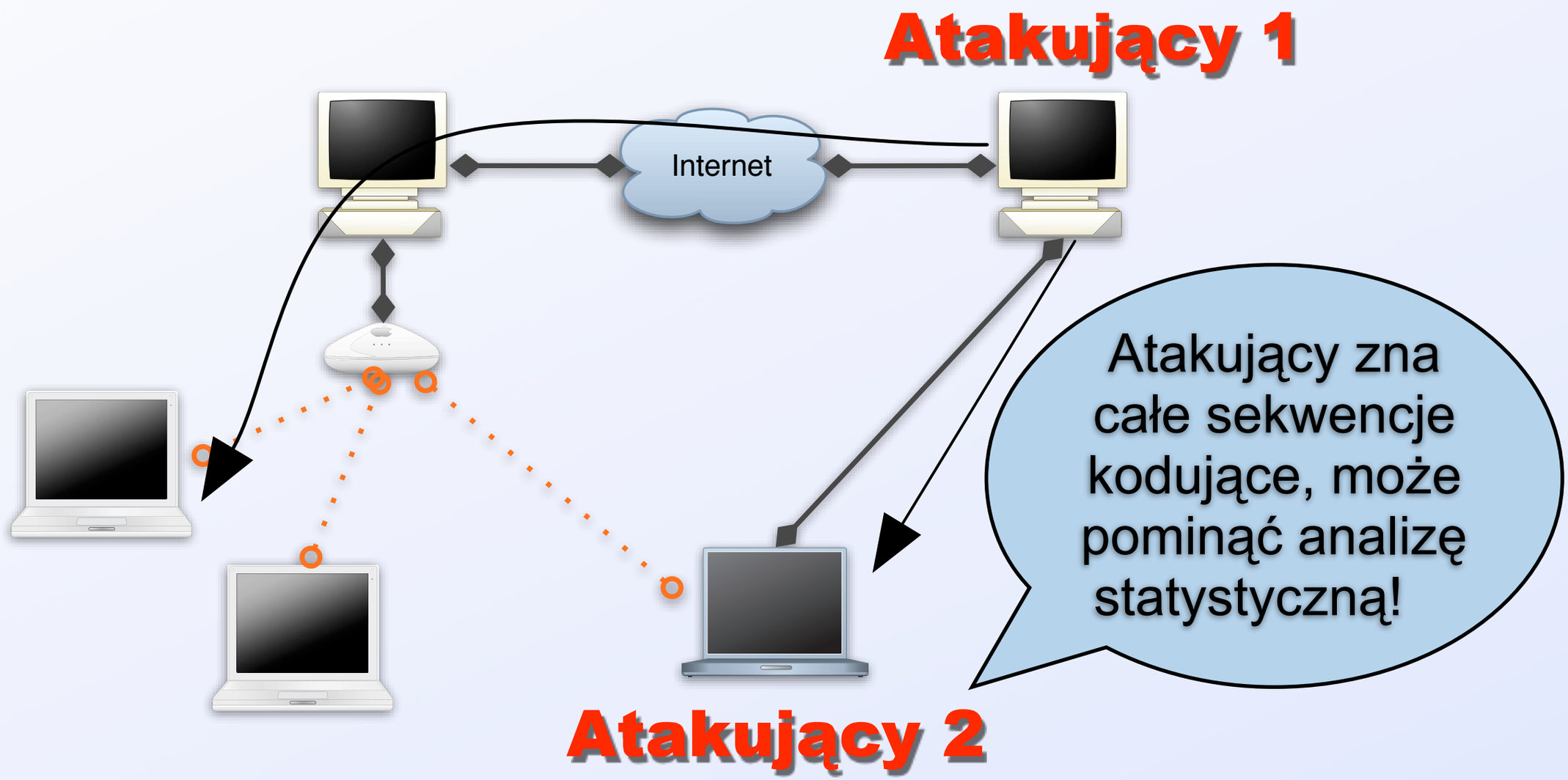
Aktywny atak na WEP



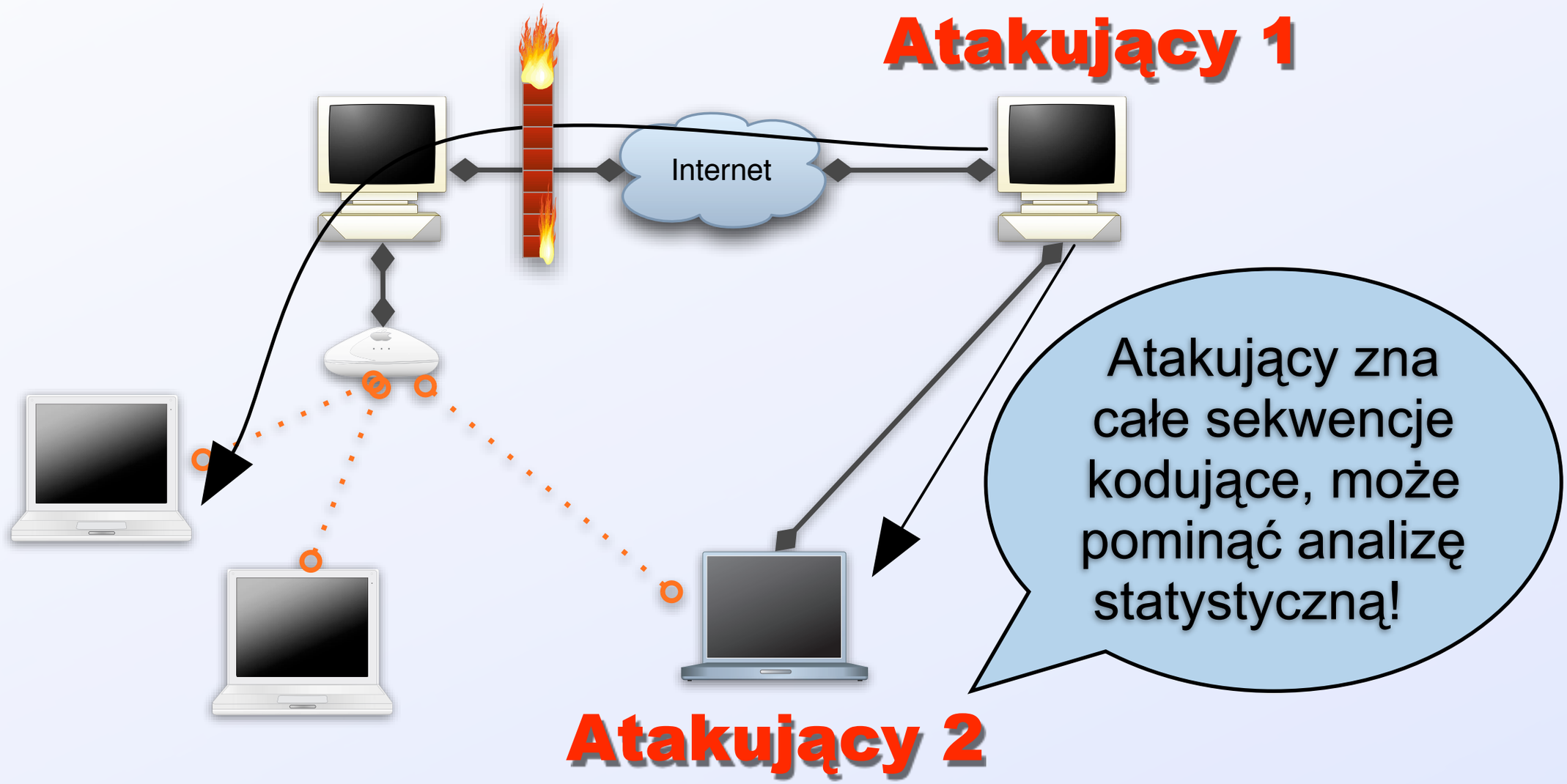
Aktywny atak na WEP



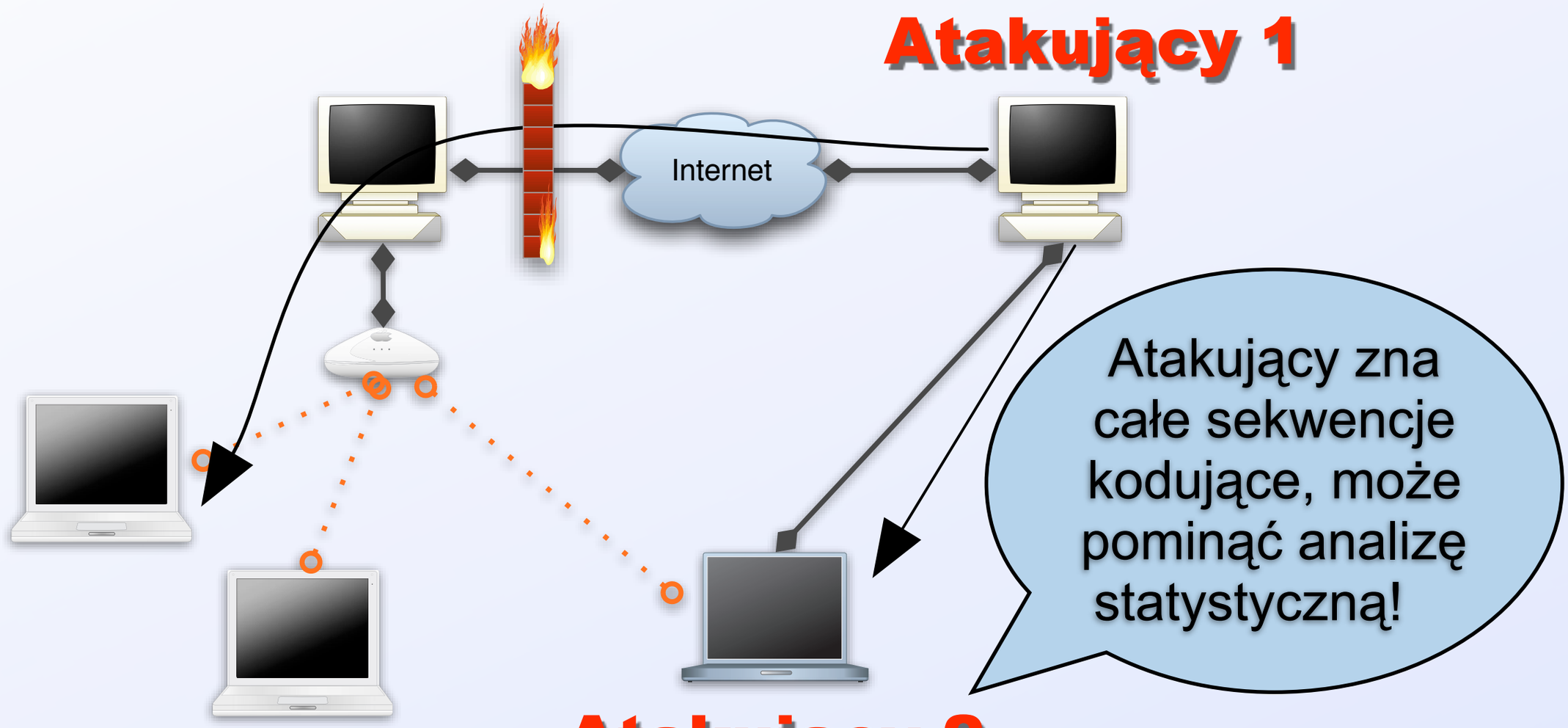
Aktywny atak na WEP



Aktywny atak na WEP



Aktywny atak na WEP



Sieci radiowe muszą być za firewallem!!!

Atak na WEP

I jeszcze jeden sposób ataku...

Atak na WEP

I jeszcze jeden sposób ataku...

Słownikowy ...

Atak na WEP

I jeszcze jeden sposób ataku...

Słownikowy ...

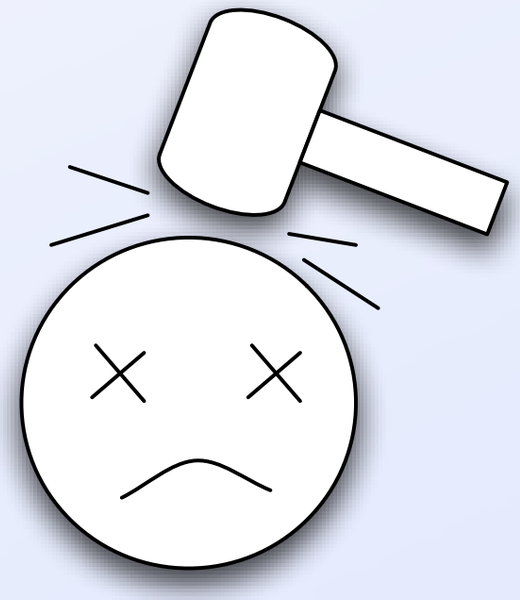
Zaskakująco często klucz WEP=SSID,
lub proste i krótkie słowo ...

Atak na WEP

I jeszcze jeden sposób ataku...

Słownikowy ...

Zaskakująco często klucz WEP=SSID,
lub proste i krótkie słowo ...



Praktyka?

Praktyka?

Praktyka?

Praktyka?

Jeśli zobaczysz na chodniku przed swoją firmą znak) (znaczy, że jest źle!

IEEE 802.1X - EAPol

- Bezpieczna sieć musi mieć mechanizm uwierzytelniania użytkownika

- Użytkownik powinien móc zweryfikować autentyczność sieci

- Cały proces musi przebiec w sposób bezpieczny w kanale który może być podsłuchiwany

- Autentykacja powinna przebiec w jak najniższej warstwie modelu OSI, szyfrowanie musi być szybkie

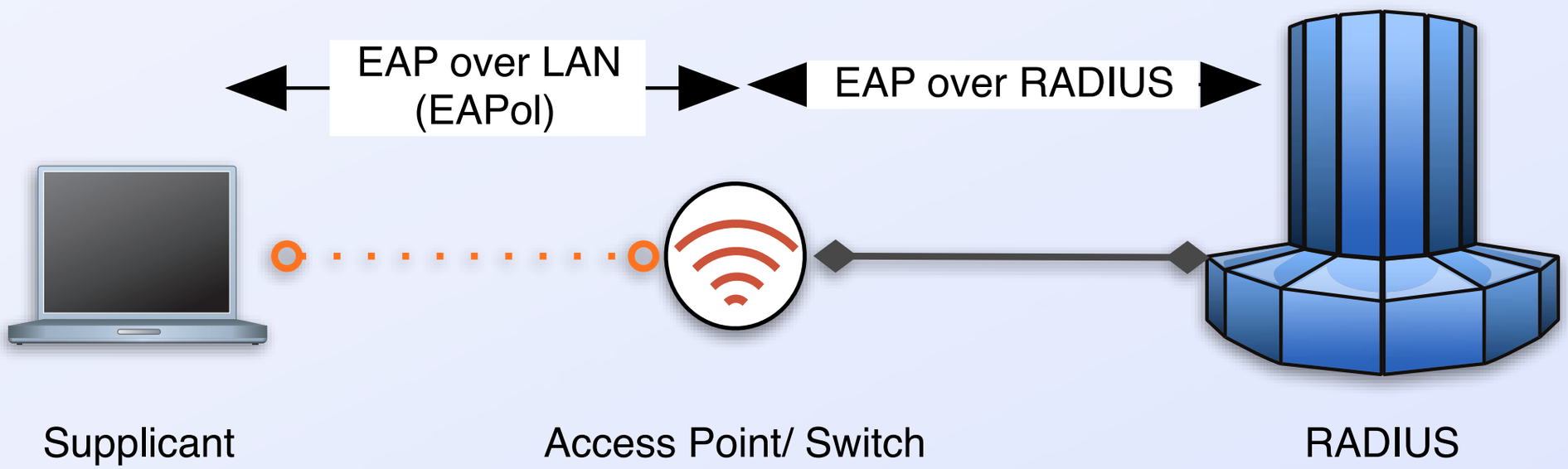
IEEE 802.1X - EAPol

- Bezpieczna sieć musi mieć mechanizm uwierzytelniania użytkownika

- Użytkownik powinien móc zweryfikować autentyczność sieci

- Cały proces musi przebiec w sposób bezpieczny w kanale który może być podsłuchiwany

- Autentykacja powinna przebiec w jak najniższej warstwie modelu OSI, szyfrowanie musi być szybkie

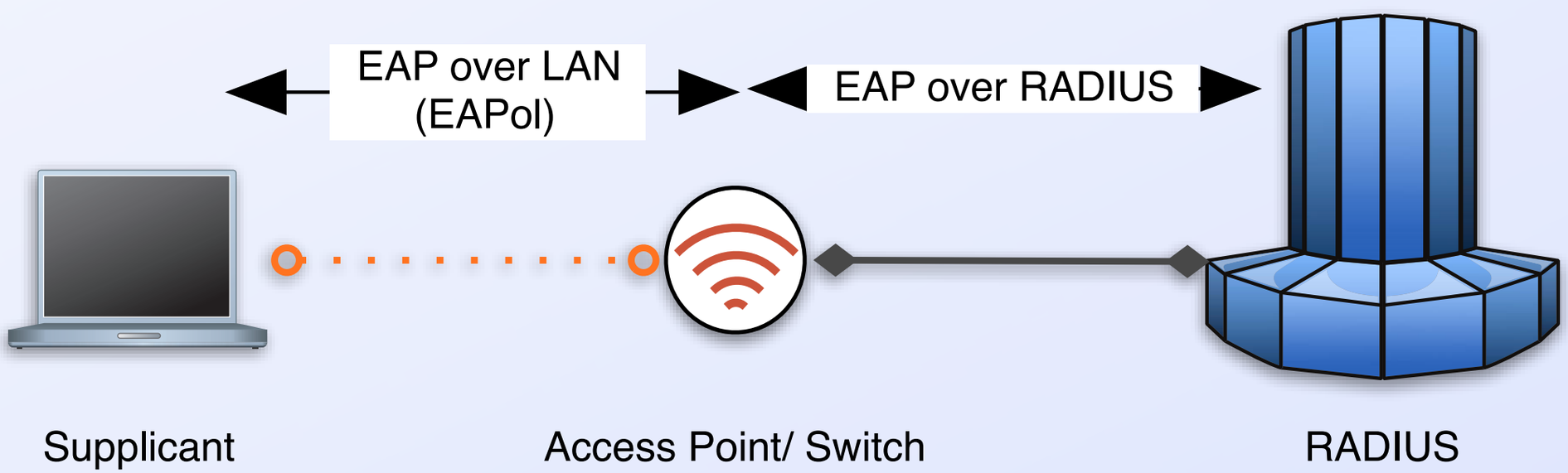


IEEE 802.1X - EAPol

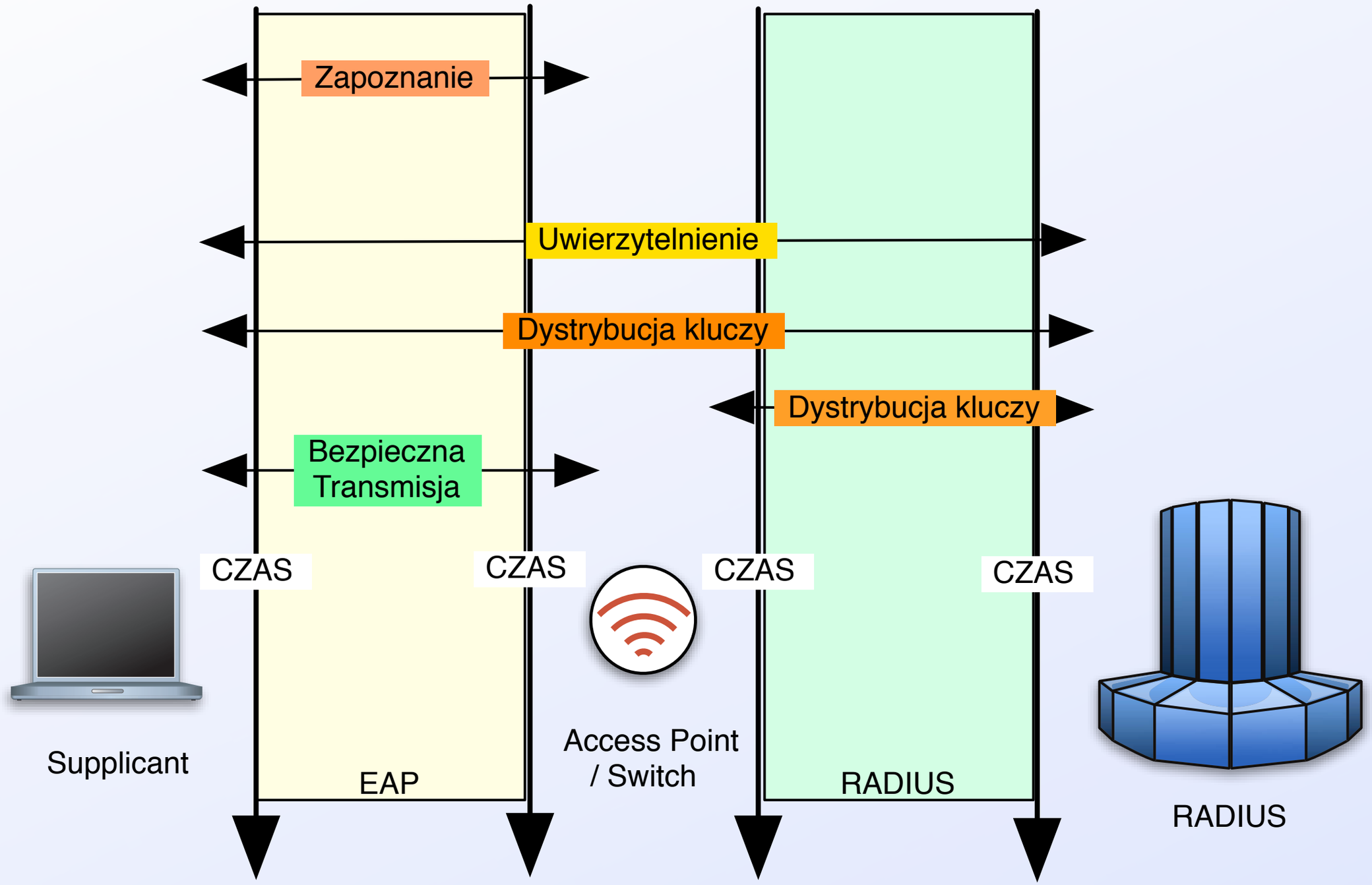
EAP - Extensible Authentication Protocol - protokół transportowy na potrzeby uwierzytelniania

