ĐẠI HỌC QUỐC GIA TP.HCM

TRƯỜNG ĐH KHOA HỌC TỰ NHIÊN

BÁO CÁO ĐỒ ÁN

Lớp: Nhập môn mã hóa ứng dụng CQ2019/22

Đề tài: Đề tài WEP, WPA, WPA2

Nhóm: 07

Tp.HCM, năm 2022

Mục Lục

I. WEP:

1. *Giới thiệu:*

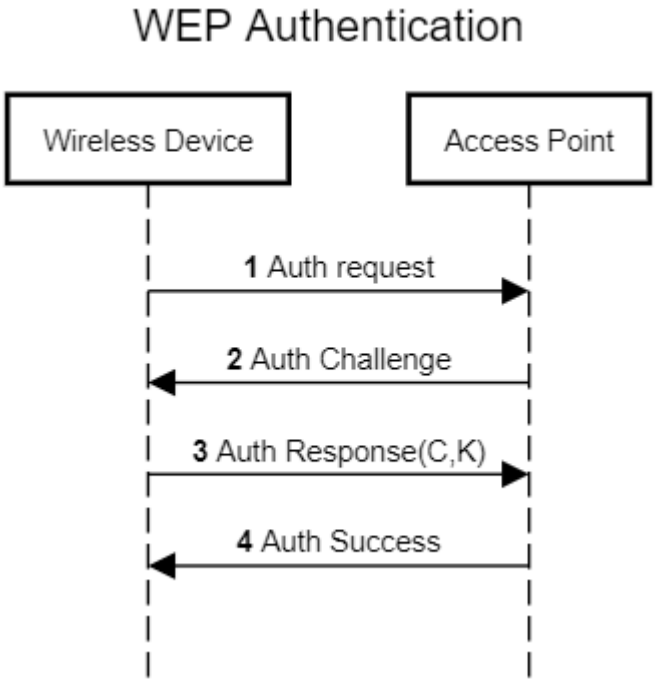
- WEP (Wired Equivalent Privacy, tạm dịch bảo mật tương đương mạng có dây (Wired LAN)) được giới thiệu là một phần của tiêu chuẩn IEEE 802.11 được phê chuẩn vào năm 1997 với dự định là cung cấp hình thức bảo mật dữ liệu như mạng mạng có dây (WLAN).
- Theo tiêu chuẩn 802.11, WEP được dùng để bảo vệ việc giao tiếp không dây (wireless communication) tránh khỏi nghe lén (eavesdropping), đồng thời ngăn chặn những tiếp cận không được phép (unauthorized access) vào mạng.

2. *Cách WEP hoạt động dựa trên tiêu chuẩn IEEE 802.11*

- WEP dựa trên khóa bí mật được chia sẻ giữa wirless device (vd: laptop, tablet) với access point (vd: mordem). Khóa bí mật sau đó được sử dụng để mã hóa các gói tin (packets) trước khi được chuyển đi trong mạng, và được sử dụng cho quá trình authentication.

a) WEP authentication:

- Diễn ra khi người dùng lần đầu tiên truy cập vào mạng LAN. Mục đích của quá trình này nhằm ngăn chặn thiết bị không biết mật khẩu truy cập vào mạng.



1: Wireless Device gửi yêu cầu authentication đến Access Point.

2: Access Point gửi response có chứa một đoạn kí tự ngẫu nhiên dài 128 bits (challenge)

3: Wireles Device sử dụng mã hóa challenge bằng preshared key bằng WEP sau đó gửi response chứa đoạn thông tin vừa mã hóa cho Access Point.

4: Access Point nhận được response sau đó giải mã challenge được mã hóa sau đó đem so sánh với challenge gốc, nếu đúng thì quá trình authenticate thành công, nếu sai thì ngược lại.

❖ ***Authentication messages:*** Thường có dạng như hình bên dưới

Algorithm Num	Transaction Seq.	Status Code	Challenge Text

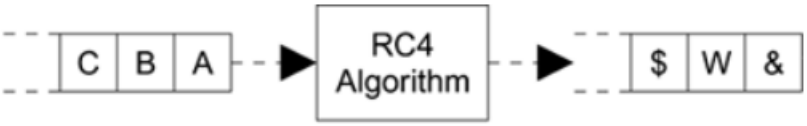
Trong đó:

- Algorithm Num: thể hiện loại authentiaction được sử dụng. Nếu bằng 0 thì tương đương với ***Open System***, nếu bằng 1 thì tương đương với ***Shared Key (WEP)***.
- Transaction Sequence: thể hiện đang ở bước nào của quá trình authentication.
- Status Code: được gửi trong message cuối cùng để thể hiện quá trình authentication là thành công hay thất bại.
- Challenge Text: được gửi bởi Access Point và đã được mô tả bên trên.

