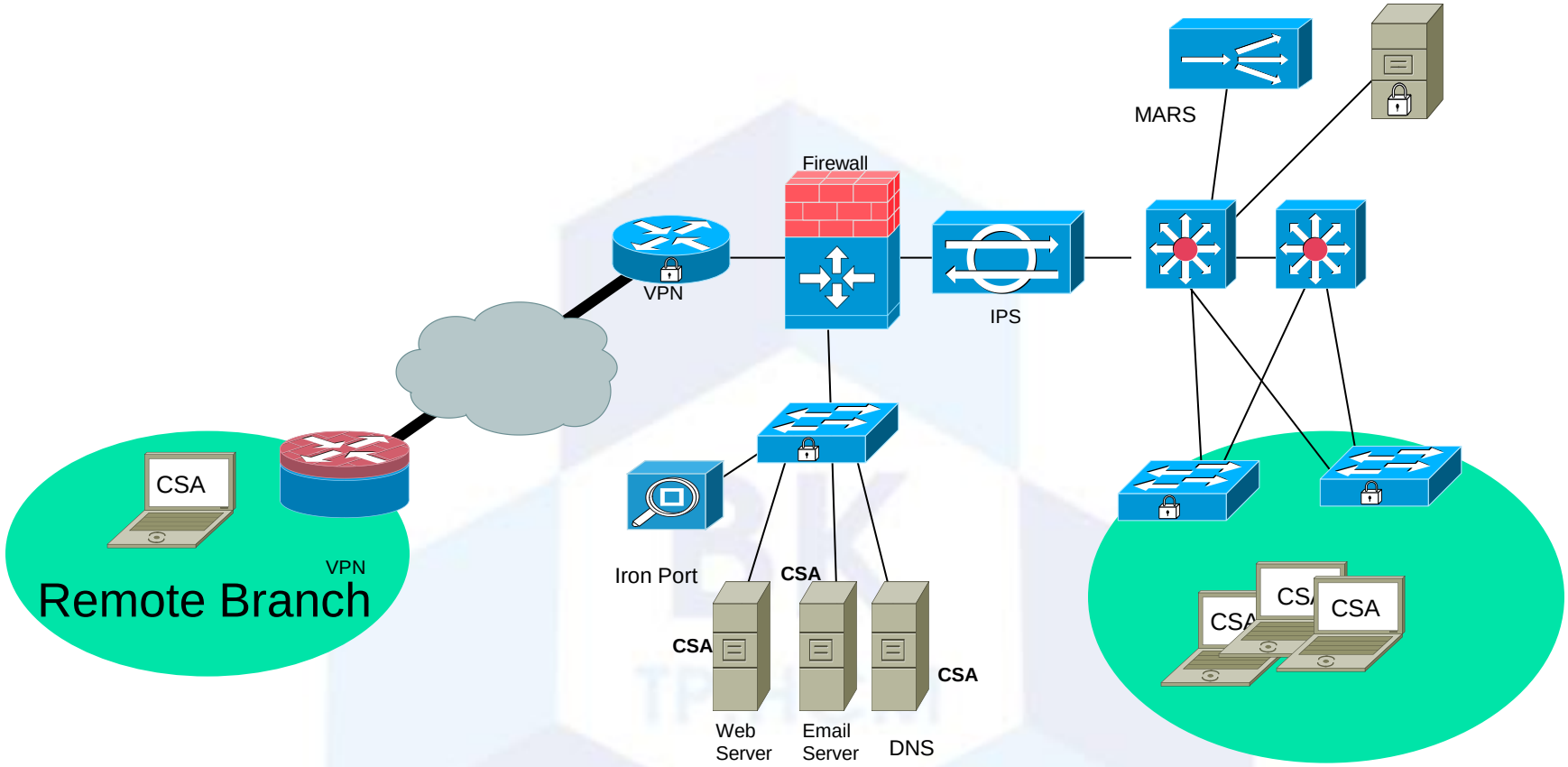
CHƯƠNG V
TRUYỀN THÔNG VÀ GIAO THỨC XÁC THỰC AN TOÀN

ThS. Nguyễn Cao Đạt
E-mail: dat@hcmut.edu.vn

NỘI DUNG TRÌNH BÀY

- **Truyền thông an toàn**
- **Giao thức xác thực an toàn**

TRUYỀN THÔNG AN TOÀN



- Thông điệp trao đổi giữa các vị trí phải được bảo mật
- Đảm bảo thông điệp không bị thay đổi, giả mạo hoặc giải mã khi bị chặn