EAP nie jest konkretnym protokołem uwierzytelniania ale raczej ogólnym schematem w którym, mogą być implementowane na różne sposoby np: EAP-SIM, EAP-TLS, EAP-TTLS, EAP-MD5

EAPol - EAP over LAN



IEEE 802.1X schemat



Dynamiczny WEP

- EAP-TLS lub EAP-TTLS pozwala na bezpieczne uwierzytelnienie i przesłanie do klienta oraz do AP materiału kryptograficznego (klucza)
- AP co pewien krótki czas (parę minut) generuje nowy klucz WEP i przesyła go do klienta szyfrując starym
- Mechanizm taki w oparciu o WEP nosi nazwę “dynamiczny WEP”
- Czy to rozwiązuje problemy?

Dynamiczny WEP

- Częsta zmiana klucza praktycznie uniemożliwia analizę statystyczną. Kolizje IV zdarzają się zbyt rzadko...

Dynamiczny WEP

- Częsta zmiana klucza praktycznie uniemożliwia analizę statystyczną. Kolizje IV zdarzają się zbyt rzadko...
- Ale system pozostaje podatny na atak aktywny!

Dynamiczny WEP

- Częsta zmiana klucza praktycznie uniemożliwia analizę statystyczną. Kolizje IV zdarzają się zbyt rzadko...
- Ale system pozostaje podatny na atak aktywny!
- Tym niemniej atakujący praktycznie nie ma szans poznać zawartości transmisji przed kolejną zmianą klucza...

Dynamiczny WEP

- Częsta zmiana klucza praktycznie uniemożliwia analizę statystyczną. Kolizje IV zdarzają się zbyt rzadko...
- Ale system pozostaje podatny na atak aktywny!
- Tym niemniej atakujący praktycznie nie ma szans poznać zawartości transmisji przed kolejną zmianą klucza...
- Ale nadal możliwe są zamiany bitów uzupełniające CRC32 (fałszowanie pakietów) !!

Dynamiczny WEP

- Częsta zmiana klucza praktycznie uniemożliwia analizę statystyczną. Kolizje IV zdarzają się zbyt rzadko...
- Ale system pozostaje podatny na atak aktywny!
- Tym niemniej atakujący praktycznie nie ma szans poznać zawartości transmisji przed kolejną zmianą klucza...
- Ale nadal możliwe są zamiany bitów uzupełniające CRC32 (fałszowanie pakietów) !!
- W praktyce zamiany bitów są trudne do wykonania technicznie a bez znajomości treści transmisji dość bezużyteczne...

Dynamiczny WEP

- Częsta zmiana klucza praktycznie uniemożliwia analizę statystyczną. Kolizje IV zdarzają się zbyt rzadko...
- Ale system pozostaje podatny na atak aktywny!
- Tym niemniej atakujący praktycznie nie ma szans poznać zawartości transmisji przed kolejną zmianą klucza...
- Ale nadal możliwe są zamiany bitów uzupełniające CRC32 (fałszowanie pakietów) !!
- W praktyce zamiany bitów są trudne do wykonania technicznie a bez znajomości treści transmisji dość bezużyteczne...
- Ale rejestrując transmisję i realizując atak aktywny można poznać treść transmisji post-factum !!!

Dynamiczny WEP

- Częsta zmiana klucza praktycznie uniemożliwia analizę statystyczną. Kolizje IV zdarzają się zbyt rzadko...
- Ale system pozostaje podatny na atak aktywny!
- Tym niemniej atakujący praktycznie nie ma szans poznać zawartości transmisji przed kolejną zmianą klucza...
- Ale nadal możliwe są zamiany bitów uzupełniające CRC32 (fałszowanie pakietów) !!
- W praktyce zamiany bitów są trudne do wykonania technicznie a bez znajomości treści transmisji dość bezużyteczne...
- Ale rejestrując transmisję i realizując atak aktywny można poznać treść transmisji post-factum !!!
- Ale atak aktywny jest łatwo wykrywalny (zatem ryzykowny)... Przez krótki okres między zamianami klucza trzeba przepchnąć sporo danych...

Dynamiczny WEP

- Częsta zmiana klucza praktycznie uniemożliwia analizę statystyczną. Kolizje IV zdarzają się zbyt rzadko...
- A
- T ości
  t
- A
  (
- W bez
  z
- A ć
  t
- Ale dla aktywny jest łatwe wykrywany (zatem fizycznym...) trzeba przepchnąć sporo danych...

Dynamiczny WEP na dzień dzisiejszy zapewnia rozsądny poziom bezpieczeństwa dla znacznej większości normalnych zastosowań. Należy jednak uważać ten mechanizm za **“przejściowy”**.

Mechanizm ten jest **zdecydowanie niewystarczający** dla systemów w których bezpieczeństwo jest czynnikiem krytycznym.

krótki okres między zamianami klucza trzeba przepchnąć sporo danych...

WPA

- **WPA - Wi Fi Protected Access** - część standardu 802.11i wprowadzona (listopad 2003) jako odpowiedź na wykryte ułomności systemu WEP, do czasu opracowania pełnej specyfikacji 802.11i.

WPA

- **WPA - Wi Fi Protected Access** - część standardu 802.11i wprowadzona (listopad 2003) jako odpowiedź na wykryte ułomności systemu WEP, do czasu opracowania pełnej specyfikacji 802.11i.

- WPA to zespół mechanizmów zwiększających bezpieczeństwo sieci, bez potrzeby nagłej wymiany całego sprzętu.

WPA

- **WPA - Wi Fi Protected Access** - część standardu 802.11i wprowadzona (listopad 2003) jako odpowiedź na wykryte ułomności systemu WEP, do czasu opracowania pełnej specyfikacji 802.11i.

- WPA to zespół mechanizmów zwiększających bezpieczeństwo sieci, bez potrzeby nagłej wymiany całego sprzętu.

- Standard IEEE 802.11i został ratyfikowany w czerwcu 2004 roku, dzisiaj implementacje tego standardu spotyka się pod nazwą WPA2.

WPA - szczegóły

WPA

WPA - szczegóły

WPA

WPA Personal

WPA Enterprise

WPA - szczegóły

WPA

WPA Personal

WPA -PSK

Pre Shared Key

WPA Enterprise

WPA - szczegóły

WPA

WPA Personal

WPA -PSK

Pre Shared Key

Zastosowanie w domach i małych firmach, mniejsze bezpieczeństwo

WPA Enterprise

WPA - szczegóły

WPA

WPA Personal

WPA -PSK
Pre Shared Key

Zastosowanie w domach i małych firmach, mniejsze bezpieczeństwo

WPA Enterprise

RADIUS + EAP

WPA - szczegóły

WPA

WPA Personal

WPA -PSK
Pre Shared Key

Zastosowanie w domach i małych firmach, mniejsze bezpieczeństwo

WPA Enterprise

RADIUS + EAP

Dystrybucja kluczy

WPA - szczegóły

WPA

WPA Personal

WPA -PSK
Pre Shared Key

Zastosowanie w domach i małych firmach, mniejsze bezpieczeństwo

WPA Enterprise

RADIUS + EAP

Dystrybucja kluczy

Zastosowanie tam gdzie dostępna jest infrastruktura RADIUS

Usprawnienia w WPA

- **TKIP - Temporal Key Integrity Protocol -** protokół dynamicznego zarządzania kluczami w oparciu o mechanizmy WEP (algorytm RC4)
- **AES - Advanced Encryption Standard -** blokowy algorytm szyfrowania oparty na algorytmie Rijndael
- **CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol -** mechanizm dostępny w WPA2, oparty o AES pozwalający jednocześnie stwierdzić integralność wiadomości

TKIP

- Temporal Key Integrity Protocol

TKIP

- Temporal Key Integrity Protocol
- Podstawowa metoda szyfrowania informacji w WPA, wypierana obecnie przez AES i CCMP (WPA2)

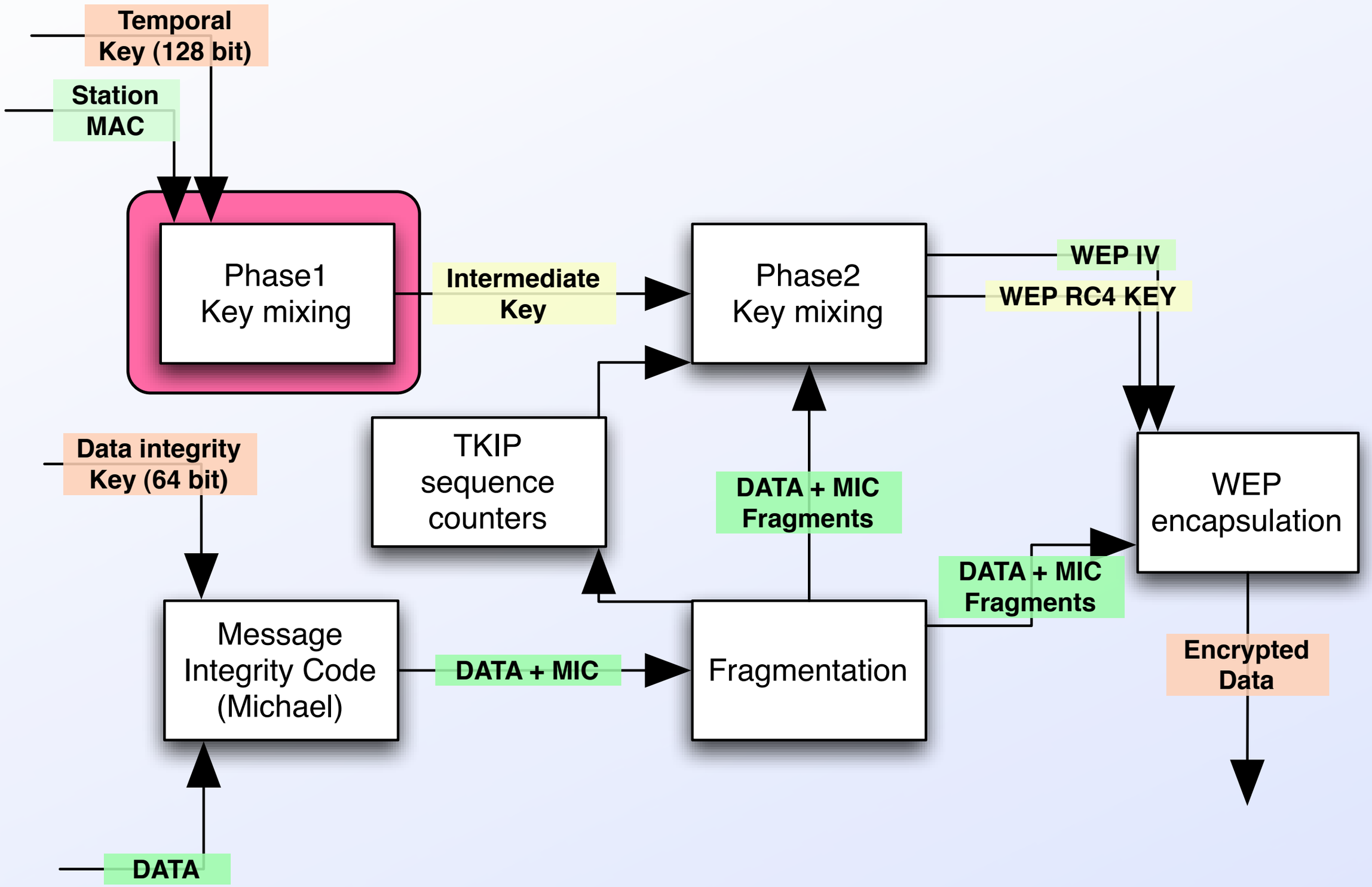
TKIP

- Temporal Key Integrity Protocol
- Podstawowa metoda szyfrowania informacji w WPA, wypierana obecnie przez AES i CCMP (WPA2)
- Zaprojektowany tak aby był szybki, dzięki temu może być wspierany na istniejącym sprzęcie

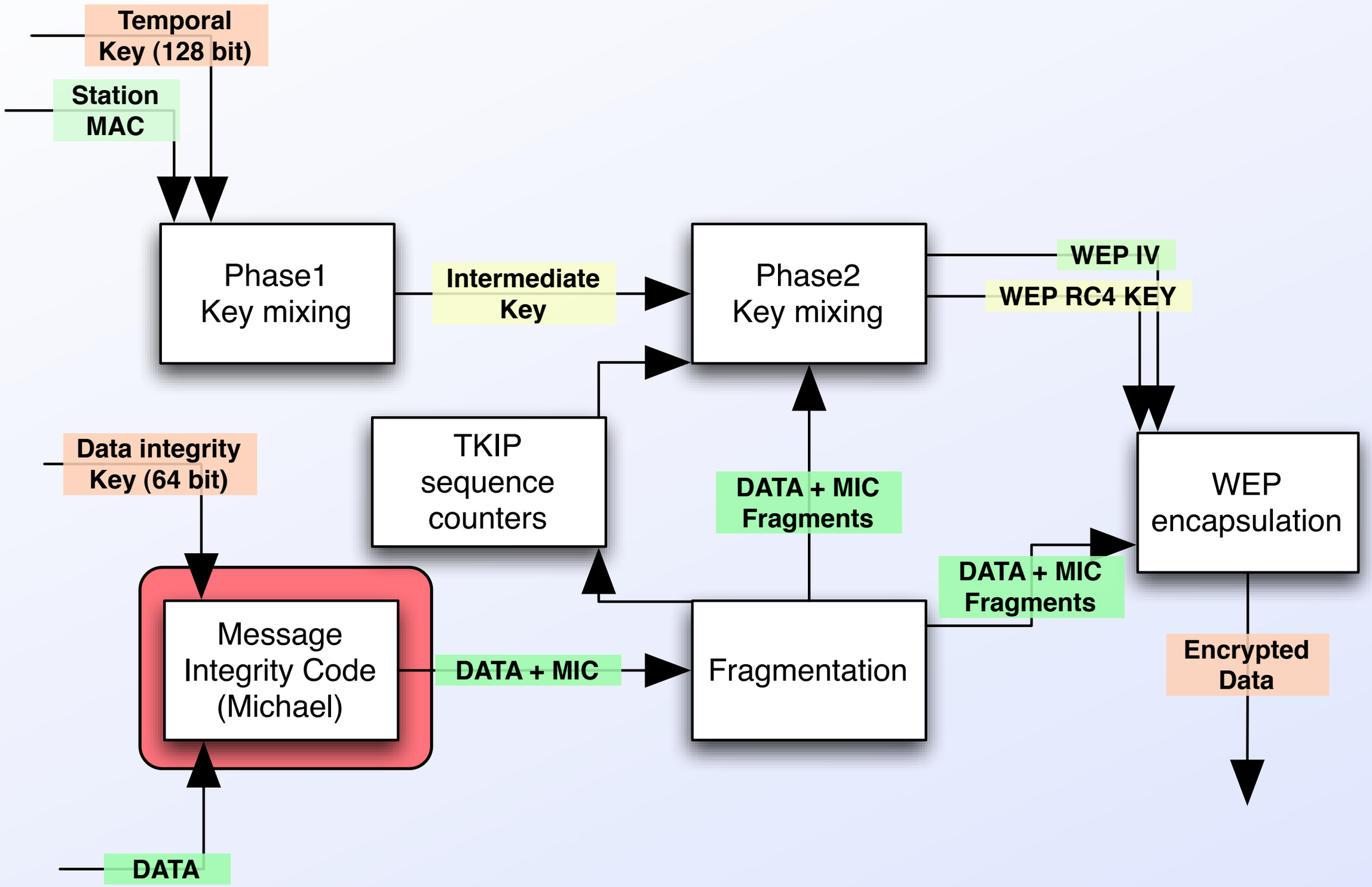
TKIP

- Temporal Key Integrity Protocol
- Podstawowa metoda szyfrowania informacji w WPA, wypierana obecnie przez AES i CCMP (WPA2)
- Zaprojektowany tak aby był szybki, dzięki temu może być wspierany na istniejącym sprzęcie
- Wykorzystuje WEP, starając się jednocześnie załatać jego słabości