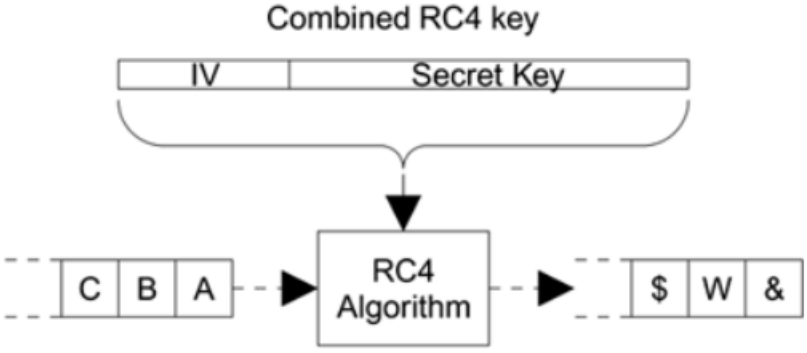
b) Mã hóa WEP (WEP Encryption):

- **WEP Privacy:**
  - Khi nhắc đến mục đích của các cơ chế bảo mật là gì, người ta thường nghĩ ngay đến tình riêng tư như là một yếu tố quyết định. Tính riêng tư có nghĩa, dữ liệu của người dùng sẽ ngăn chặn được bên thứ ba bắt và hiểu được. Trên thực tế thì tính riêng tư chỉ là một phần của các giao thức bảo mật, tuy nhiên trong các giao thức truyền tin trên mạng Wi-fi, tính riêng tư luôn luôn được xem như là một thuộc tính quan trong nhất, và đây là mục tiêu trung tâm của WEP.
- **WEP Encryption:**
  - Để đảm bảo tính riêng tư, WEP sử dụng thuật toán mã hóa dòng (stream cipher) RC4 để mã hóa các gói tin. Bởi vì bài viết không phải về chủ đề thuật toán RC4, nên chúng ta sẽ không đi sâu tìm hiểu cách thức vận hành của RC4, ta chỉ cần xem thuật toán RC4 là một hộp đen (black box).
  - Công thức:

$$\text{Ciphertext} = (\text{Plaintext}+\text{ICV}) \oplus \text{RC4\_Keystream (secret key)}$$



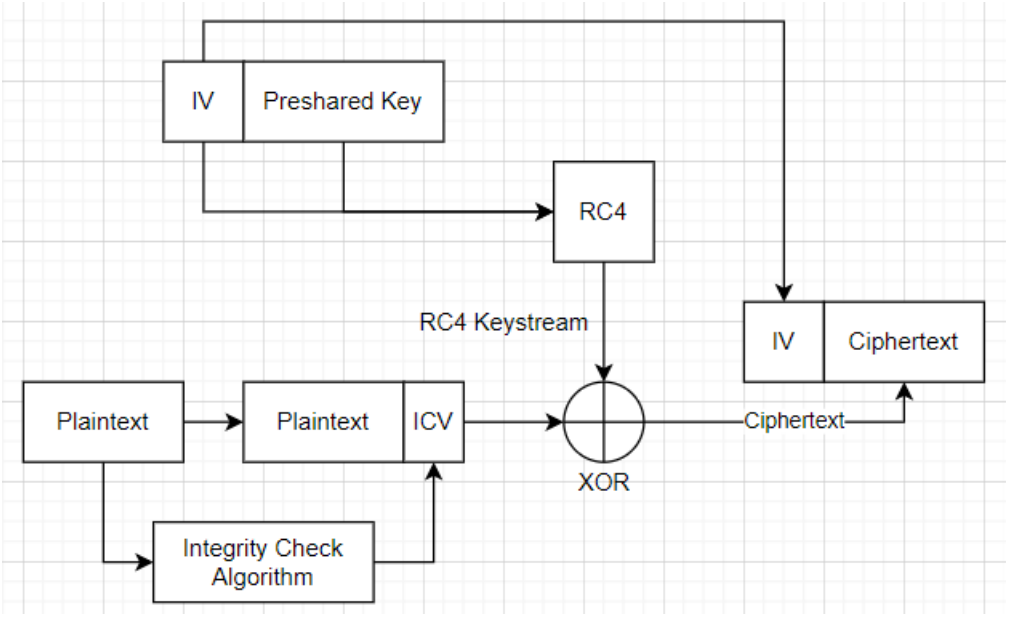
  - Tuy nhiên, ta nhận thấy rằng nếu sử dụng một khóa không đổi cho RC4 thì chỉ cần một lộ một cặp ciphertext và plaintext thì kẻ tấn công sẽ biết được keystream và giải mã các ciphertex khác.
- **Initialization Vector (IV):**
  - Để khắp phục vấn đề trên, giải pháp được đưa ra là sử dụng một initialization vector (IV). Cách sử dụng vô cùng đơn giản, thay vì chỉ dùng preshared key để làm khóa cho RC4, ta có thể sử dụng kết hợp IV và preshared key. Bởi vì khóa của RC4 luôn đổi nên dù trong hai gói tin khác nhau có chứa cùng một đoạn thông tin thì cũng sẽ không cho ra một đoạn ciphertex giống nhau.