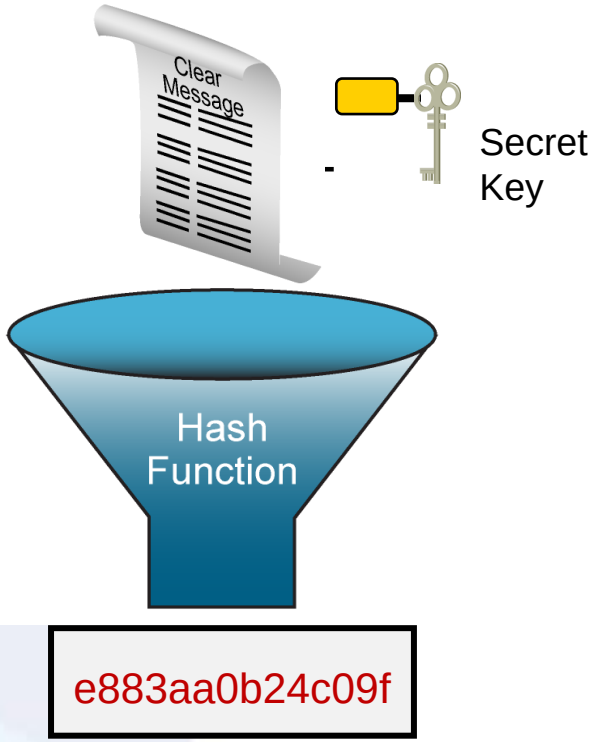
TRUYỀN THÔNG AN TOÀN

- Không thể thay đổi ~ toàn vẹn thông điệp
- Không thể giả mạo ~ xác thực thông điệp
- Không thể giải mã(an toàn với phân tích mã)