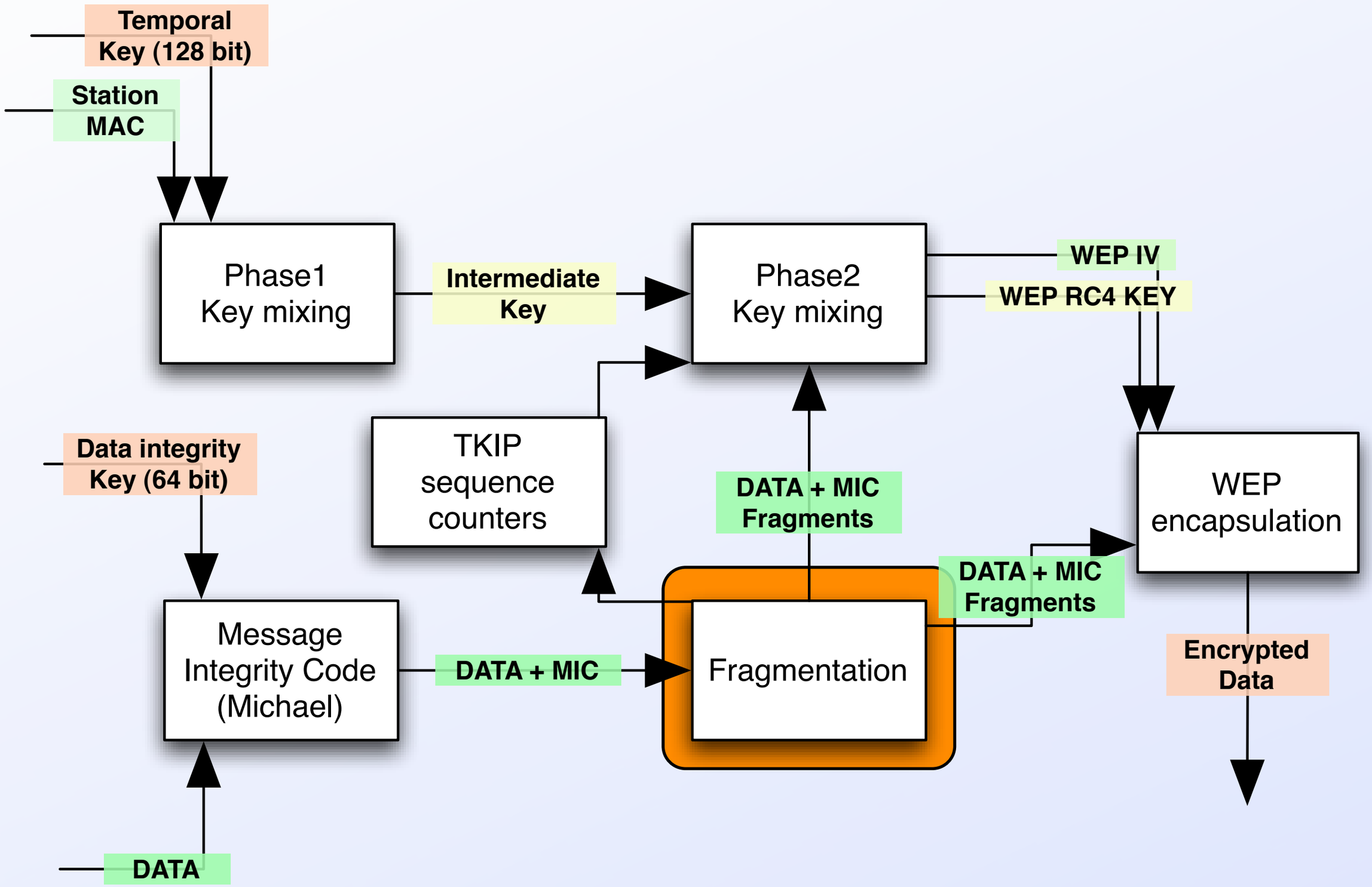
TKIP - Szyfrowanie



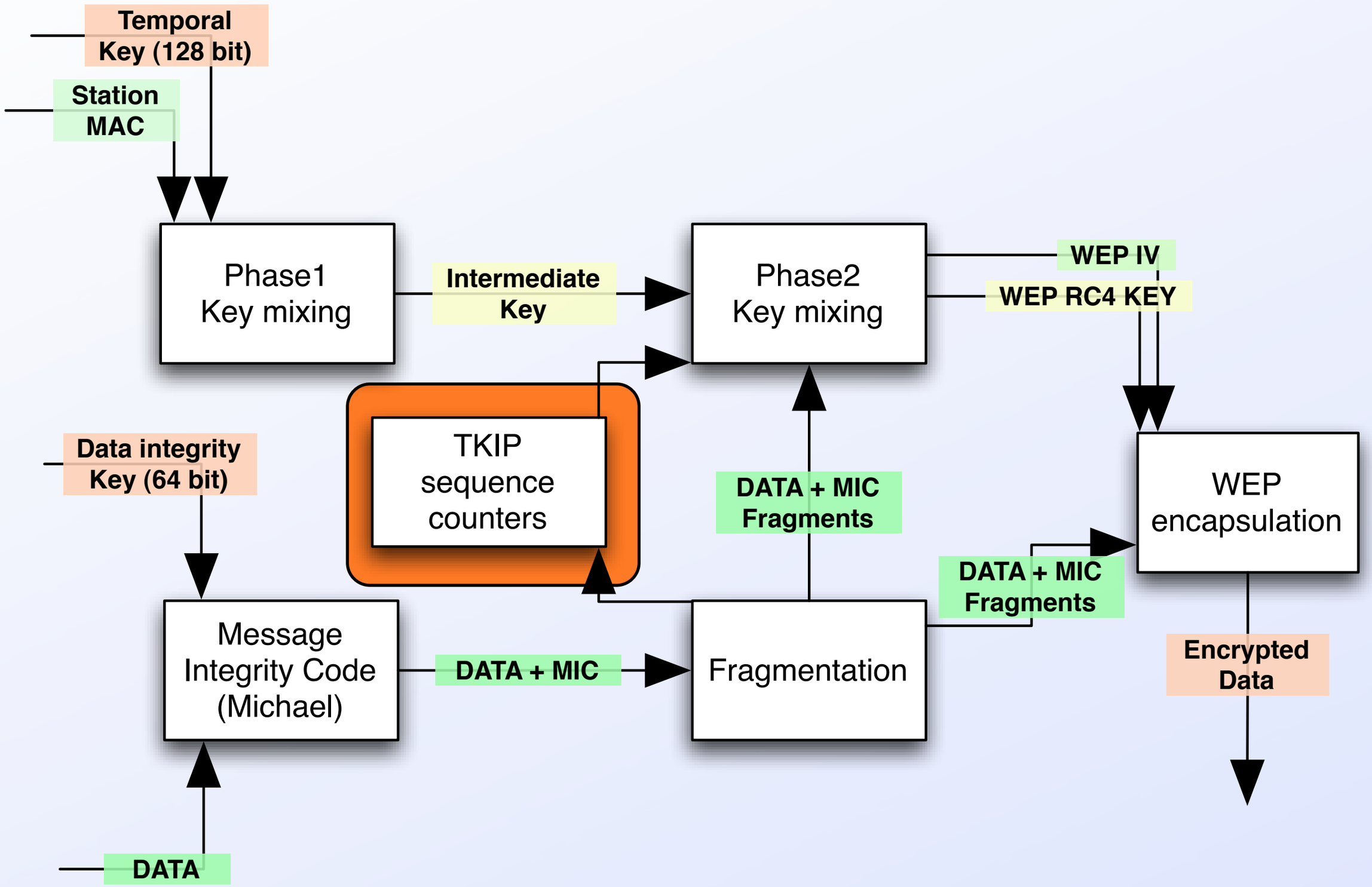
TKIP - Szyfrowanie



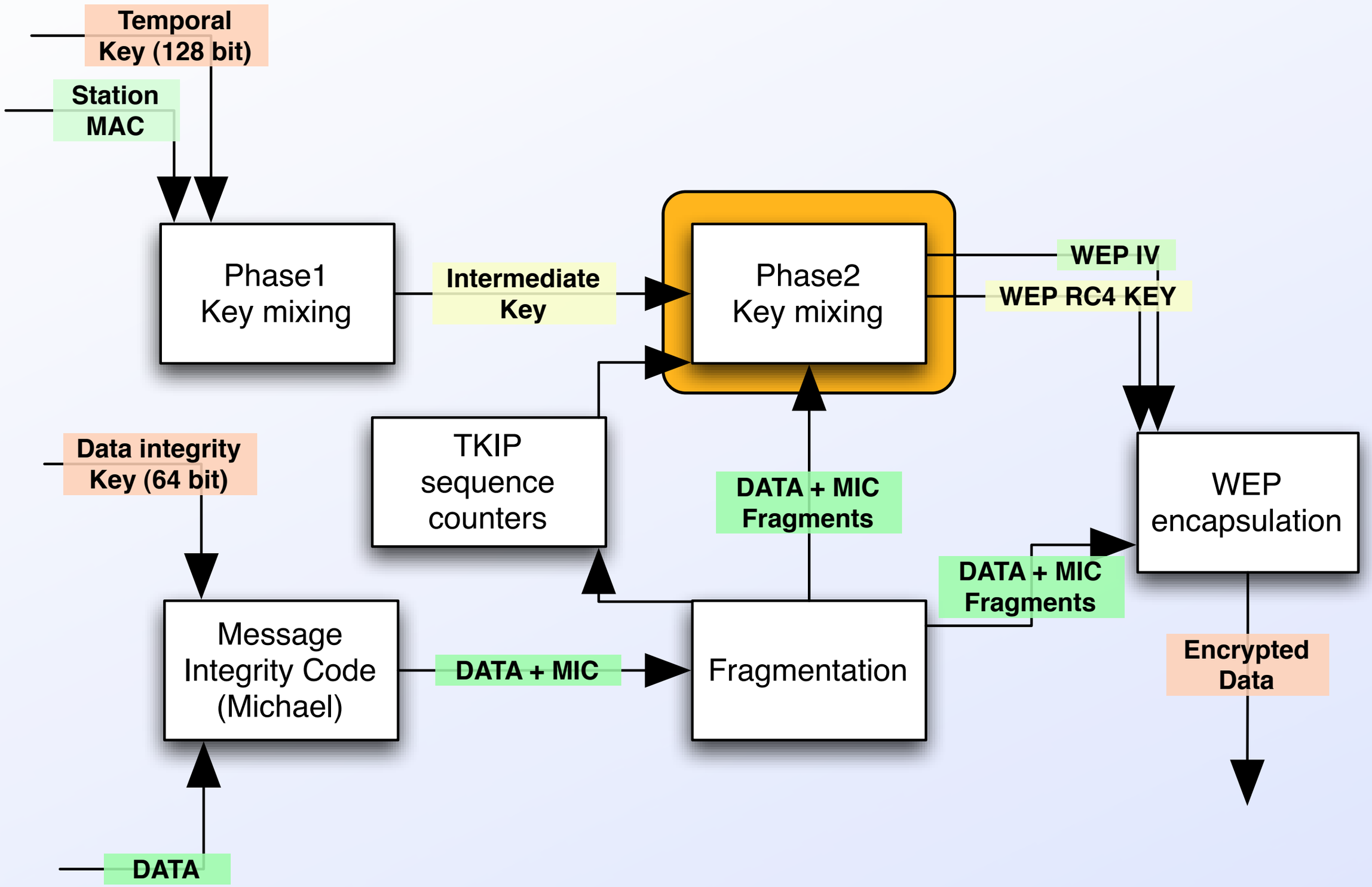
TKIP - Szyfrowanie



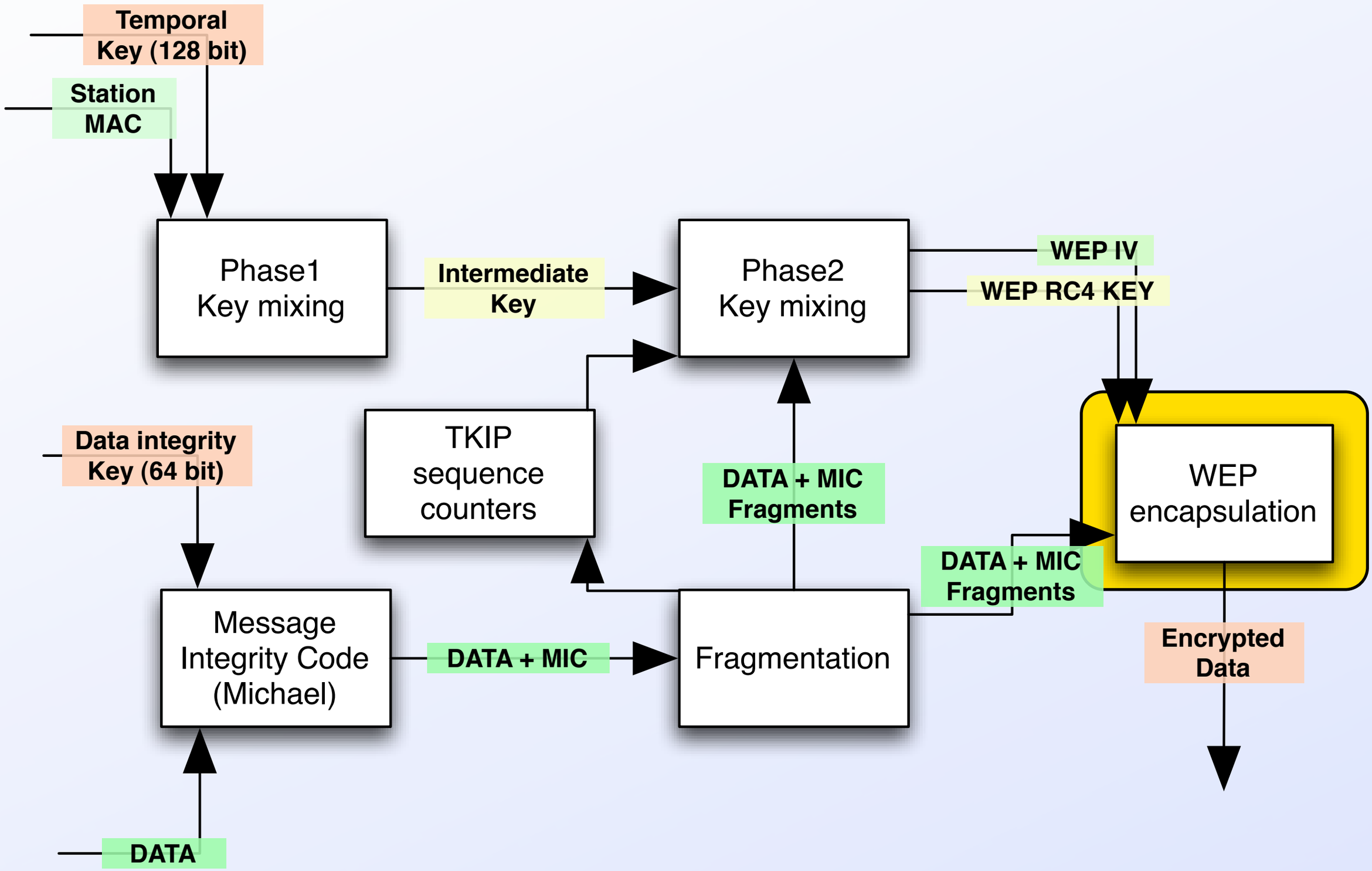
TKIP - Szyfrowanie



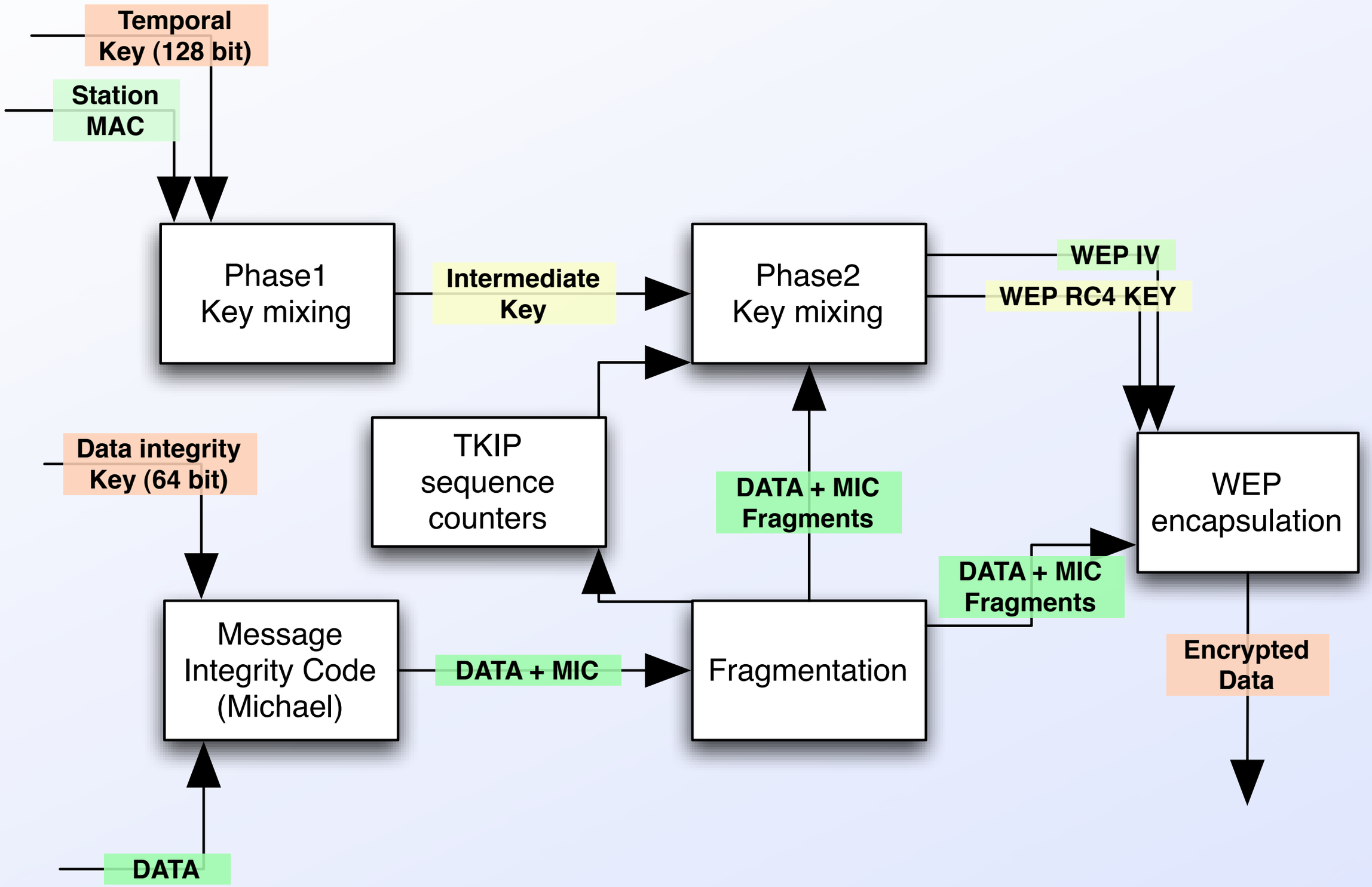
TKIP - Szyfrowanie



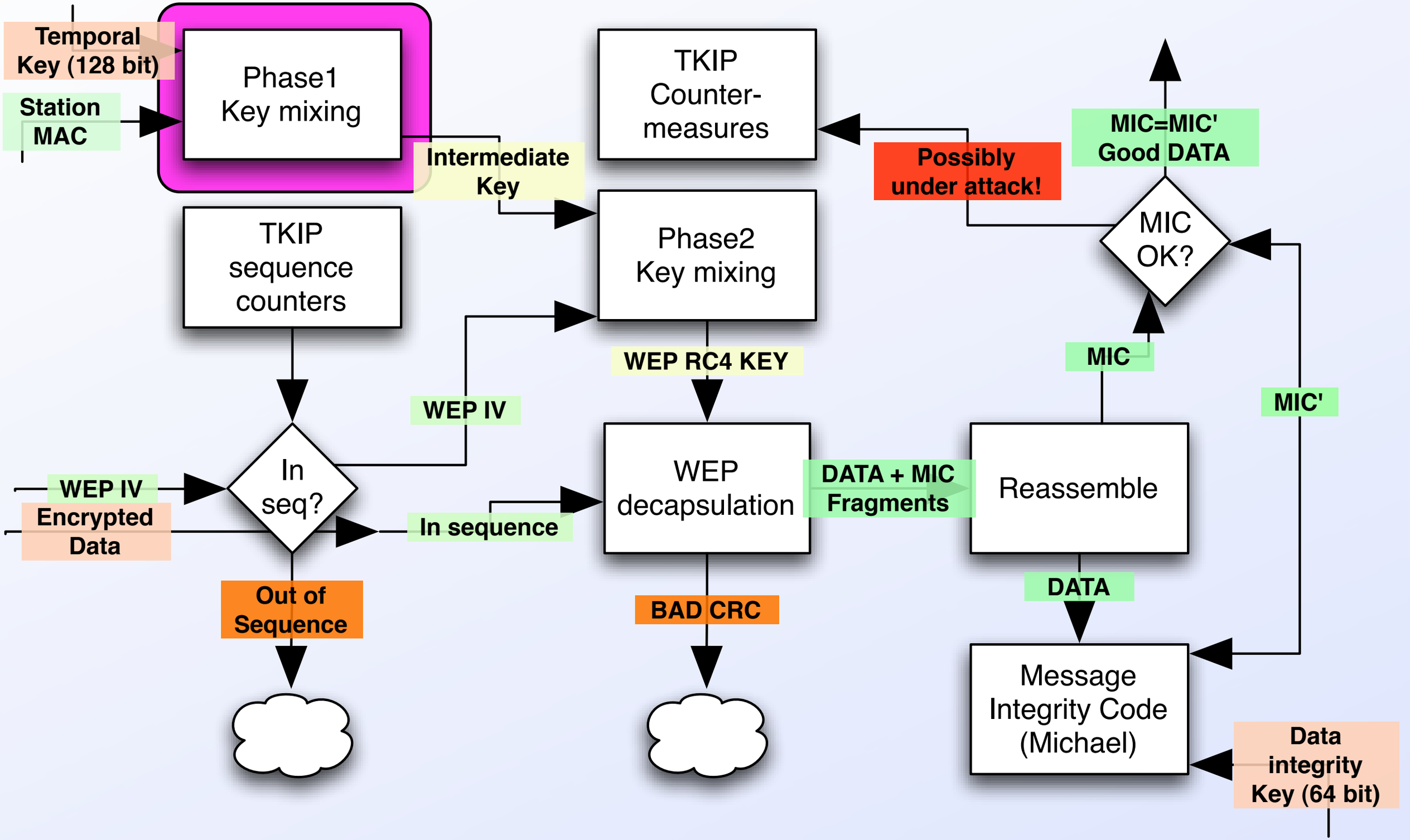
TKIP - Szyfrowanie



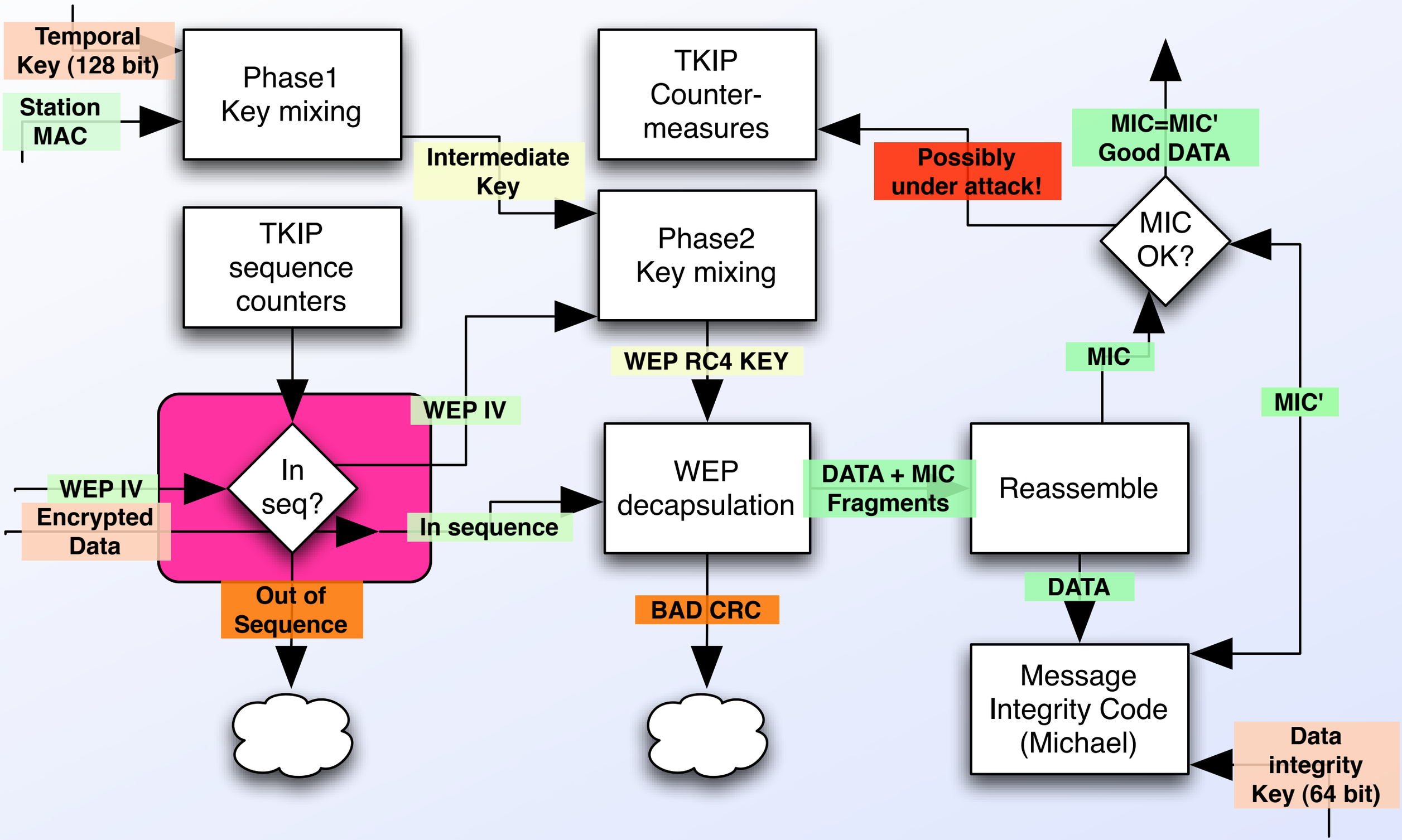
TKIP - Szyfrowanie



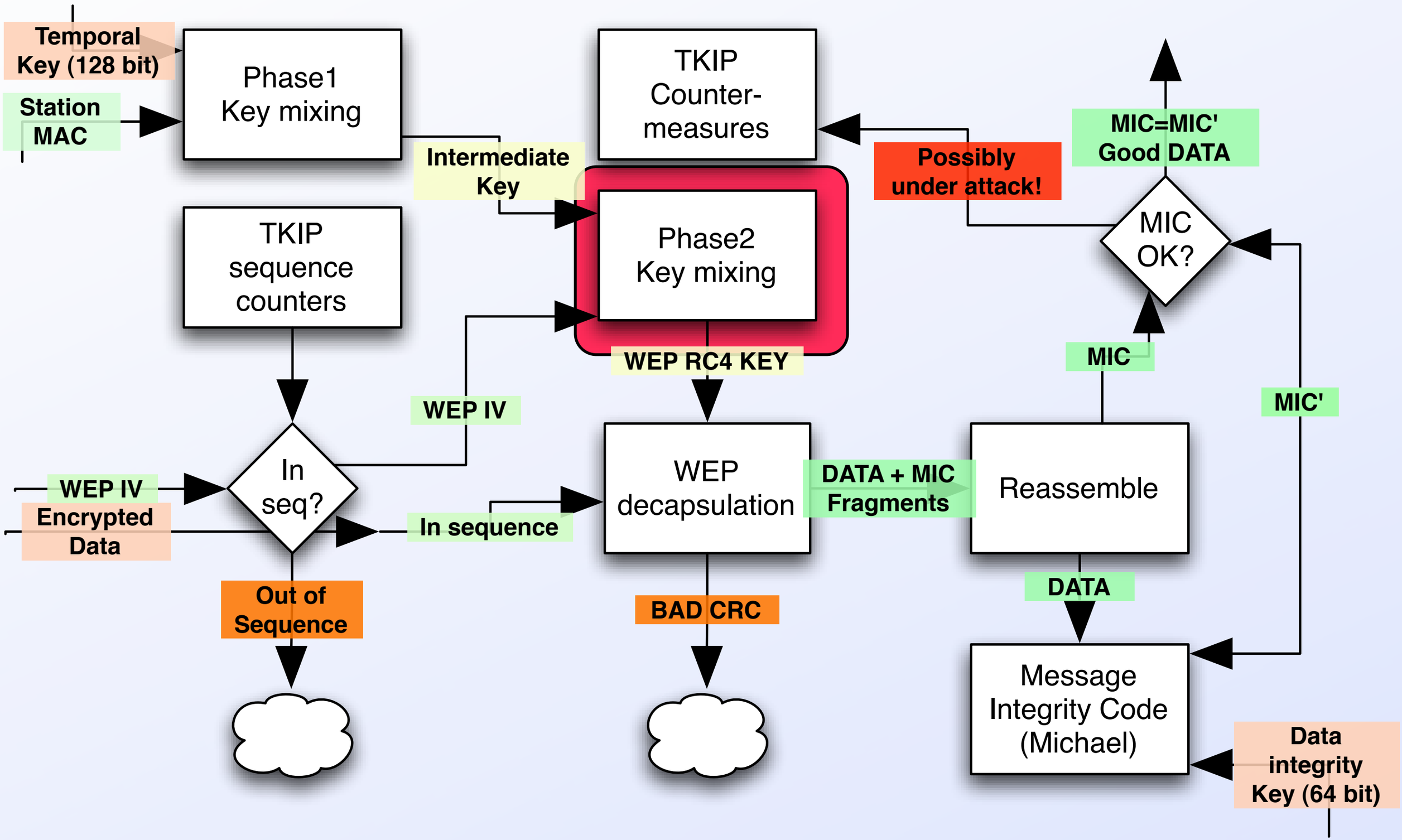
TKIP - deszyfrowanie



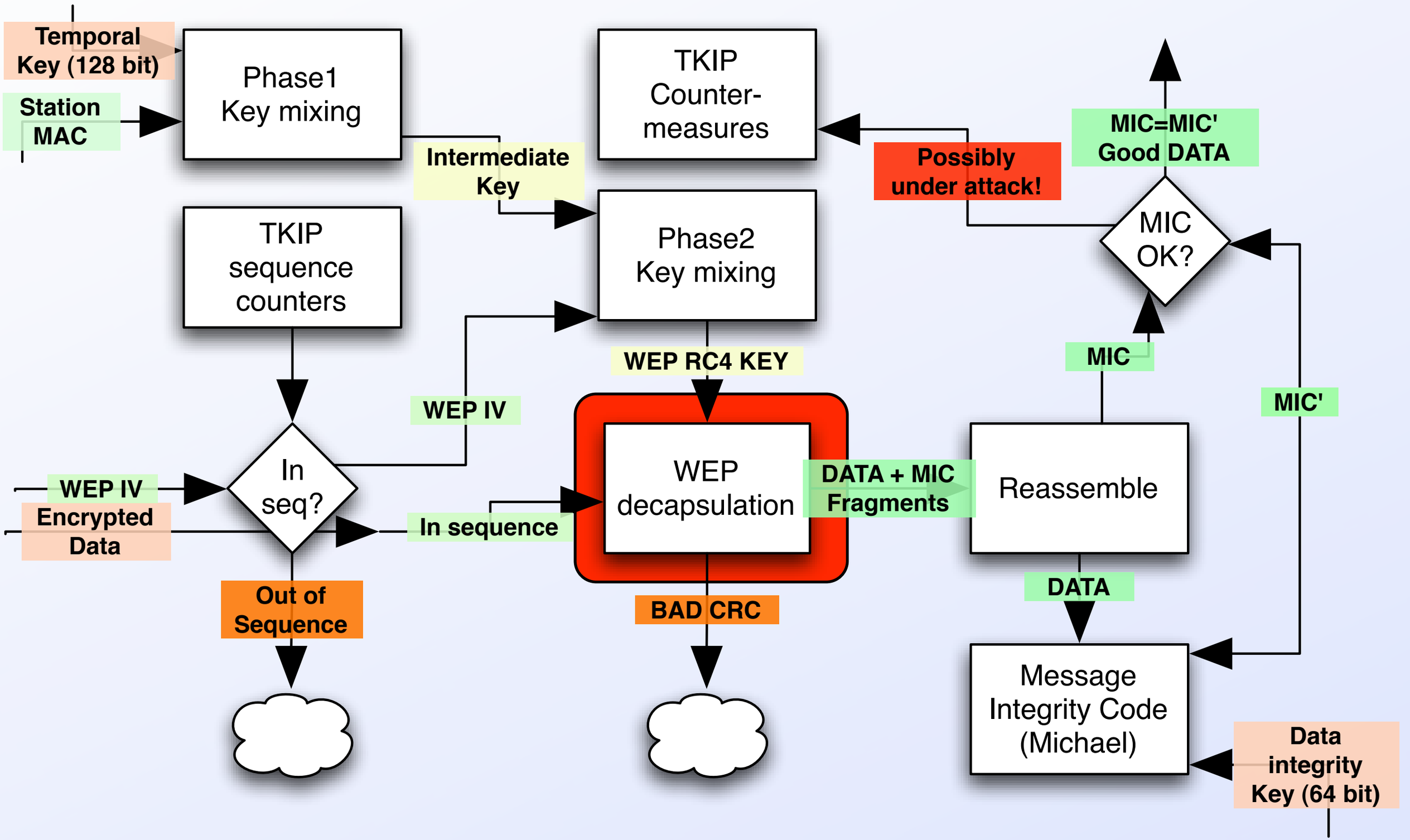
TKIP - deszyfrowanie



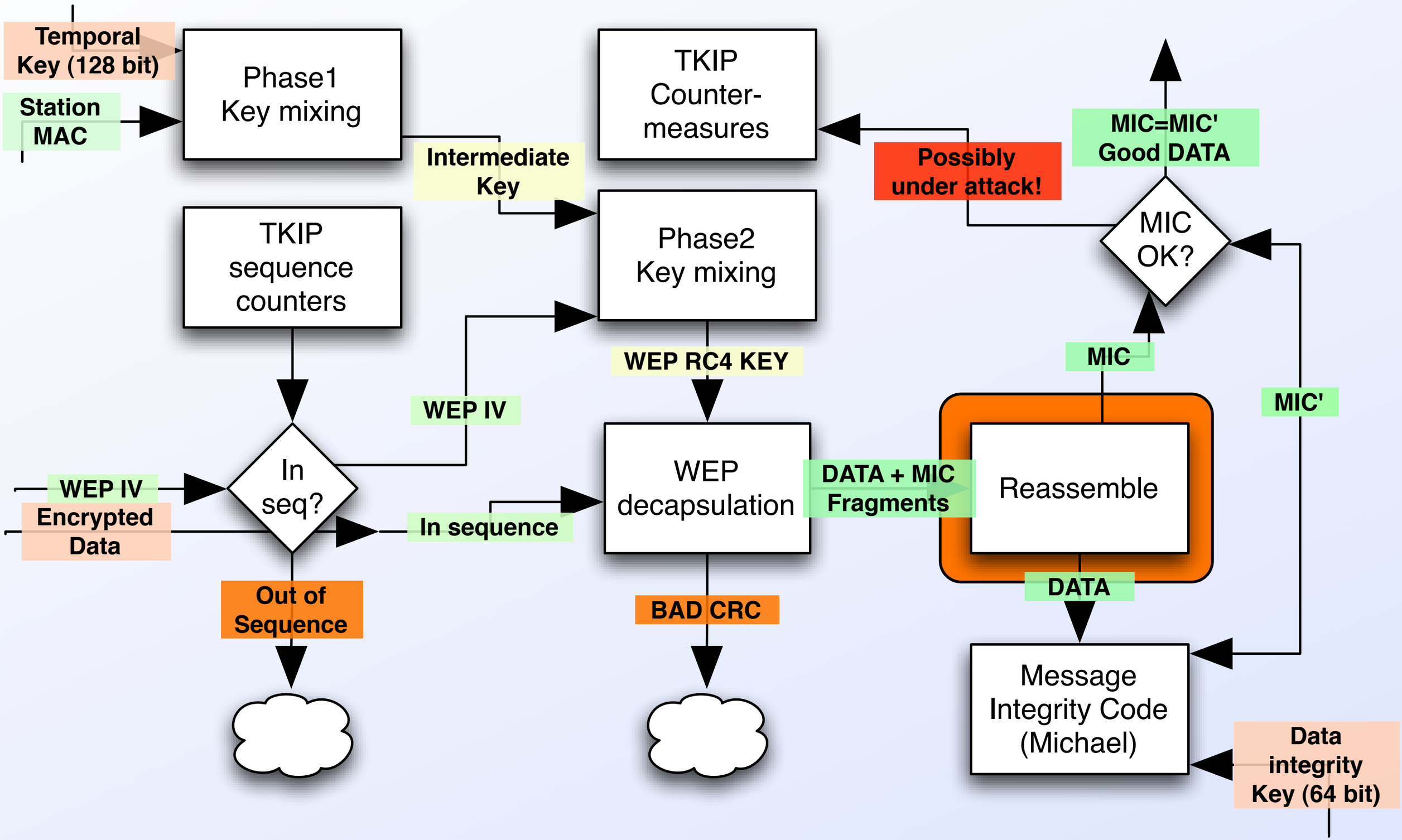
TKIP - deszyfrowanie



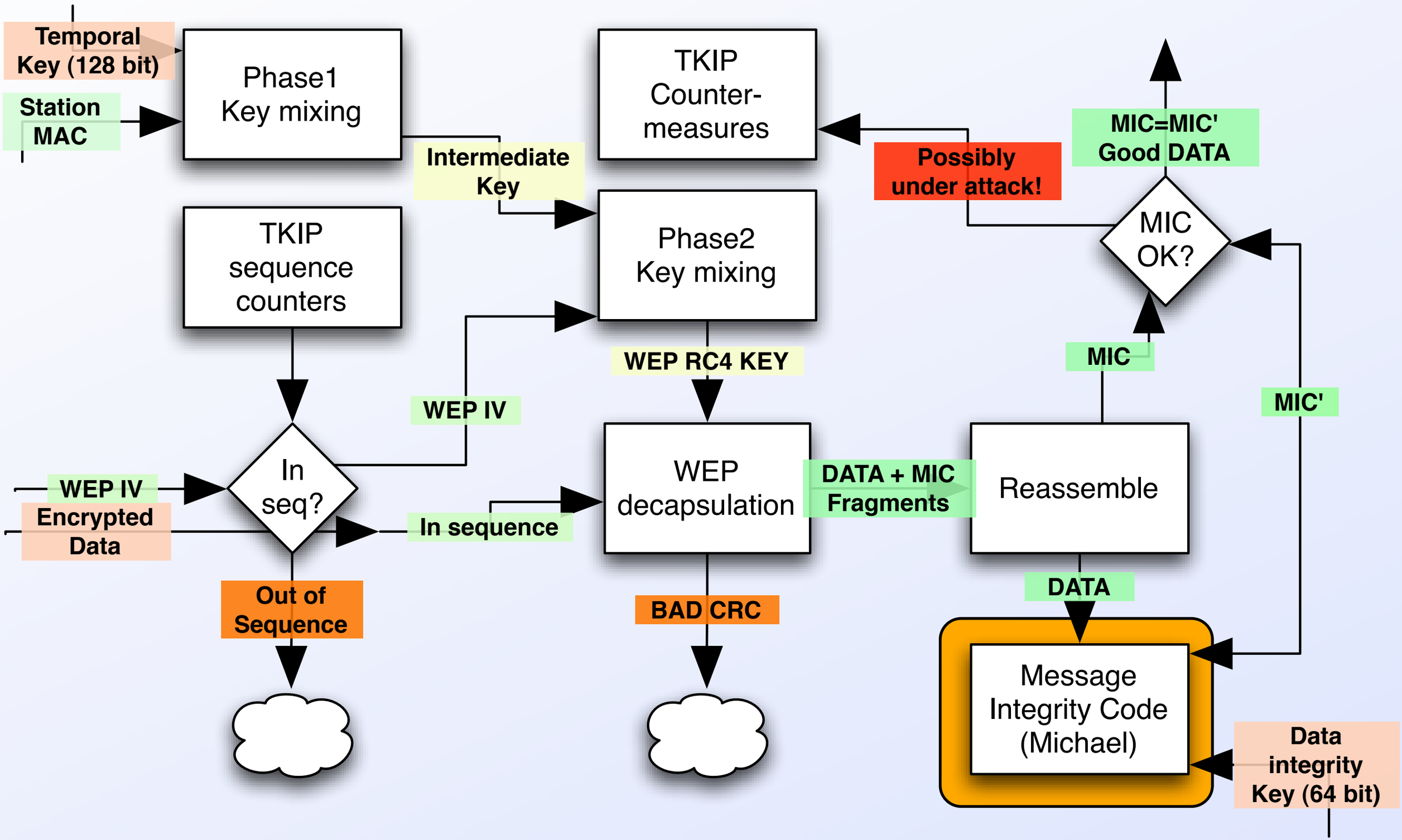
TKIP - deszyfrowanie



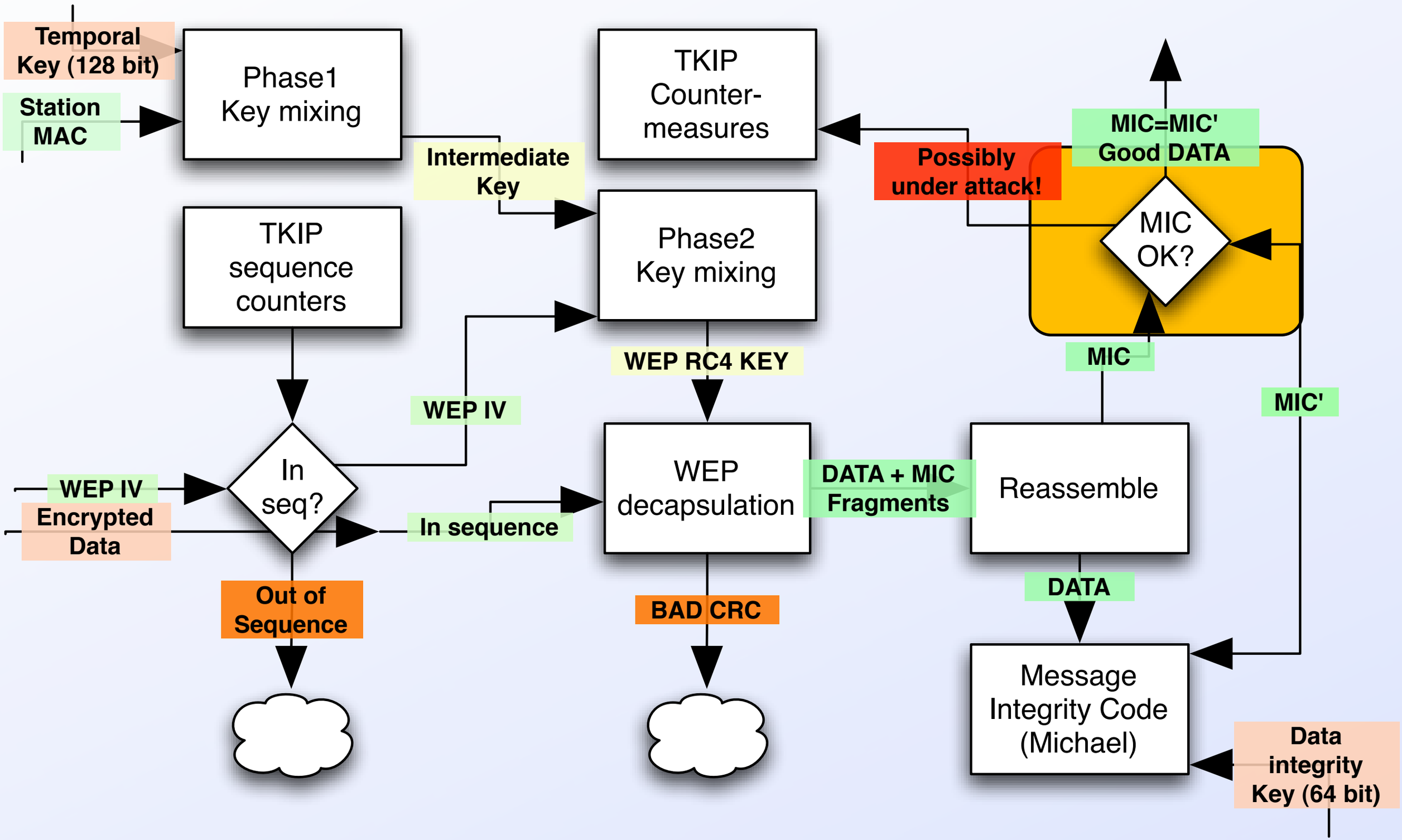
TKIP - deszyfrowanie



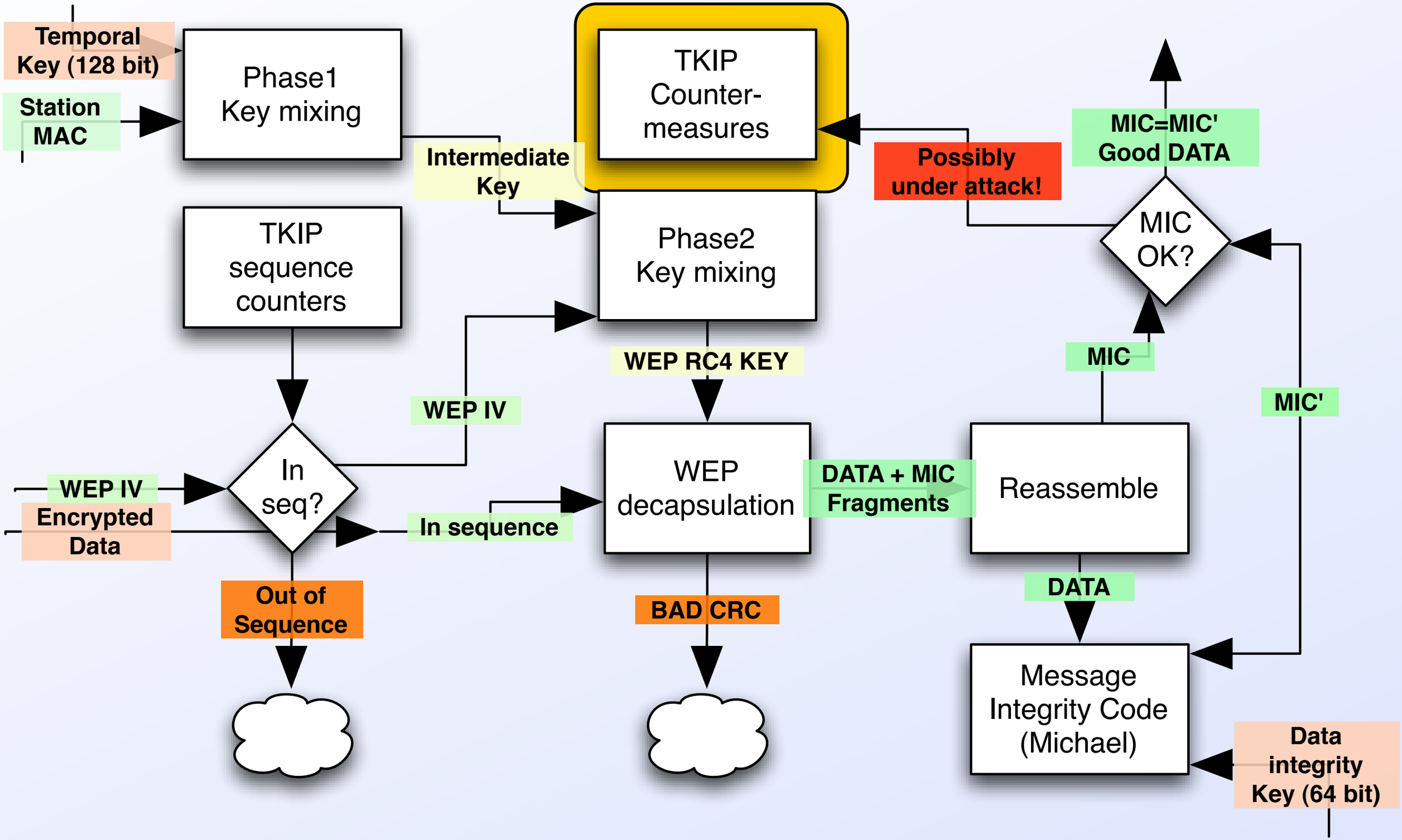
TKIP - deszyfrowanie



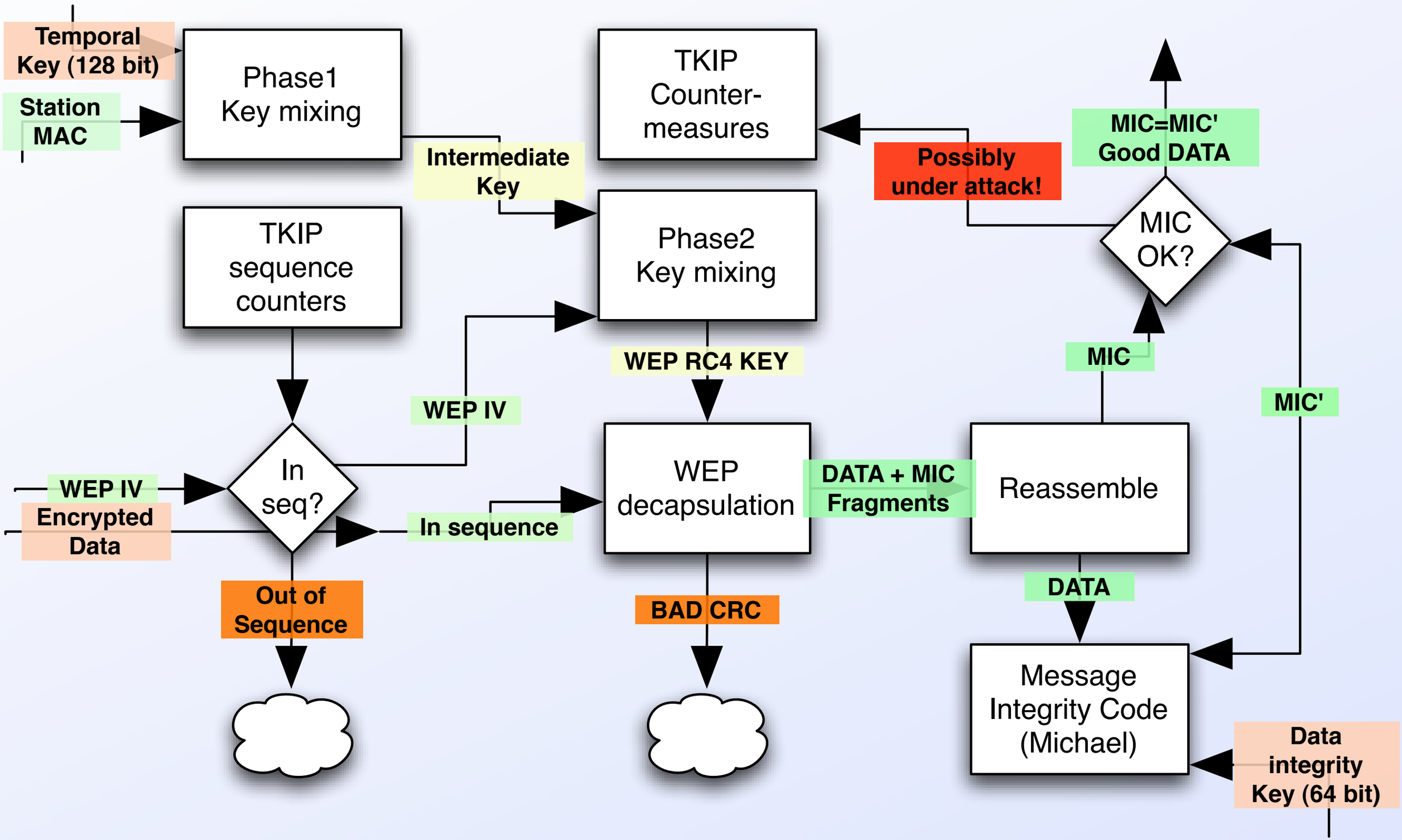
TKIP - deszyfrowanie



TKIP - deszyfrowanie



TKIP - deszyfrowanie