  - Mặc dù vậy, một vấn đề mới được phát sinh khi trong tiêu chuẩn IEEE 802.11 WEP định nghĩa độ dài của IV là 24 bits. Điều này cho thấy rằng chỉ có gần 17 triệu giá trị IV khác nhau. Điều này có nghĩa với một preshared key thì ta có khoảng gần 17 triệu cách kết hợp khác nhau. Với việc đảm bảo không xảy ra tình trạng cùng một đoạn plaintext thì sau khi dùng RC4 cho ra một đoạn ciphertext giống nhau thì các khóa kết hợp chỉ được ***sử dụng 1 lần duy nhất***. Với một Access Point có tốc độ là 11Mbps thì khả năng chuyển/nhận gói tin sẽ là 700 packet/s. Vì vậy chỉ cần khoảng 7 giờ để sử dụng hết 17 triệu khóa kết hợp.

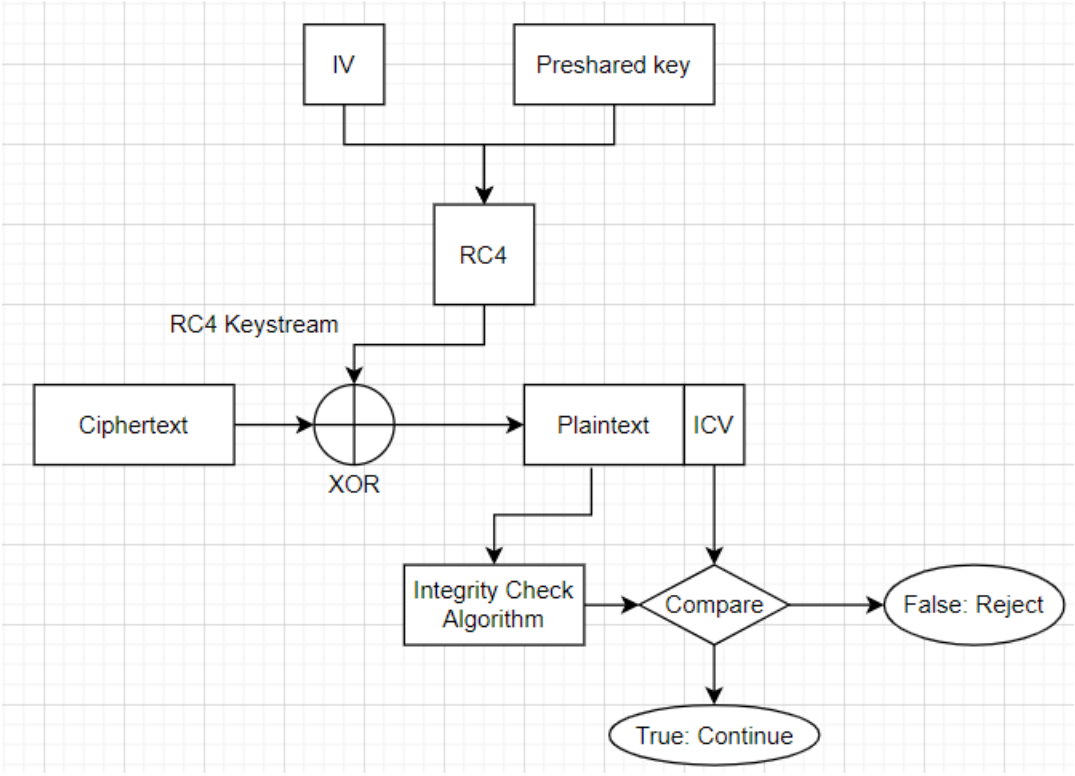
- **Cơ chế của WEP (Mechanic of WEP)**

  - Pha mã hóa WEP (WEP Encryption)



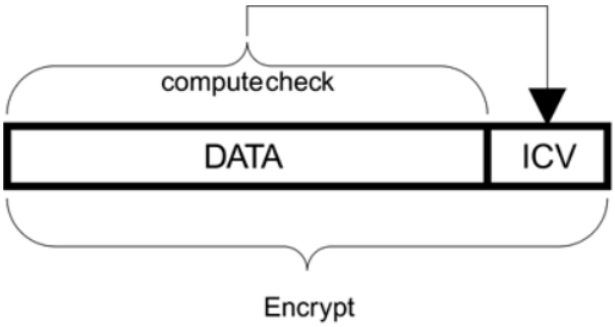
ICV = Integrity_Check_Algorithm (Plaintext)
RC4_Keystream = RC4(IV, Preshared_Key)
Ciphertext = (Plaintext+ICV) ⊕ RC4_Keystream

  - Pha giải mã WEP (WEP Decryption)