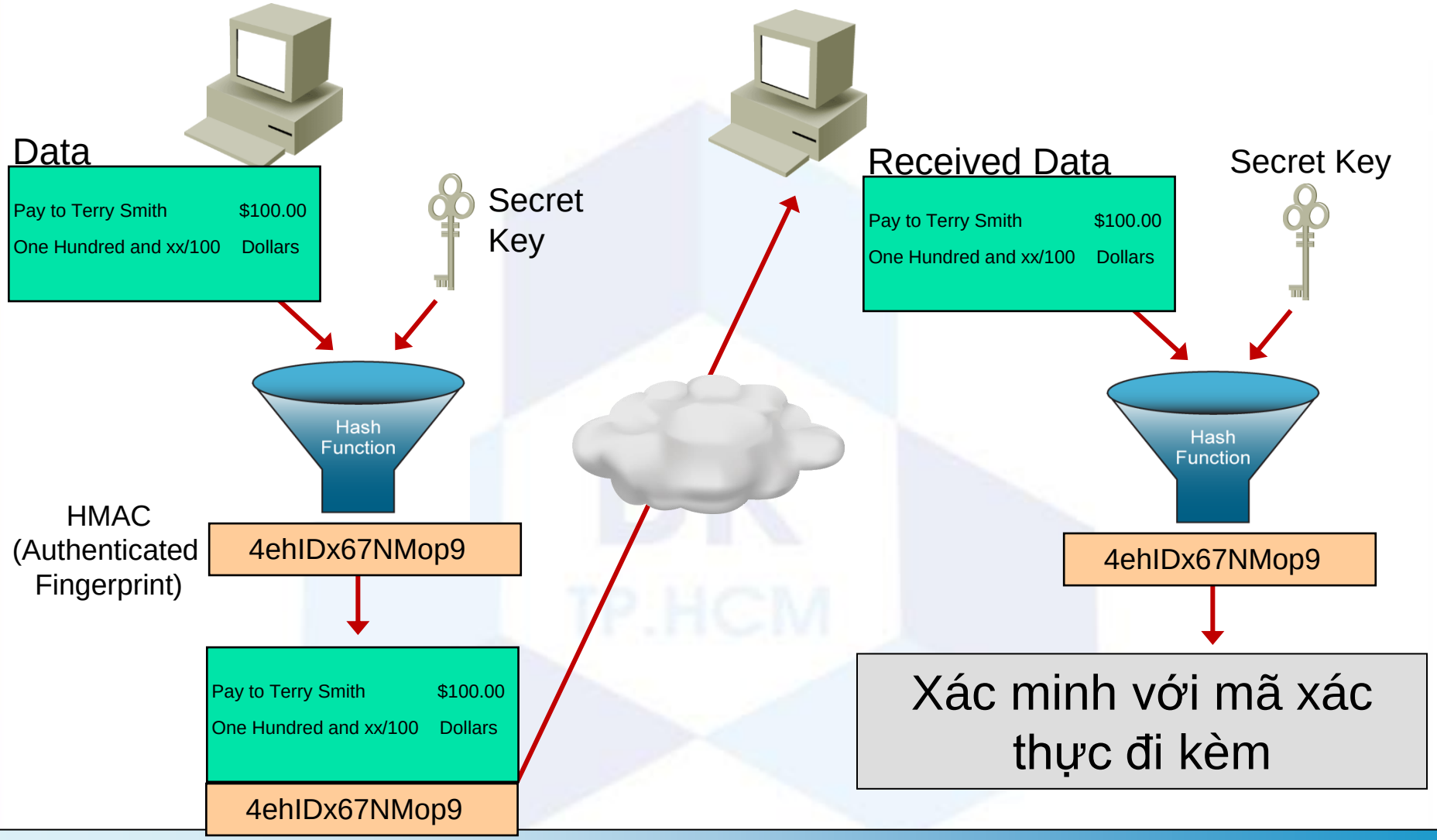
Toàn ven	Xác thực	Bí mật
MD5 SHA-1 SHA-2	HMAC-MD5 HMAC-SHA-1 RSA và DSA	DES 3DES AES RSA

HMAC (Hash Based Message Authentication Code)

- Sử dụng một khóa bí mật bổ sung.
- Khóa bí mật được người gửi và người nhận biết.
- Thêm xác thực để đảm bảo tính toàn vẹn.
- Đánh bại các cuộc tấn công trung gian.
- Dựa trên các hàm băm hiện có như MD5 và SHA-1.