Cechy TKIP

- Do każdej transmisji używane są **4 klucze**, po dwa dla każdego kierunku

Cechy TKIP

- Do każdej transmisji używane są **4 klucze**, po dwa dla każdego kierunku
- Klucze temporalne są **zmieniane** co ściśle określoną ilość pakietów

Cechy TKIP

- Do każdej transmisji używane są **4 klucze**, po dwa dla każdego kierunku
- Klucze temporalne są **zmieniane** co ściśle określoną ilość pakietów
- TKIP **wykrywa potencjalne ataki**, gdy ilość błędów MIC przekroczy pewien próg następuje minutowa deasocjacja

Cechy TKIP

- Do każdej transmisji używane są **4 klucze**, po dwa dla każdego kierunku
- Klucze temporalne są **zmieniane** co ściśle określoną ilość pakietów
- TKIP **wykrywa potencjalne ataki**, gdy ilość błędów MIC przekroczy pewien próg następuje minutowa deasocjacja
- Mechanizm miksujący (2 faza) **dekoreluje** klucz RC4 z wektorem inicjalizującym (który jednocześnie numeruje pakiet)

AES

- AES - Advanced Encryption Standard - wersja algorytmu Rijndael
- Skonstruowany przez dwóch belgijskich kryptologów (Joan Daemen, Vincent Rijmen), został uznany przez rząd USA jako standardowy algorytm szyfrowania używany w administracji
- AES wykorzystuje operacje na macierzy 8 x 8 bajtów, nad ciałem Galois $GF(2^8)$ wielomianów nad ciałem $\mathbb{Z}_2$ modulo wielomian $x^8 + x^4 + x^3 + x + 1$

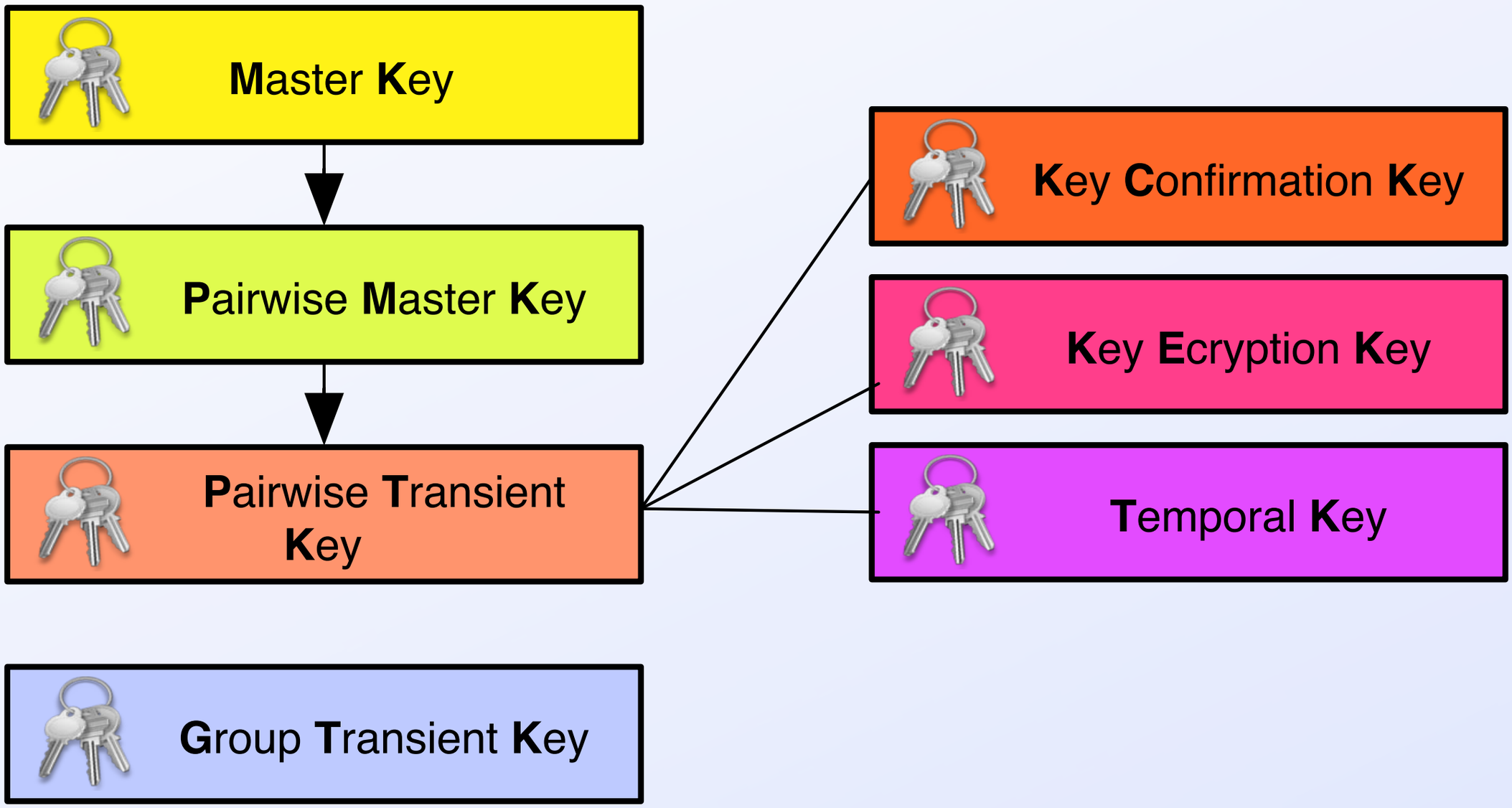
Cechy AES

- Jest znacznie bardziej skomplikowany niż RC4
- Wygląda na znacznie bezpieczniejszy (najlepsze znane ataki na AES są praktycznie niemożliwe do zrealizowania przy obecnych środkach)
- Wymaga znacznie większej mocy obliczeniowej AP i karty (wymiana sprzętu)

802.11i

- Porządny system autoryzacji/szyfrowania transmisji
- Poprawione zarządzanie kluczami
- Obligatoryjne stosowanie mechanizmów szyfrowania TKIP/AES/CCMP
- 802.11i nareszcie spełnia oczekiwania w sprawie bezpieczeństwa sieci bezprzewodowych !