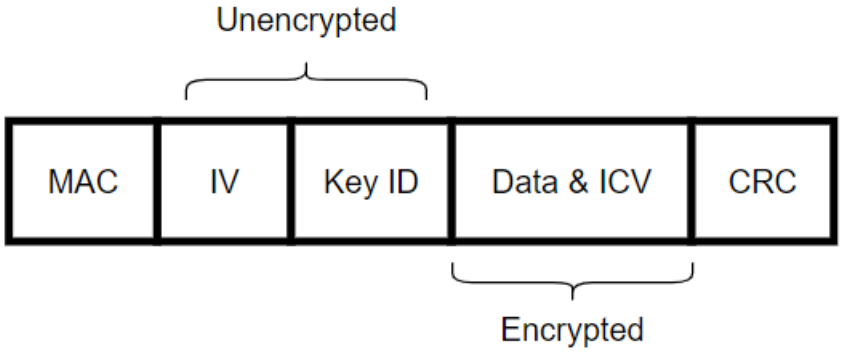


RC4_Keystream = RC4(IV, Preshared_Key)
Plaintext+ICV= (Ciphertext) ⊕ RC4_Keystream
If (ICV == Integrity_Check_Algorithm (Plaintext)) ***return Continue***
Else ***return Reject***

- Giá trị kiểm tra tính toàn vẹn (Integrity Check Value-ICV)
    - Mục đích đằng sau của ICV là nhằm phát hiện những thông tin bị thay đổi khi truyền tin. Trên lý thuyết, ICV được ghép vào ngay sau phần plaintext và cả 2 sẽ được mã hóa, vì vậy kẻ tấn công không thể nào tính toán lại được giá trị ICV khi thay đổi nôi dụng plaintext.
    - ICV được tính toán bằng việc kết hợp tất cả các byte dữ liệu để tạo checkwork có độ dài 4-byte và sau đó được ghép vào ngay sau plaintext



- Cấu trúc của một Frame (Frame Structure)



    - Trong đó:
        - MAC: MAC Header, chứa thông tin của thiết bị nguồn và thiết bị đích.
        - IV: Initialization Vector, được truyền đi để kết hợp với preshared key để mã hóa RC4.
        - Data & ICV: Dữ liệu và ICV được mã hóa.
        - CRC: Cyclic Redundancy Check, tổng kiểm tra có độ dài 4-byte nhằm kiểm tra xem gói tin có bị mất mát hoặc thay đổi gì trên đường truyền hay không
    - Trong cấu trúc trên ngoại trừ phần MAC và phần CRC là mặc định của mô hình truyền tin trên mạng. Các thành phần còn lại đều được thêm vào để đảm bảo rằng thiết bị đích có thể giải mã được cũng như kiểm tra xem gói tin có bị thay đổi hay không. Nếu ta bỏ bớt bất cứ thành phần nào thì sẽ không còn đảm bảo hai tính chất trên.

c) WEP Vulnerability:

- Cuộc tấn công khôi phục Keystream (Keystream Recorery)
    - Nếu kẻ tân công biết được Plaintext, thì Keystream rất đơn giản có thể được suy ra từ công thức dưới đây:

Ciphertext ⊕ Plaintext = Key_stream ⊕ Plaintext ⊕ Plaintext = Key_stream

- Thậm chí ngay cả khi không biết Plaintext là gì, kẻ tấn công vẫn có thể suy ra được nội dung gói tin dựa vào những trường cố định trong các gói tin. VD: Header, IP, vv…
- Tuy nhiên, kẻ tấn công sẽ không đạt được mục đích nếu như Keystream không bao giờ trùng lại. Nhưng như đã đề cập bên trên Keystream chắc chắc sẽ trùng lại sau vài giờ sử dụng. Lúc này kẻ tấn công chỉ cần lưu trữ các cặp Keystream tương ứng với giá trị IV sau đó chờ giá trị IV được sử dụng lại thì có thể giải mã và lấy được thông tin mà không cần biết chính xác khóa bí mật là gì.
- Nhược điểm của kiểu tấn công này là thụ động và rất khó trong trường hợp mạng ít hoạt động.

- Tấn công trực tiếp vào khóa (Directly Key Attacks)[1]
  - Trong bài báo khoa học của Fluhrer, Mantin và Shamir với tên gọi "Weaknesses in the Key Scheduling Algorithm of RC4", họ cho thấy rằng việc sử dụng giá trị công khai IV được thêm vào khóa bí mật đã tạo ra một điểm yếu rất lớn vì nó cho phép kẻ tấn công đợi những khóa có khả năng yếu và tấn công trực tiếp vào nó.
  - Họ cũng chứng minh được, trường hợp IV được chèn vào ngay trước preshared key thì dễ bị tấn công hơn là trường hợp IV được chèn vào sau preshared key.
  - Phương thức tấn công này có thể được lập trình để tấn công tự động. Việc thay đổi độ dài preshared key từ 40-bit thành 104-bit chỉ có tác dụng làm cho thời gian tìm ra preshared key lâu hơn 2.5 lần.