802.11i - klucze



802.11i - klucze

Reprezentuje udane uwierzytelnienie, posiada go klient i serwer uwierzytelniający

Master **K**ey

Pairwise **M**aster **K**ey

Pairwise **T**ransient **K**ey

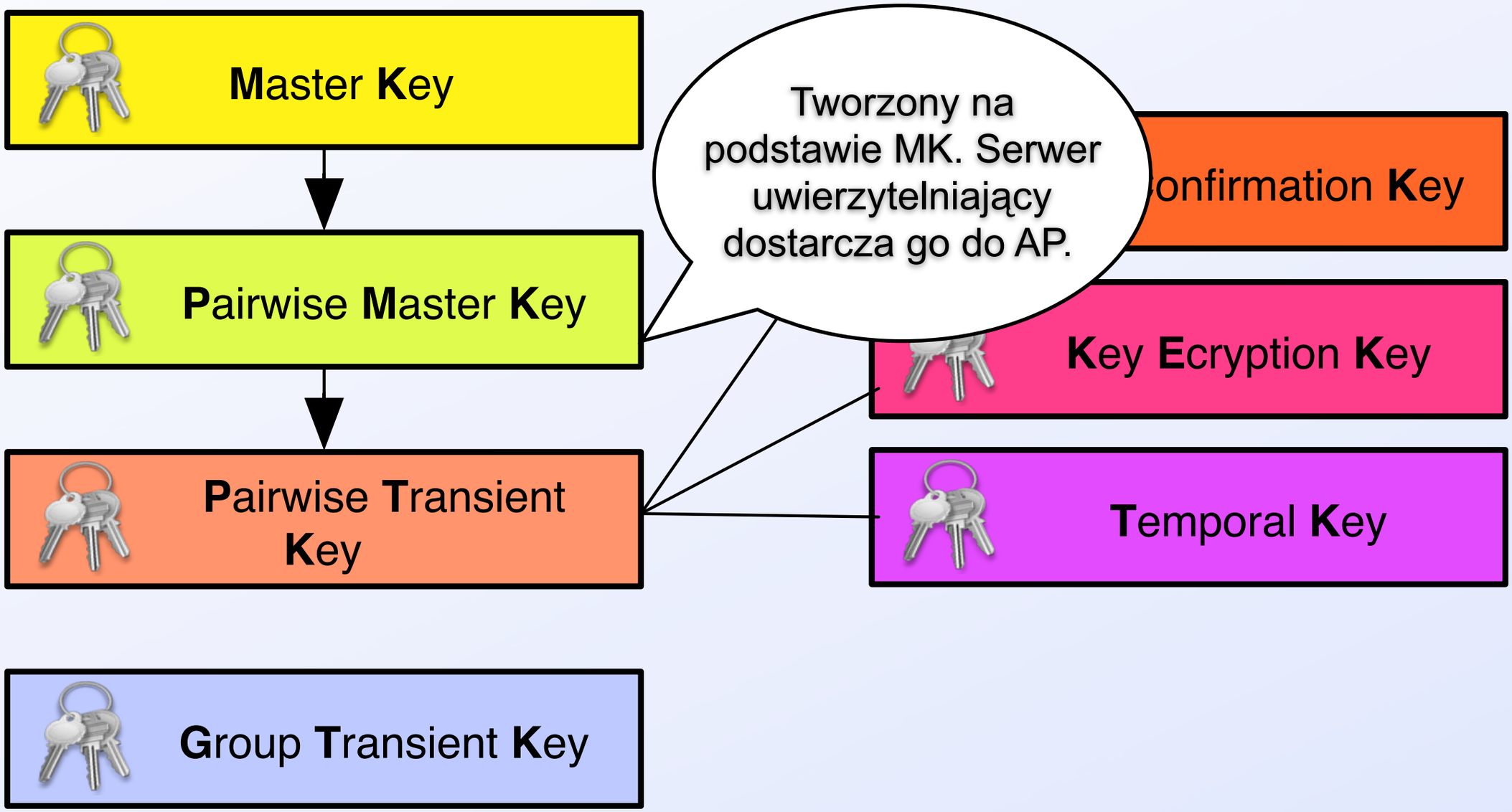
Group **T**ransient **K**ey

Key **C**onfirmation **K**ey

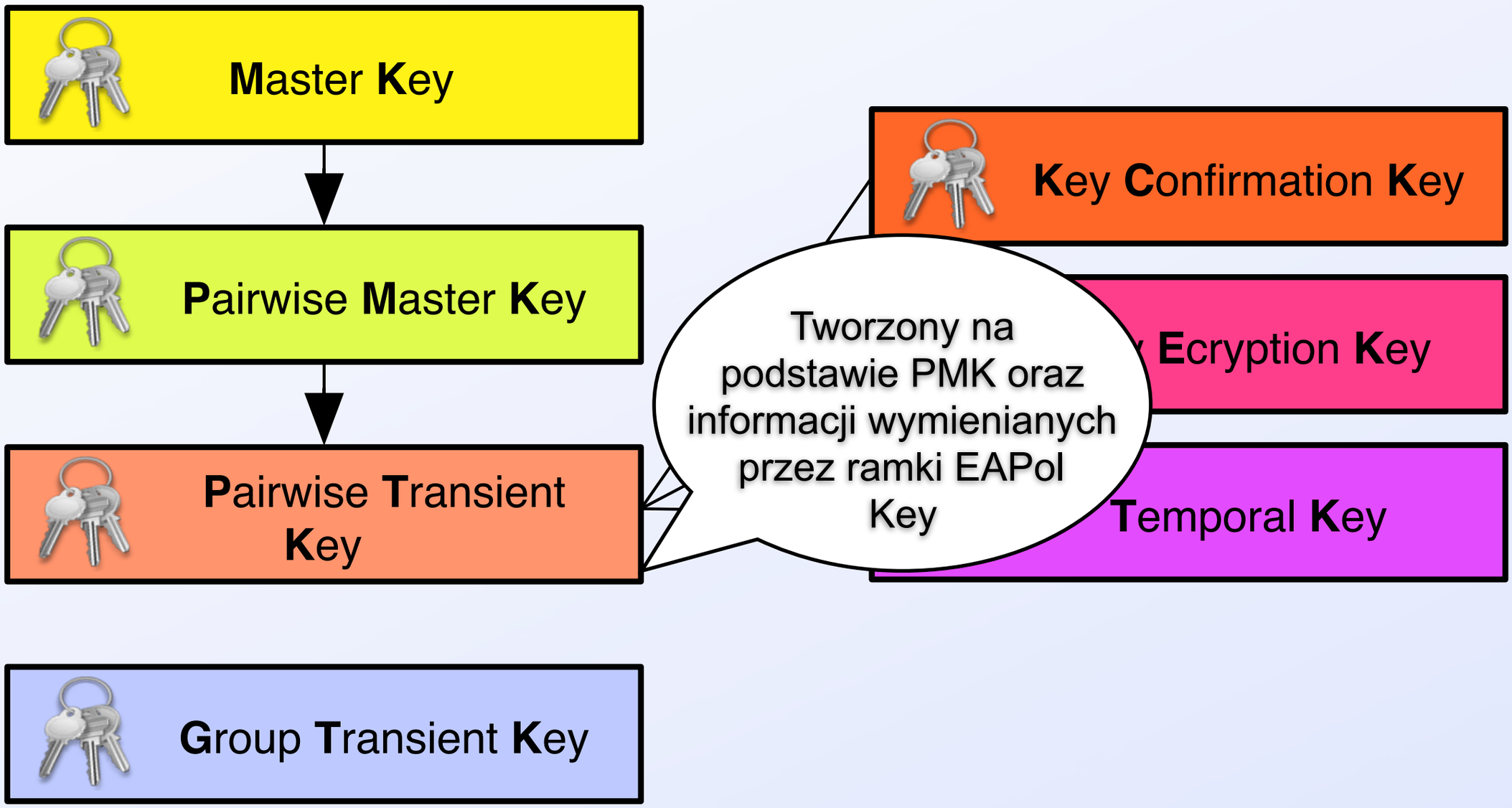
Key **E**cryption **K**ey

Temporal **K**ey

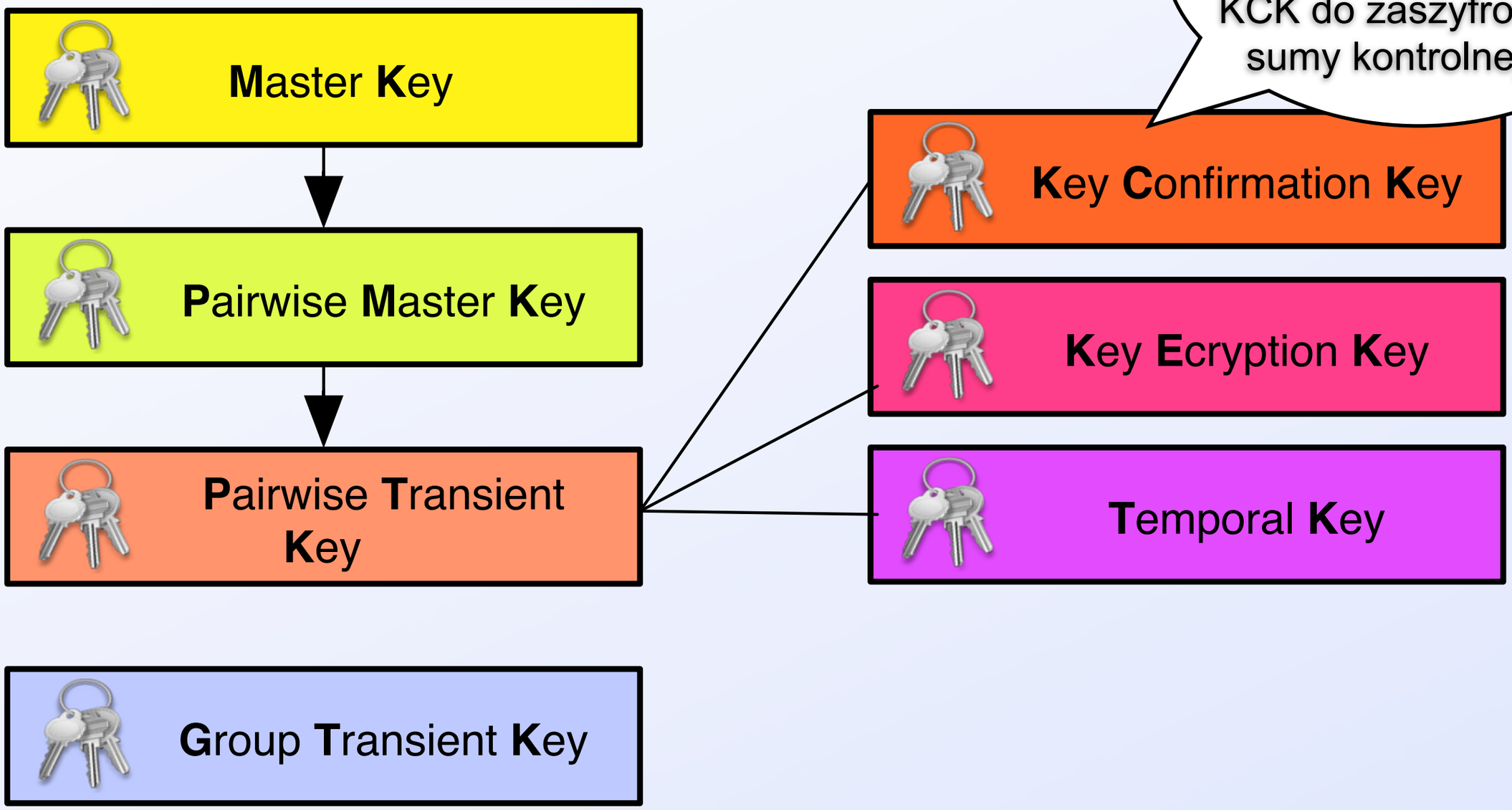
802.11i - klucze



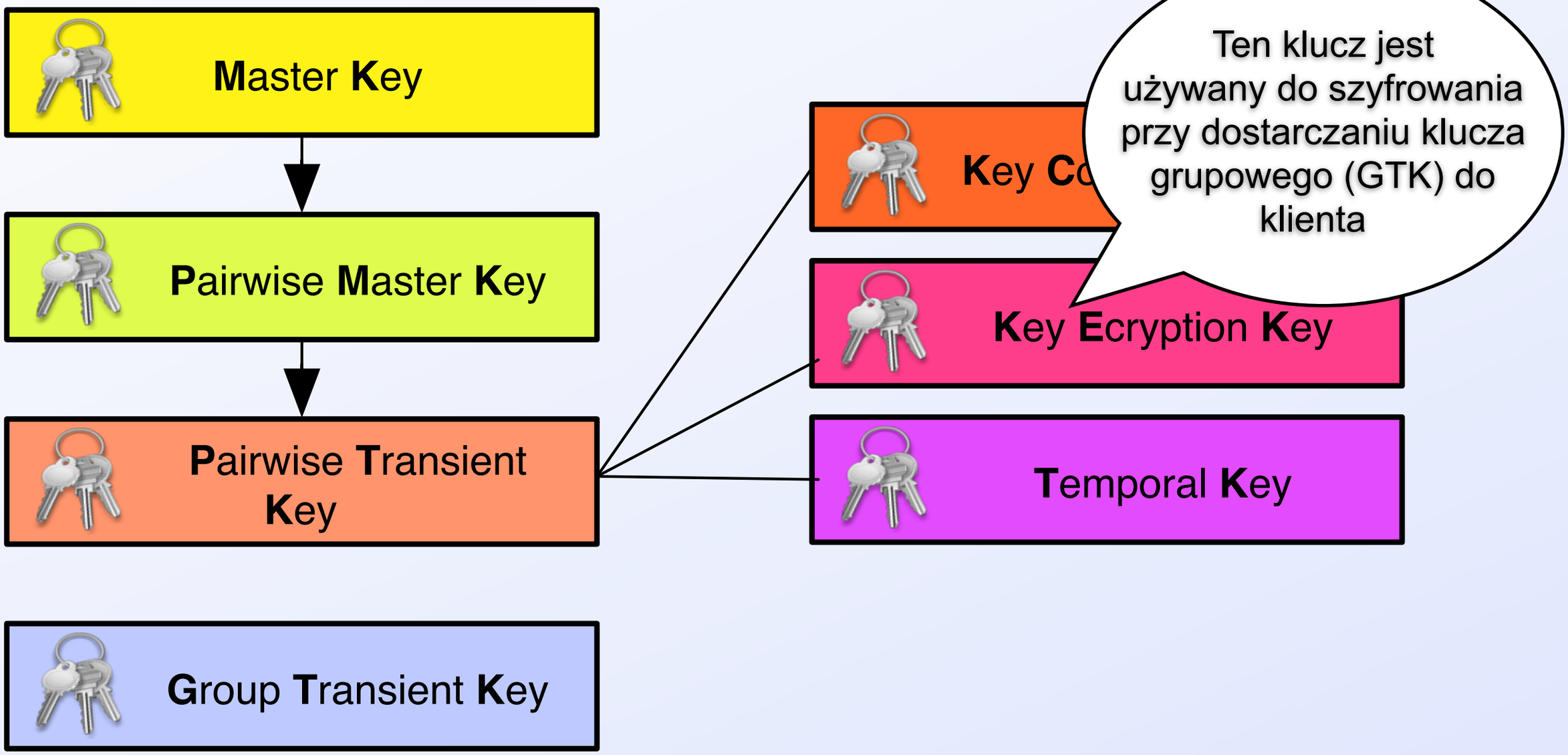
802.11i - klucze



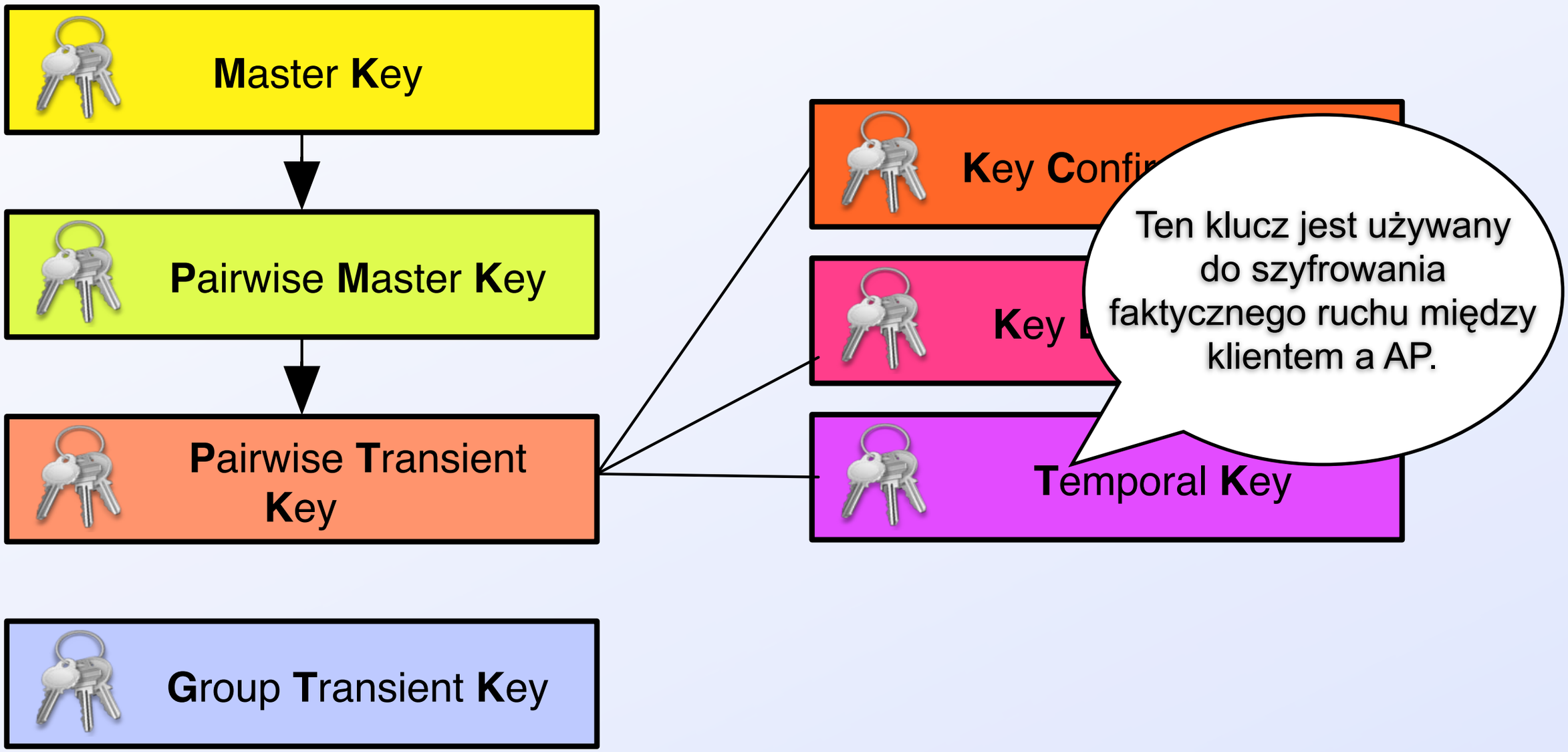
802.11i - klucze



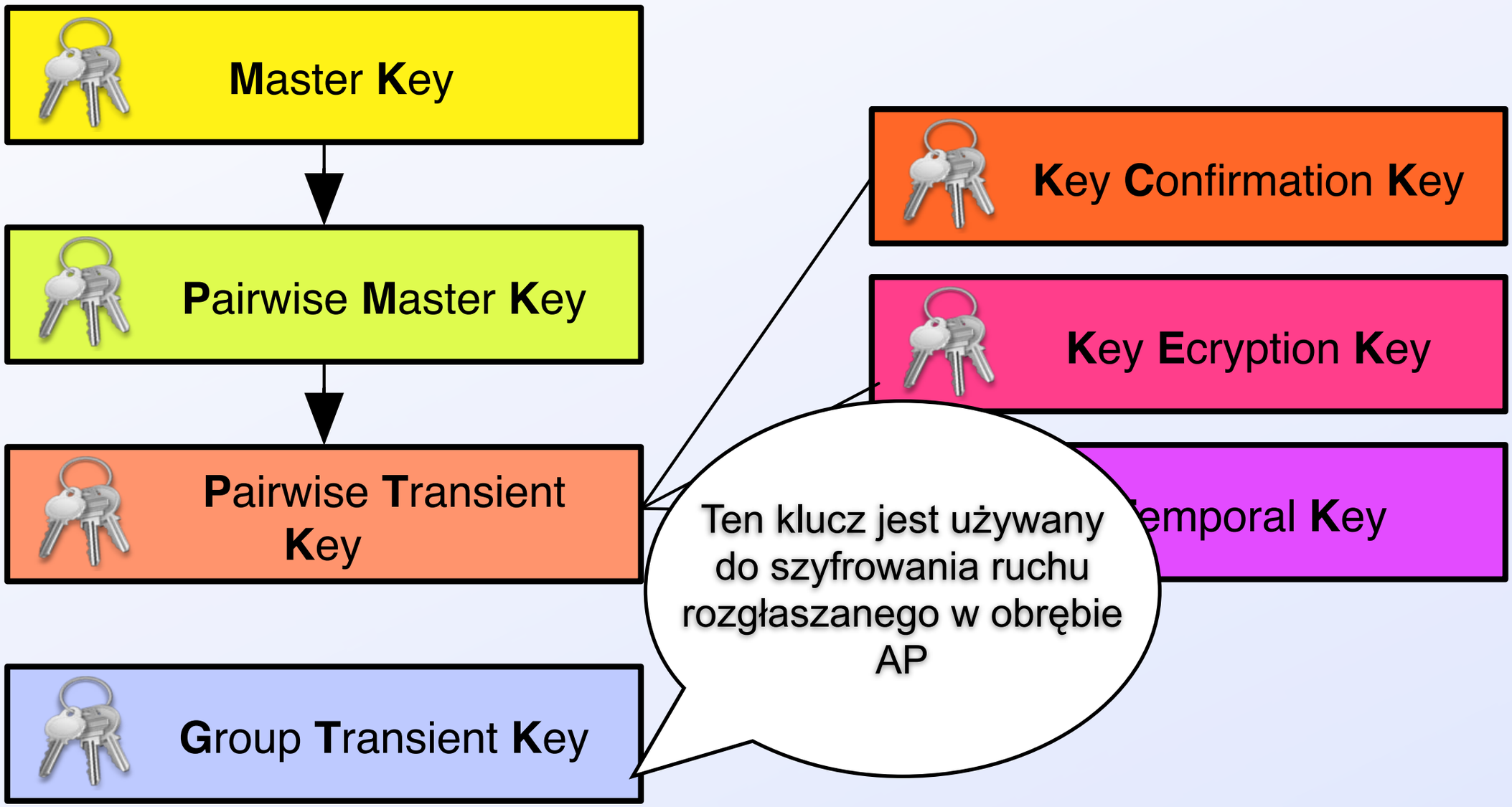
802.11i - klucze



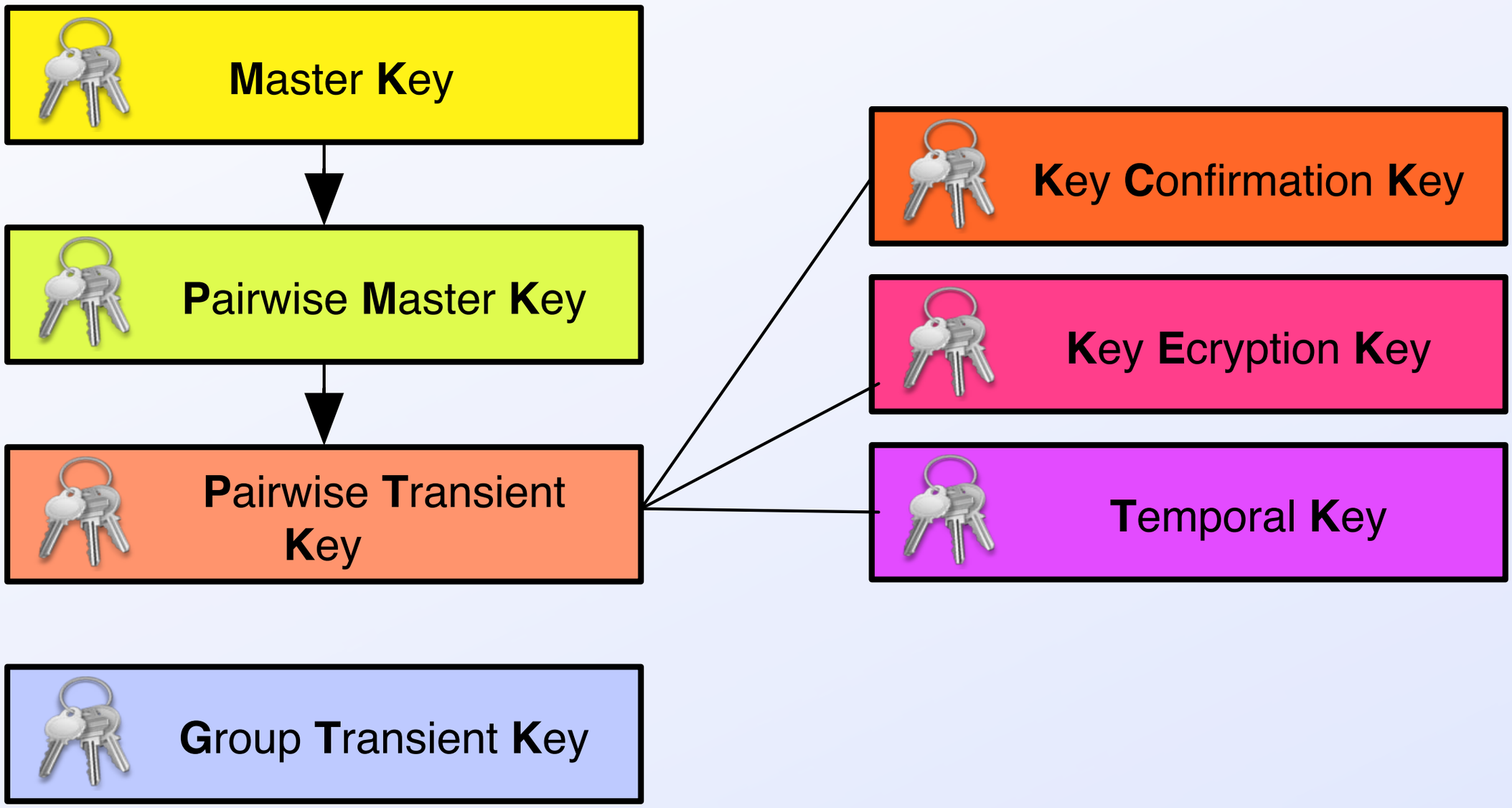
802.11i - klucze



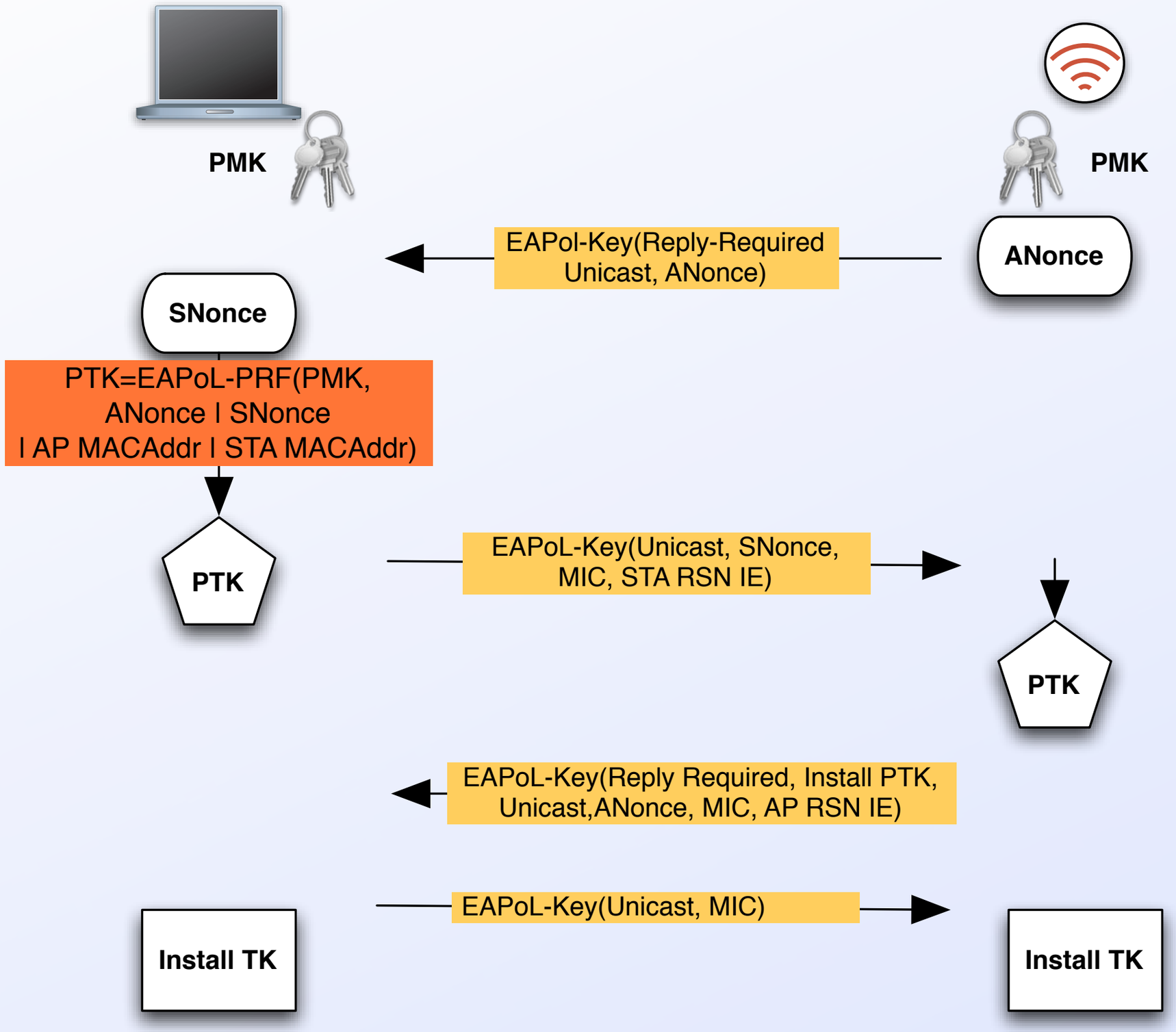
802.11i - klucze



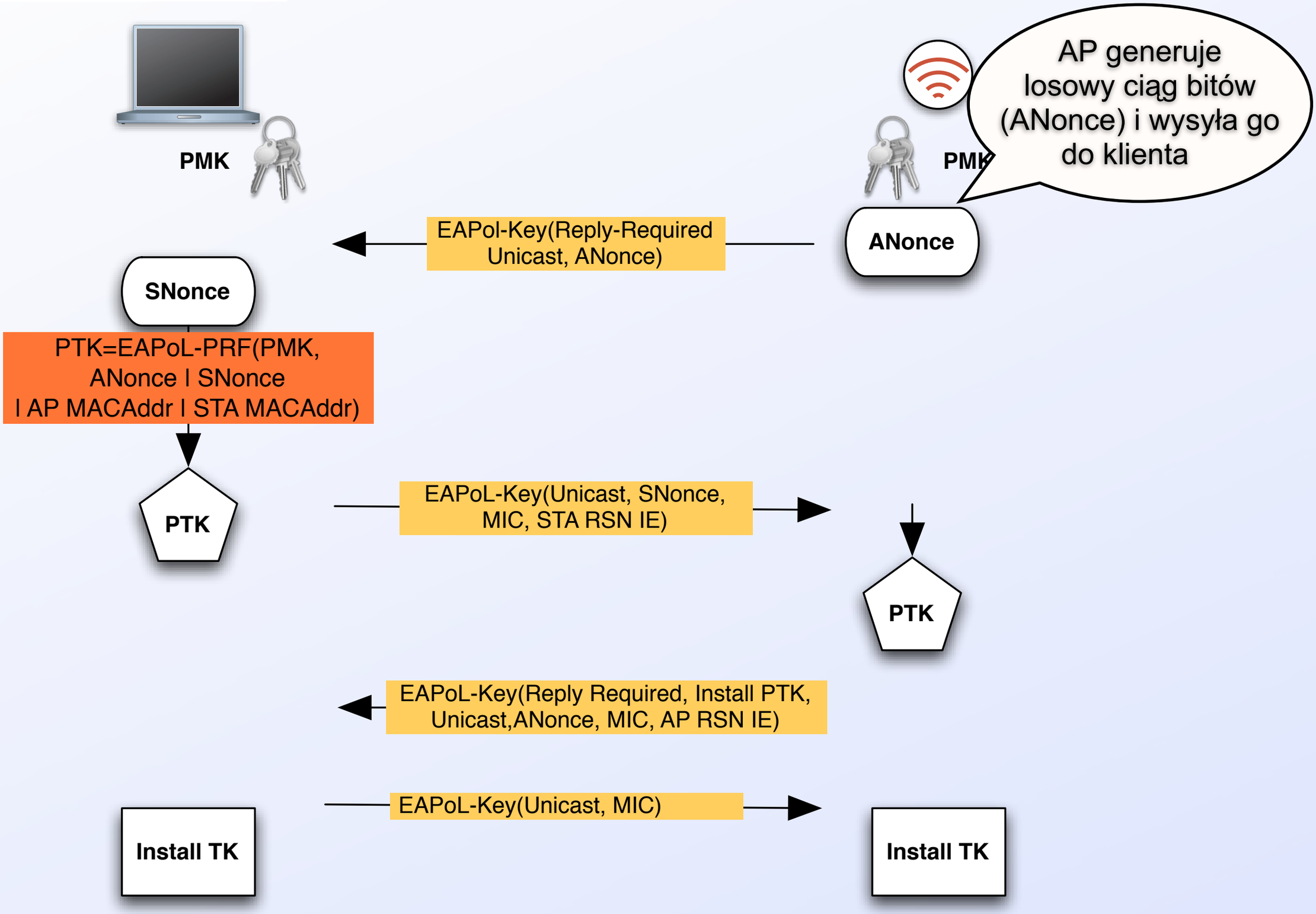
802.11i - klucze



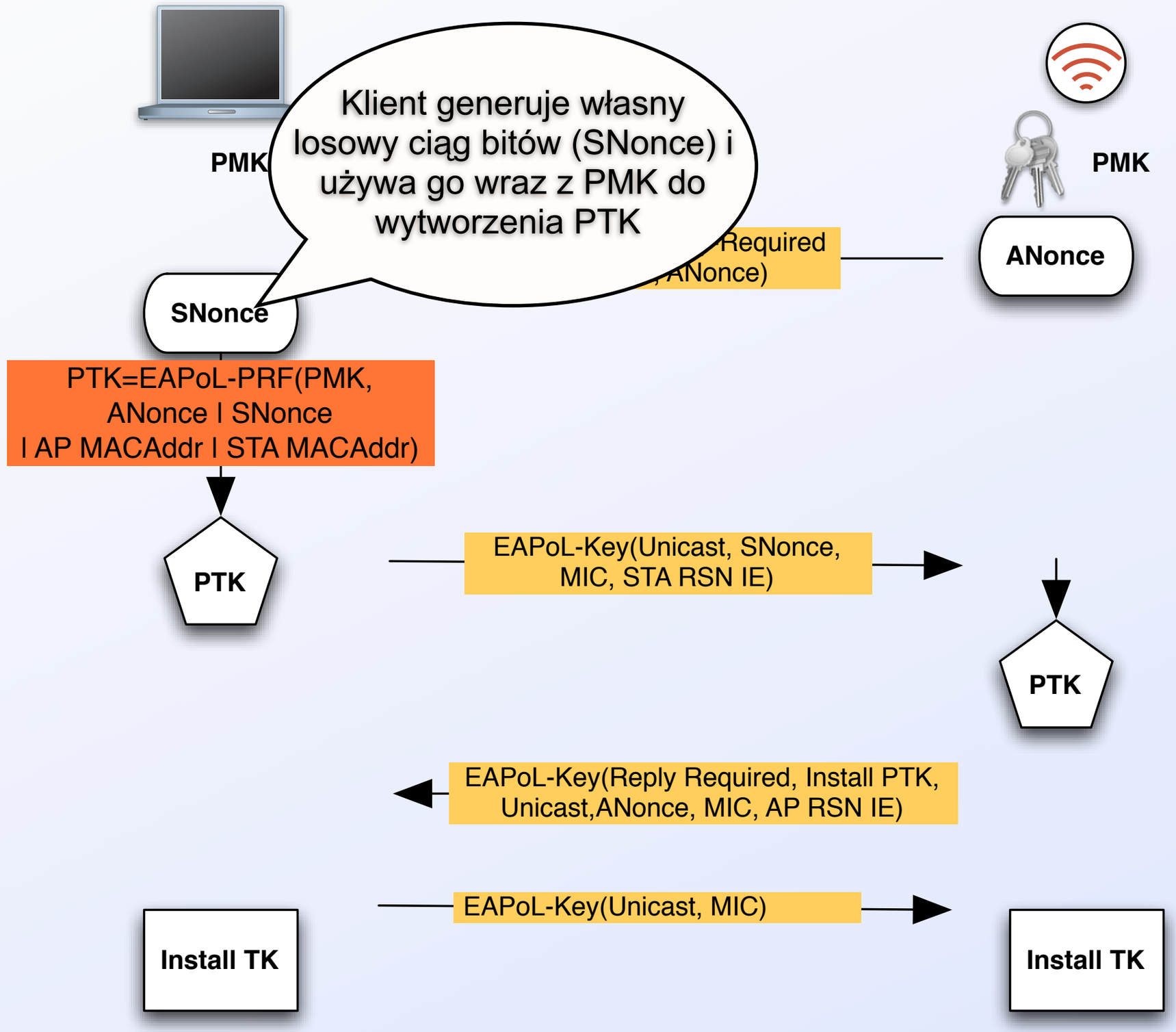