3. Tài liệu tham khảo:

- RC4 Algorithm: https://www.geeksforgeeks.org/rc4-encryption-algorithm/
- How WEP works: Chapter 6. How IEEE 802.11 WEP Works and Why It Doesn't
- Directly Key Attack: Fluhrer, Mantin and Shamir attack - Wikipedia

II. WPA và WPA 2:

1. Giới thiệu:

- Từ việc WEP chứa nhiều lỗ hổng bảo mật như trên, các kĩ sữ đã nghiên cứu một tiêu chuẩn mới có là 802.11i nhằm định nghĩa một giao thức mới mạnh mẽ hơn có trên là RSN (Robust Security Network). Tuy nhiên vấn đề của RSN là các phần cứng thời điểm đó không thể xử lý được thuật toán mã hóa trong RSN. Hơn nữa, các nhà sản xuất thiết bị không dây kết luận rằng người dùng không thể ngay lập tức bỏ hết tất cả các thiết bị đang tương thích với WEP để chuyển qua các thiết bị tương thích với RSN. Người dùng mong muốn một nâng cấp về phần mềm.
- Vào năm 2003, tổ chức Wi-Fi Alliance đã đưa ra dự thảo tiêu chuẩn IEEE 802.11i nhằm định nghĩa cho WPA với mục đích thử nghiệm. Và đến năm 2004, tiêu chuẩn IEEE 802.11i đầy đủ (hay IEEE 802.11i-2004) đã định nghĩa giao thức WPA2 phức tạp hơn nhưng an toàn hơn.
- Vào tháng 1 năm 2028, với một số cải tiến trên giao thức WPA2 tổ chức Wi-Fi Alliance đã công bố giao thức WPA3 thay thế cho giao thức WPA2. Tuy nhiên ngày nay giao thức WPA2 vẫn

2. WPA/WPA2 Authentication:

- Trong quá trình Authentication, cả WPA và WPA2 rất giống nhau. Cụ thể, WPA/WPA2 (bây giờ sẽ tạm gọi chung là WPA) sử dụng hai mode khác nhau:
  - WPA-Personal: còn được biết đến với tên gọi WPA-PSK (Pre-Shared Key), được thiết kế cho hộ gia đình hoặc mạng cỡ nhỏ. Nó sử dụng một mật khẩu cho tất cả

[1] Scott Fluhrer, Itsik Mantin, Adi Shamir "Weaknesses in the Key Scheduling Algorithm of RC4" Lecture Notes In Computer Science; Vol. 2259 archive. Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography table of contents Pages: 1 - 24 Year of Publication: 2001 ISBN:3-540-43066-0

user. Ưu điểm của hệ thống là dễ dàng cài đặt và triển khai. Tuy nhiên, nếu một thiết bị bị lộ mật khẩu hoặc bị khai thác thì cần phải đổi đổi mật khẩu truy cập cho tất cả các thiết bị.

- WPA-Enterprise: còn được biết đến với tên gọi WPA-802.1x, được thiết kế cho mạng cỡ trung bình và lớn (trong một công ty hoặc một tập đoàn lớn). Hệ thống yêu cần một RADIUS server và người dùng sử dụng định danh cá nhân của họ (personal identifier) để kết nối vào mạng. Ưu điểm, nếu một thiết bị bị khai thác hoặc bị lộ mật khẩu thì chỉ cần hủy kết nối của thiết bị này và không làm ảnh hưởng đến các thiết bị khác trong mạng. Nhược điểm, hệ thống này khó triển khai hơn WPA-Personal tuy nhiên người quản trị có thể quản lý được từng người dùng khác nhau (management user-by-user).

a) WPA-PSK:

- WPA-PSK sử dụng một Pre-shared Key (PSK) để thực hiện Authentication, được chia sẻ giữa các wireless devices và Access Point (AP). Độ dài của PSK nằm trong khoảng từ 8 đến 63 kí tự.
- Từ PSK đó, mỗi wireless devices lấy và lưu trữ một *bộ khóa chính* (Pairwise Master Key – PMK) cho đến khi PSK hoặc SSID (tên của AP) thay đổi.
- Khi một người dùng kết nối đến một AP, protocol 4-ways handshake (tạm dịch là bắt tay 4 bước) được thiết lập để tạo ra một *bộ khóa khóa tạm thời* (Pairwise Transient Key – PTK). Khóa này được dùng để mã hóa dữ liệu giữa người dùng và AP và được thay đổi sau ít nhất 65535 gói tin. Đây là một điều đã được cải tiến hơn so với WEP.
- ***Sinh PMK (PMK Generation)***
  - Đầu tiên, tất cả các wireless devices lấy Pairwise Master Key (PMK) từ Pre-shared Key (PSK)
  - PMK được tính toán bằng cách sử dụng *Hàm lấy khóa dựa trên mật khẩu* (Password-Based Key Derivation Function 2 – PBKDF2). Mục đích sử dụng của hàm này nhằm hạn chế những ảnh hưởng của tấn công Brute-force bởi vì hàm lượng tính toán lớn của nó.
  - Công thức

    PMK = PBKDF2(HMAC-SHA1, PSK, SSID, 4096, 256)

    Trong đó:

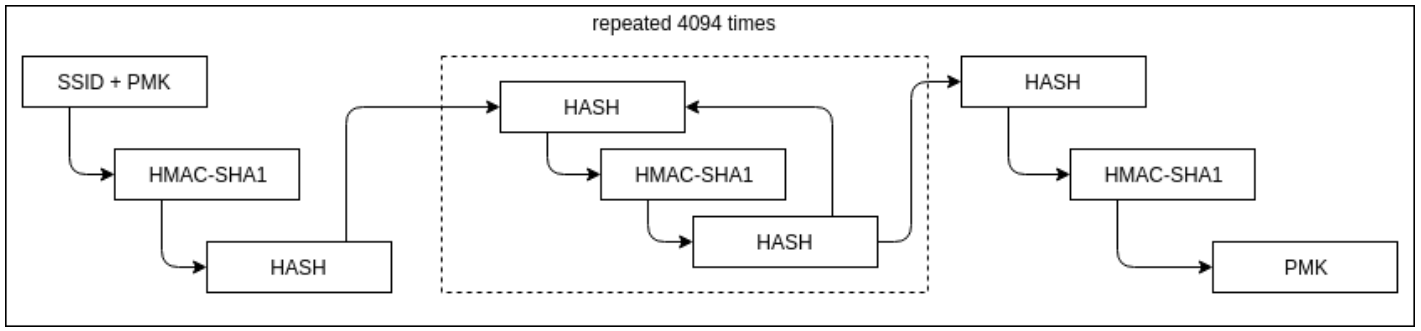
    HMAC-SHA1[2]: là một loại mã tin nhắn xác thực (Message Authentication Code) bao gồm hàm băm mật mã và khóa bí mật.

    PSK: Pre-shared Key

    SSID: Được sử dụng như một message đầu vào của HMAC-SHA1.