802.11i - wymiana kluczy



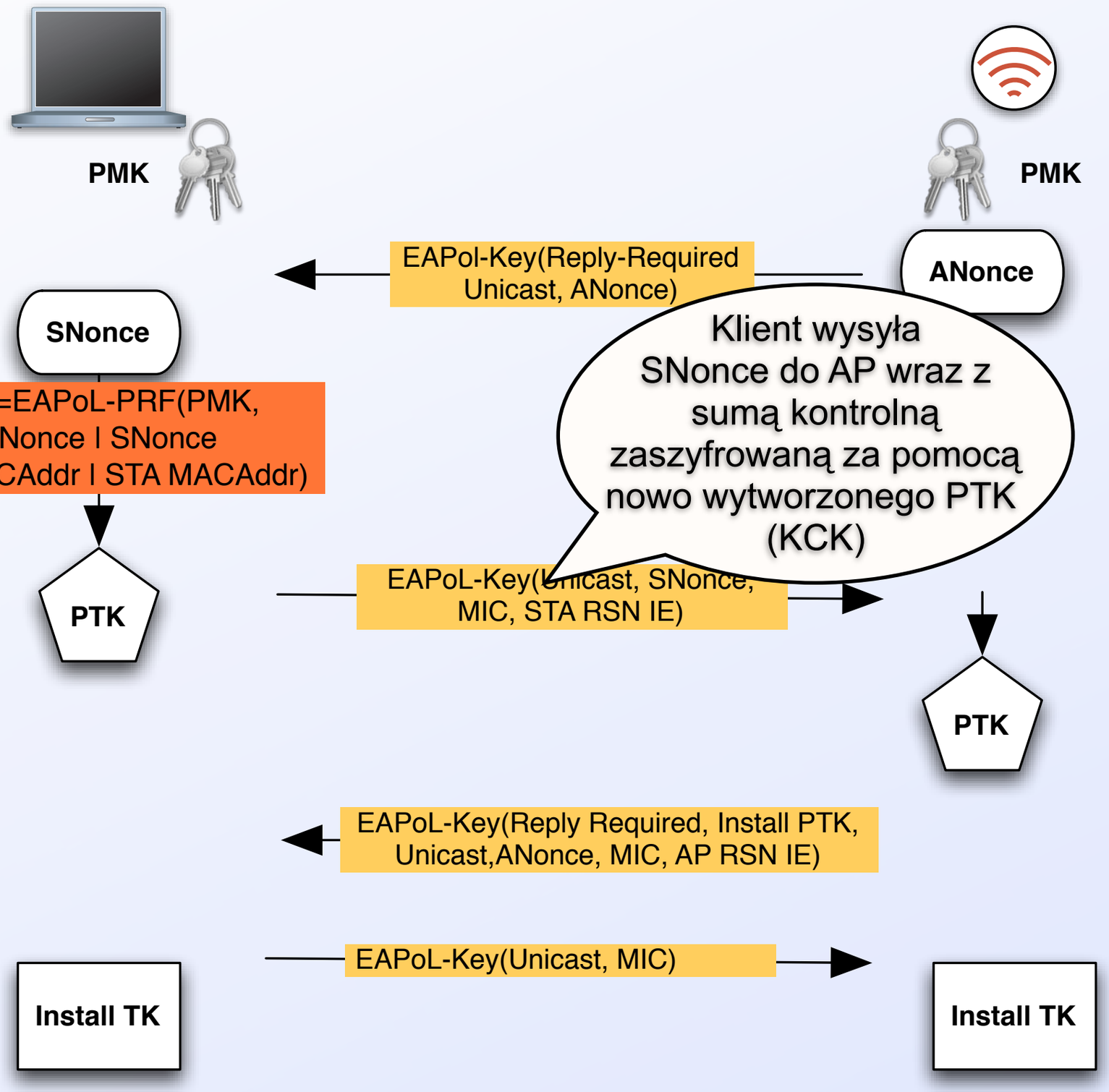
802.11i - wymiana kluczy



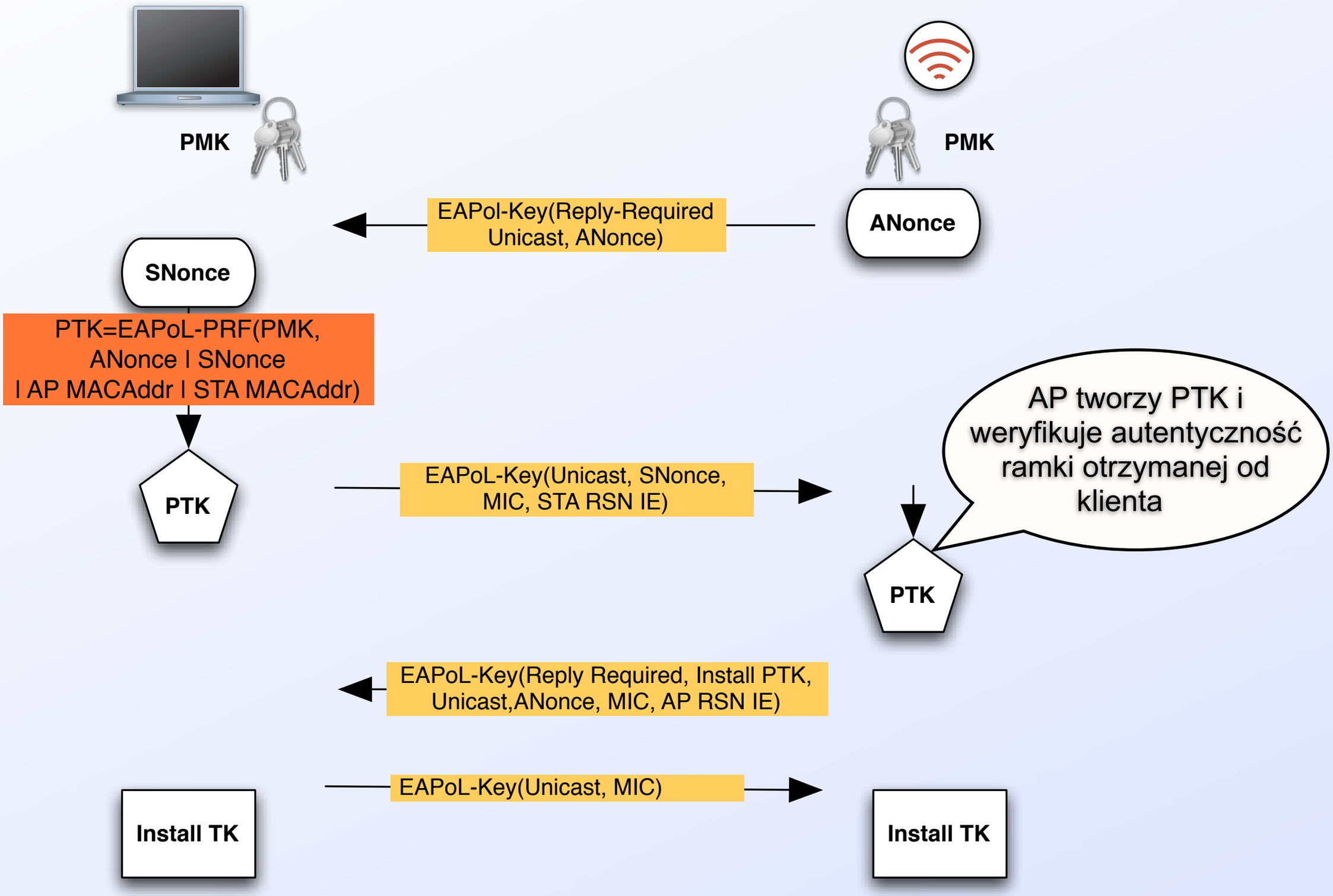
802.11i - wymiana kluczy



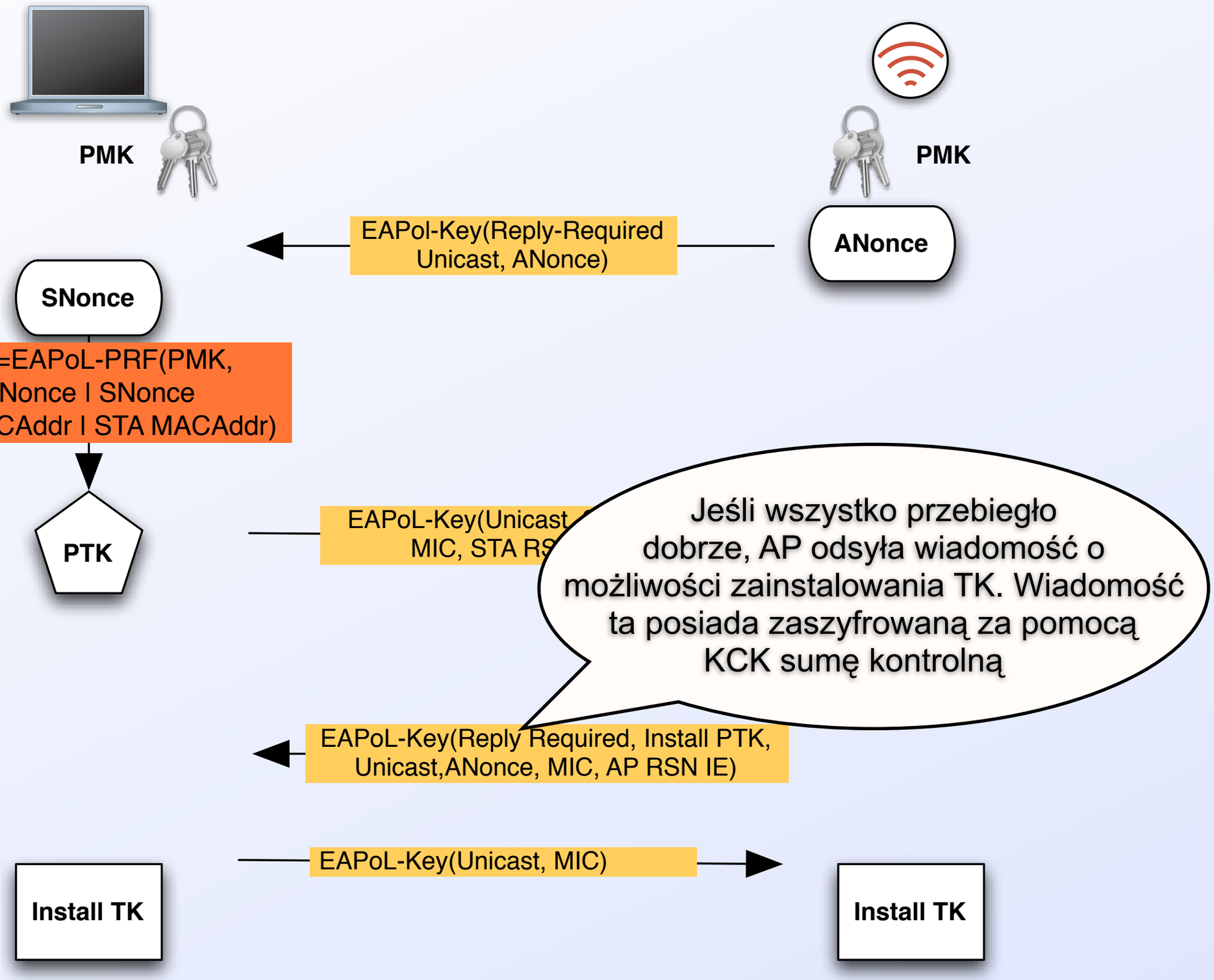
802.11i - wymiana kluczy



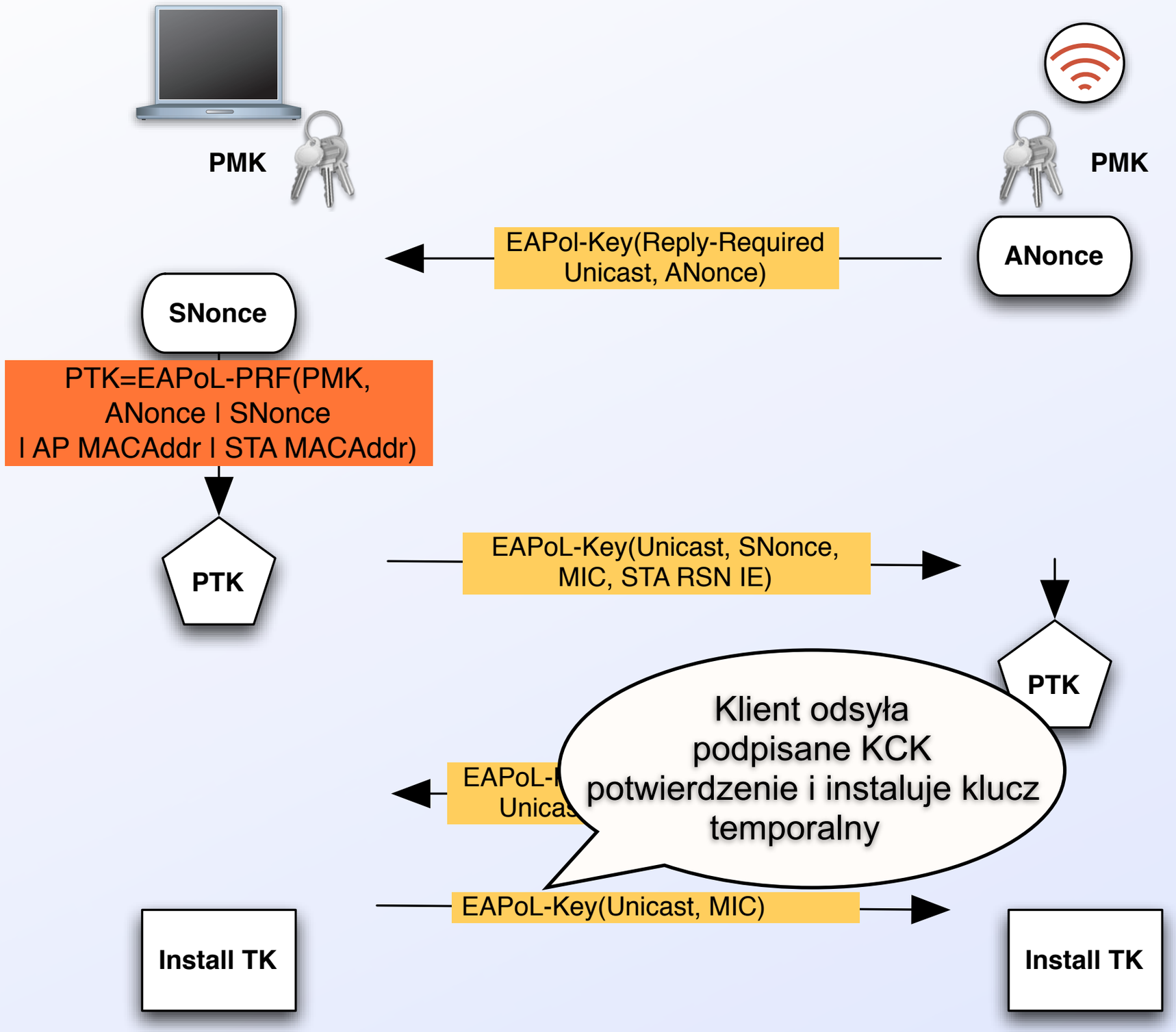
802.11i - wymiana kluczy



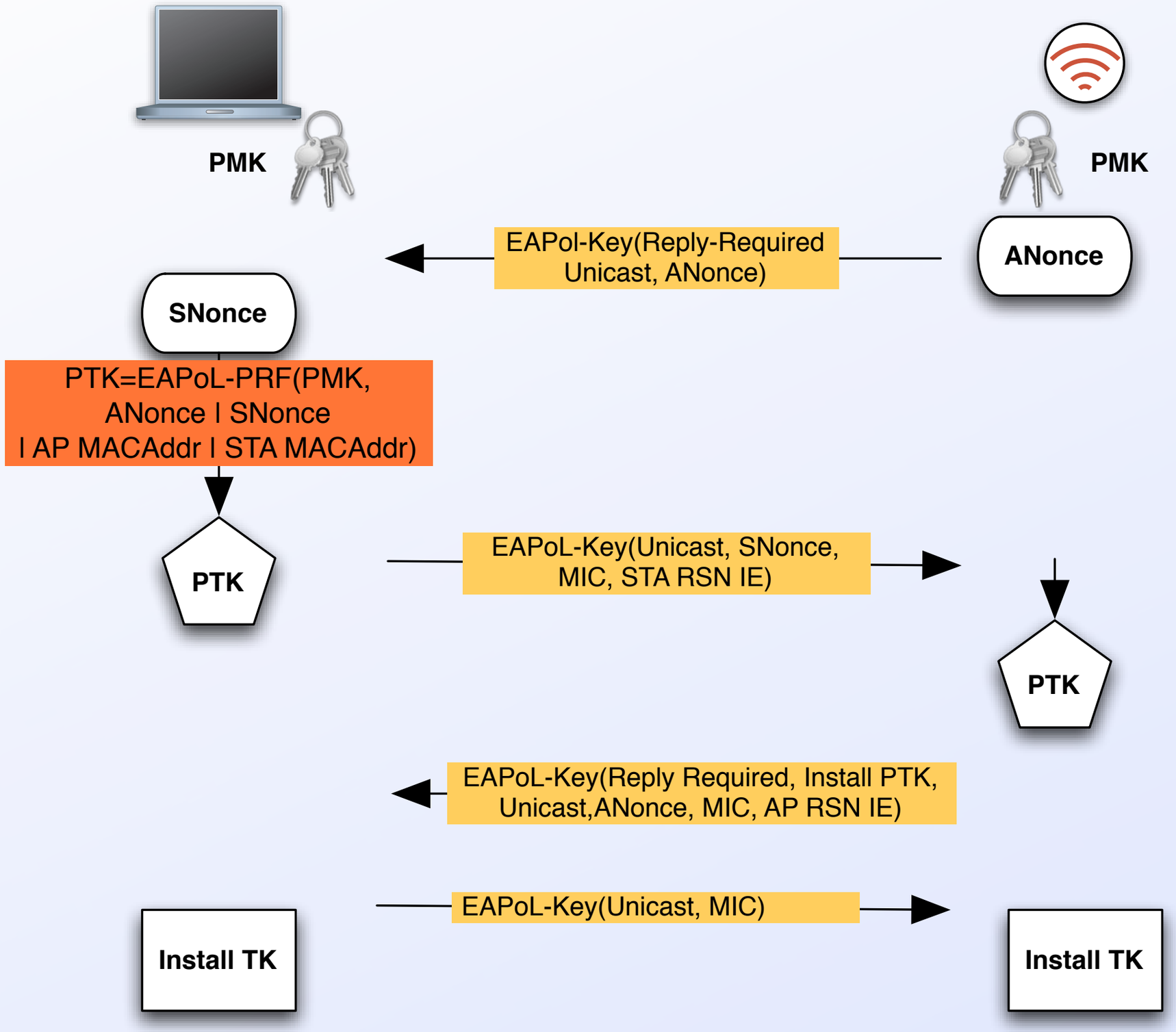
802.11i - wymiana kluczy



802.11i - wymiana kluczy



802.11i - wymiana kluczy



Podsumowanie

Niebezpiecznie

Bezpiecznie

Podsumowanie

Niebezpiecznie

Brak szyfrowania

Bezpiecznie

Podsumowanie

Niebezpiecznie

Brak szyfrowania

Statyczny WEP

Bezpiecznie

Podsumowanie

Niebezpiecznie

Brak szyfrowania

Statyczny WEP

WPA - PSK (TKIP)

Bezpiecznie

Podsumowanie

Niebezpiecznie

Brak szyfrowania

Statyczny WEP

WPA - PSK (TKIP)

802.1x + dynamiczny WEP

Bezpiecznie