    4096: số lần lặp lại quá trình băm

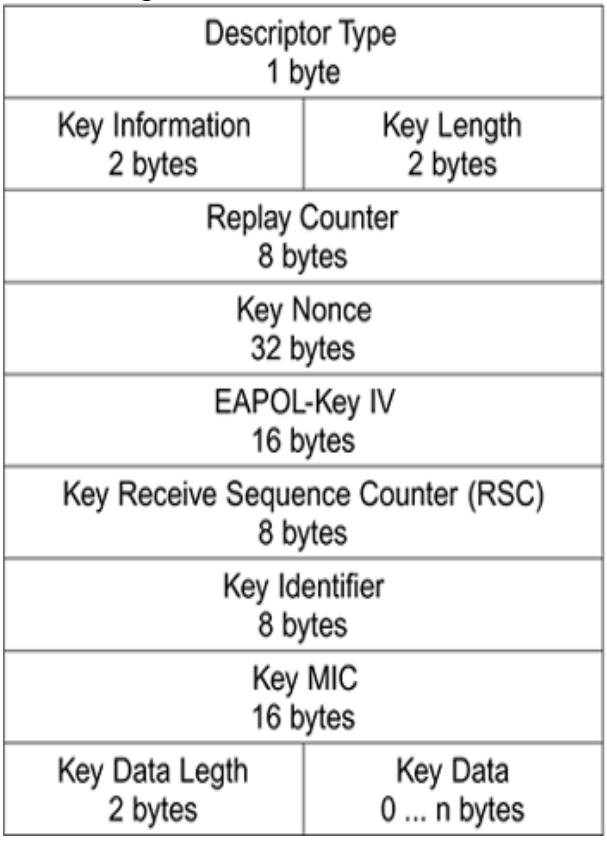
    256: Độ dài mong muốn của PMK



[2] HMAC - Wikipedia

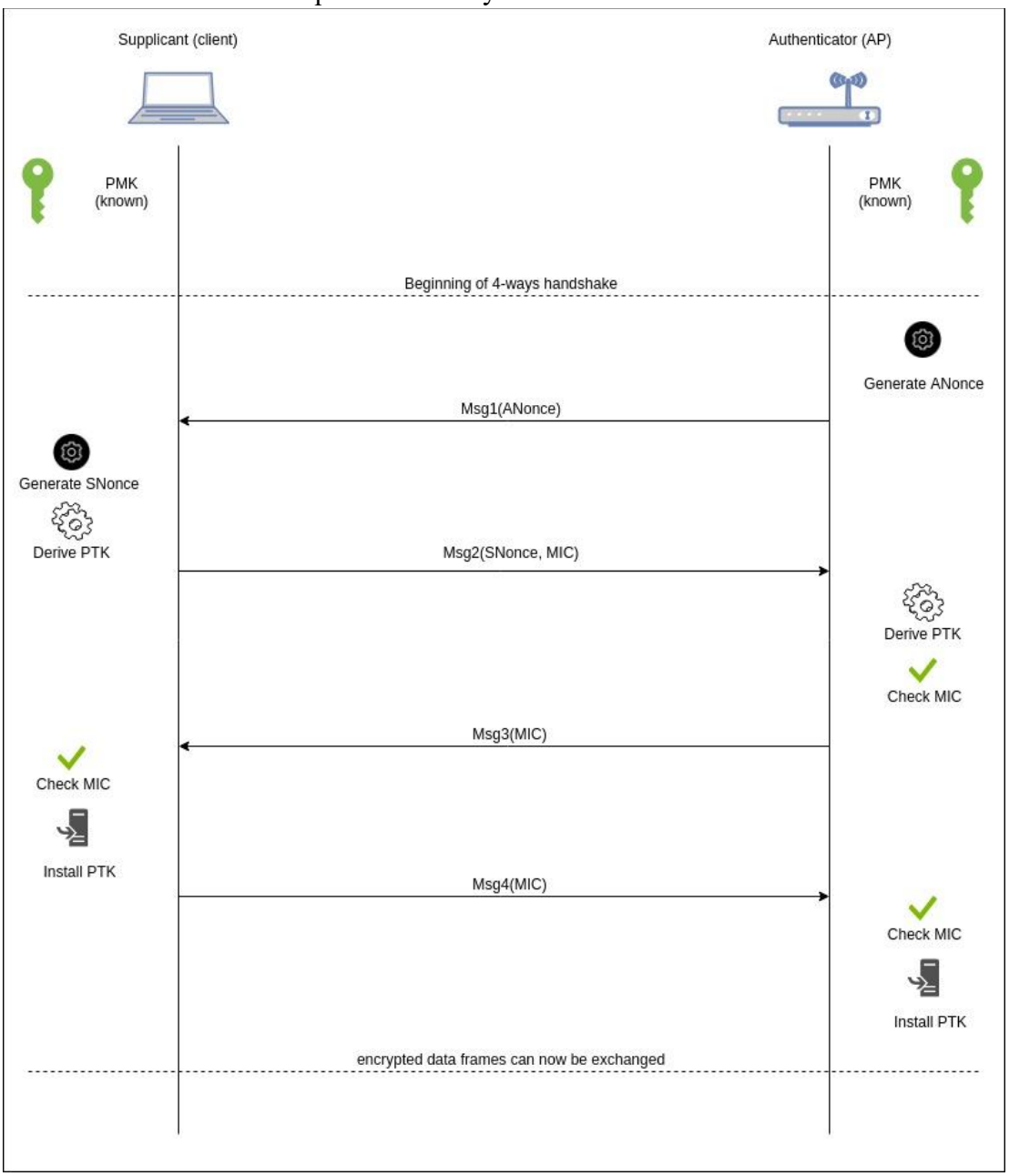
- PKM là sự kết hợp của 256-bit đầu của quá trình tính toán. Quá trình trên được thực hiện một lần bởi tất cả những wireless devices và kể cả AP. Cuối cùng kết quả tính toán sẽ được lưu lại cho đến khi PSK hoặc SSID thay đổi.

- ***Bắt tay bốn bước (4-ways handshake)***
  - Bắt tay bốn bước cung cấp phương thức Authentication qua lại dựa trên Pre-shared Key và PMK và tạo ra một session key mới là PTK (Pairwise Transient Key). PTK được lấy từ PMK, kết hợp với hai số nonces, địa chỉ MAC của cả wireless device và AP.
  - 64-byte của PTK được chia thành:
    - 16-byte Key Confirmation Key (KCK). Được dùng để tính MIC (Message Integrity Check).
    - 16-byte Key Encryption Key (KEK). Được dùng để mã hóa thêm thông tin từ AP đến wirelses device trong suốt quá trình bắt tay.
    - 16-bytes Tempoaral Key (TK). Được sử dụng để mã hóa hoặc giải mã thông tin sau khi quá trình Authenticate kết thúc.
    - 8-byte MIC Authenticator Tx Key (MIC Tx). Được dùng để tính MIC trên các gói tin được truyền đi bởi AP
    - 8-byte MIC Authenticator Rx Key (MIC Rx). Được dùng để tính MIC trên các gói tin được truyền đi bởi wireless device.
  - Trong quá trình diễn ra bắt tay, tất cả các message đều tuân theo EAPOL frame[3]. EAPOL frame có dạng như sau:



[3] Details of Key Derivation for WPA

- Các bước của quá trình bắt tay:



  - AP: Authenticator (AP) sinh ra một số nonce[4] (Authenticator Nonce – ANonce)
  - ***Bước 1:*** Authenticator gửi Anonce đến wireless device. Message này không chứa Message Integrity Code (MIC)
  - Wireless Device: Sinh ra một số nonce (Supplicant Nonce – Snonce)
  - Wireless Device: Lấy ra PTK bằng công thức sau:

PTK = PRF (PMK || Anonce || Snonce || AMAC || SMAC)

Trong đó:

PTK: Pairwise Transient Key.

AMAC: địa chỉ MAC của AP.

SMAC: địa chỉ MAC của Wireless Device.

[4] Nonce Selection

PRF: là Pseudo-Random Function. Trong trường hợp này đối với WPA là SHA-1 và đối với WPA2 là MD5.

||: phép ghép chuỗi.

- ***Bước 2***: Wireless Device gửi message với SNonce (không được mã hóa) và MIC tương ứng. MIC được tính bằng cách sử dụng KCK (16-byte đầu tiên của PTK) bằng cách sử dụng Michael Algorithm[5].
  - AP: Lấy ra PTK bằng công thức trên và SNonce vừa nhận được.
  - AP: Kiểm tra tính toàn vẹn của Snonce bằng MIC.
- ***Bước 3***: Gửi một đoạn message chứa một vài dữ liệu (được mã hóa bằng KEK) và MIC
  - Wireless Device: kiểm tra MIC.
  - Wireless Device: cài đặt PTK
- ***Bước 4***: Wireless Device gửi message chứa MIC. Đay có thể xem là một message để xác nhận.
  - AP: kiểm tran MIC
  - AP: Cài đặt PTK
  - Sau khi quá trình bắt tay kết thúc, tất cả các message phía sau đó sẽ được mã hóa bằng khóa TK trong PTK.

- Cần lưu ý rằng, sau ít nhất 65535 gói tin, PTK sẽ được làm mới, nhưng vì AP và Wireless Device vẫn còn giao tiếp với nhau nên chúng sẽ dùng PTK hiện tại để trao đổi dữ liệu cho quá trình hình thành PTK mới.
- Ví dụ cụ thể 4-ways Handshake[6]

b) WPA-801.1 X:

- 801.1 X là một Giao thức Xác thực mạng (Network Authentication Protocol), giao thức này mở các port kết nối khi một tổ chức muốn xác thực (authenticate) một định danh người dùng (user's identity) và phân quyền (authorize) họ khi kết nối đến mạng. Định danh người dùng được quyết định dựa trên credentials hoặc certificate của họ, mà chúng được xác thực bởi RADIUS Server. RADIUS Server có giao tiếp với dữ liệu của tổ chức thông qua các giao thức LDAP hoặc SAML.
- Chi tiết và cách thức hoạt động của 801.1 X[7]

3. WPA/WPA2 Encryption:

a) TKIP (Temporal Key Integrity Protocol):

- TKIP được đưa ra đời từ bản thảo của tiêu chuẩn IEEE 802.11i nhằm nâng cấp khả năng bảo mật của RC4 vốn đã bị phá vỡ trước đó. Sở dĩ ta phải sử dụng TKIP bởi vì những phần cứng cũ không tương thích với các thuật toán an toàn khác.
- Những tính năng được thêm vào TKIP bao gồm:

  - MIC: một thuật toán kiểm tran tính toàn vẹn của message là Michael, trong đó thêm vào một giá trị hash cho mỗi frame.
  - TIKP sequence counter: cung cấp các bản ghi của các frame được gửi bởi mỗi địa chỉ MAC khác nhau. Mục đích là để ngăn chặn một cuộc tấn công lặp lại (replay attack) bằng các gửi lại các frame đã gửi.
  - Key mixing algorithm: thuật toán tính toán khóa WEP 128-bit duy nhất cho mỗi frame.
  - IV: độ dài từ 24-bit chuyển thành 48-bit.

---

[5] IEEE Std 802.11i. 2004. Amendment 6: Medium Access Control (MAC) Security Enhancements; pp 45, 48, 49.

[6] Details of Key Derivation for WPA phần Four-way Handshake

[7] What is 802.1X? How Does it Work?

    - Timestamp (tạm dịch là dấu thời gian): để ngăn chặn một cuộc tấn công lặp lại.
    - Sender MAC address: MIC bao gồm cả địa chỉ MAC của người gửi. Mục đích nhằm chứng minh ai mới là người thực sự gửi gói tin đó.
  - Tuy vậy TKIP chỉ là giải pháp tạm trước khi IEEE đưa ra bản chính thức của tiêu chuẩn 802.11i. Hiện nay, TKIP chứa nhiều lỗ hổng và nó đã bị "khai tử" từ tiêu chuẩn 802.11-2012.

b) CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol):

- CCMP bao gồm hai thuật toán:
    - AES (sử dụng Counter Mode – CTR)
    - CBC-MAC (Cipher Block Chaining Message Authentication Code): đây là một kĩ thuật tạo ra một message authentication code từ block cipher. Dữ liệu sẽ được mã hóa bởi AES và được tạo thành một chuỗi các khối (chain of block). Block sau phụ thuộc vào sự mã hóa của block ngay phía trước.
- Tuy tính bảo mật cao nhưng nhược điểm của CCMP là phần cứng hỗ trợ xử lý thuật toán AES và CBC-MAC. Chúng ta không thể dùng CCMP cho các phần cứng cũ chỉ hỗ trợ WEP hoặc TKIP.

4. Tài liệu tham khảo:

- Overview TKIP and CCMP: Wireless Encryption and Integrity
- WPA-PKS and how to crack it: How does WPA/WPA2 WiFi security work, and how to crack it?
- Type of wireless encryption: What are WPA-PSK/WPA2-PSK, TKIP and AES?