Podsumowanie

Niebezpiecznie

Brak szyfrowania

Statyczny WEP

WPA - PSK (TKIP)

802.1x + dynamiczny WEP

WPA2 - PSK (AES)

Bezpiecznie

Podsumowanie

Niebezpiecznie

Brak szyfrowania

Statyczny WEP

WPA - PSK (TKIP)

802.1x + dynamiczny WEP

WPA2 - PSK (AES)

802.11i (TKIP)

Bezpiecznie

Podsumowanie

Niebezpiecznie

Brak szyfrowania

Statyczny WEP

WPA - PSK (TKIP)

802.1x + dynamiczny WEP

WPA2 - PSK (AES)

802.11i (TKIP)

802.11i (AES)

Bezpiecznie

Podsumowanie

Niebezpiecznie

Brak szyfrowania

Statyczny WEP

WPA - PSK (TKIP)

802.1x + dynamiczny WEP

WPA2 - PSK (AES)

802.11i (TKIP)

802.11i (AES)

802.11i (CCMP)

Bezpiecznie

Podsumowanie

Niebezpiecznie

Brak szyfrowania

Statyczny WEP

WPA - PSK (TKIP)

802.1x + dynamiczny WEP

WPA2 - PSK (AES)

802.11i (TKIP)

802.11i (AES)

802.11i (CCMP)

Bezpiecznie

Koniec