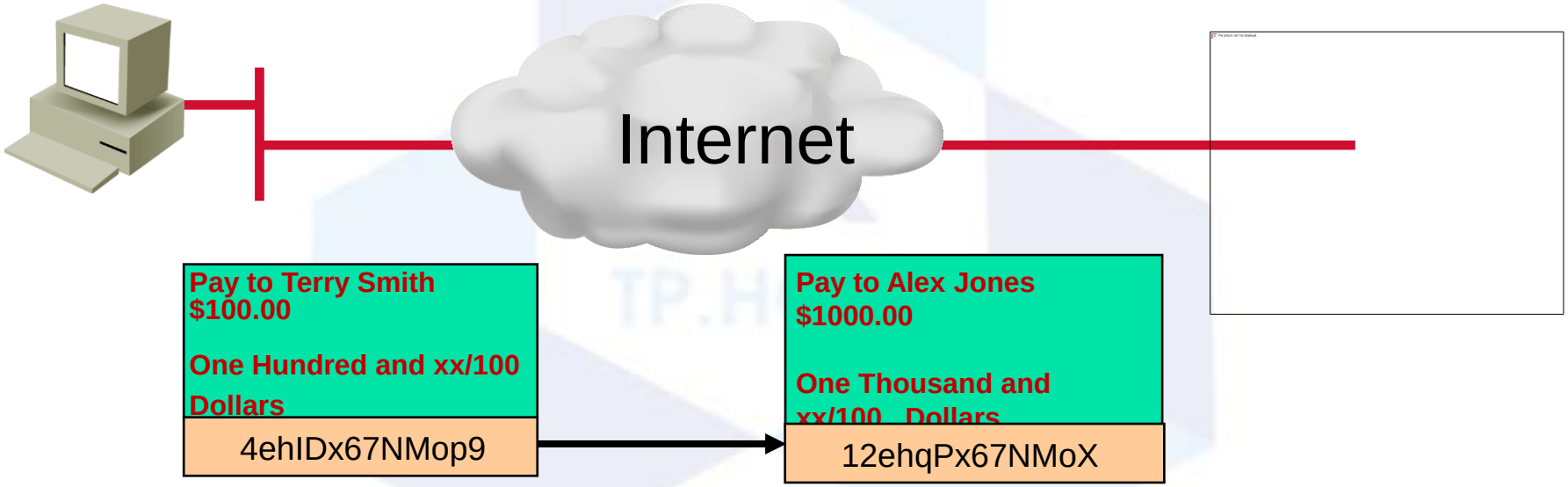


VÍ DỤ SỬ DỤNG HMAC



LƯU Ý VỀ HÀM BĂM

- Sử dung hàm băm không an toàn dẫn đến nguy cơ bị tấn công trung gian(man in the midle attack)
- SHA-224, SHA-256, SHA-384 và SHA-512 là mới hơn và là các phiên bản an toàn hơn của SHA và được biết như là SHA-2.

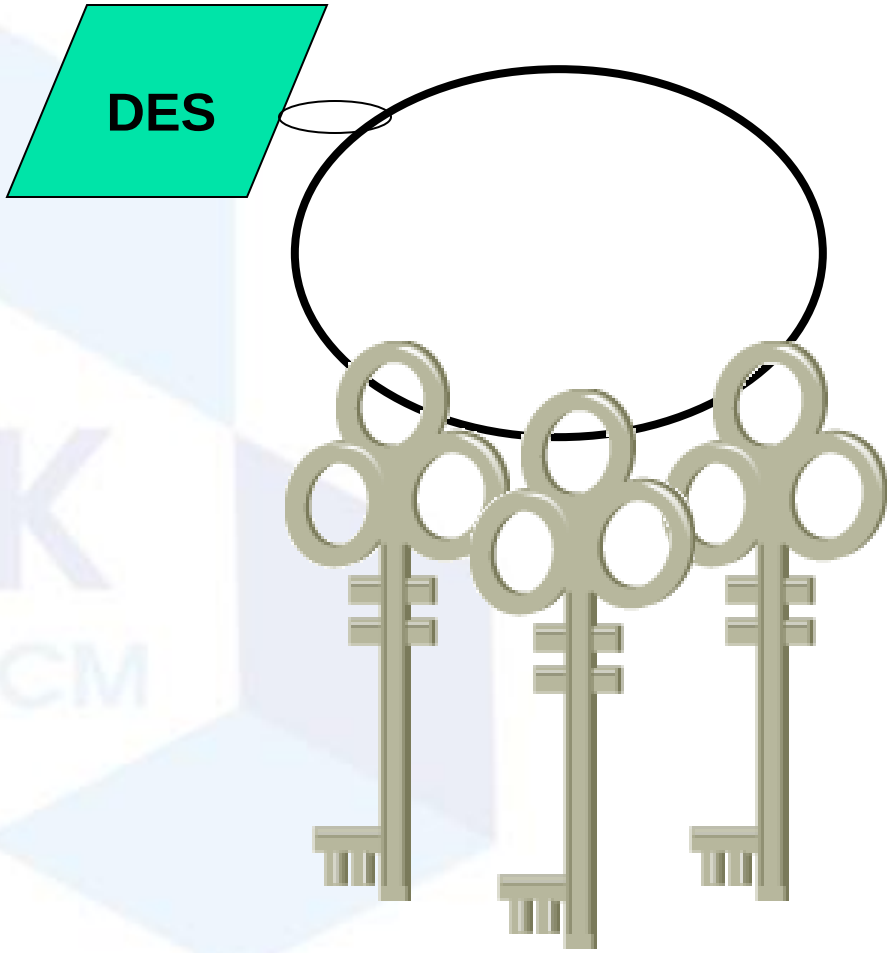


LỰA CHỌN THUẬT TOÁN MÃ HÓA ĐỐI XỨNG

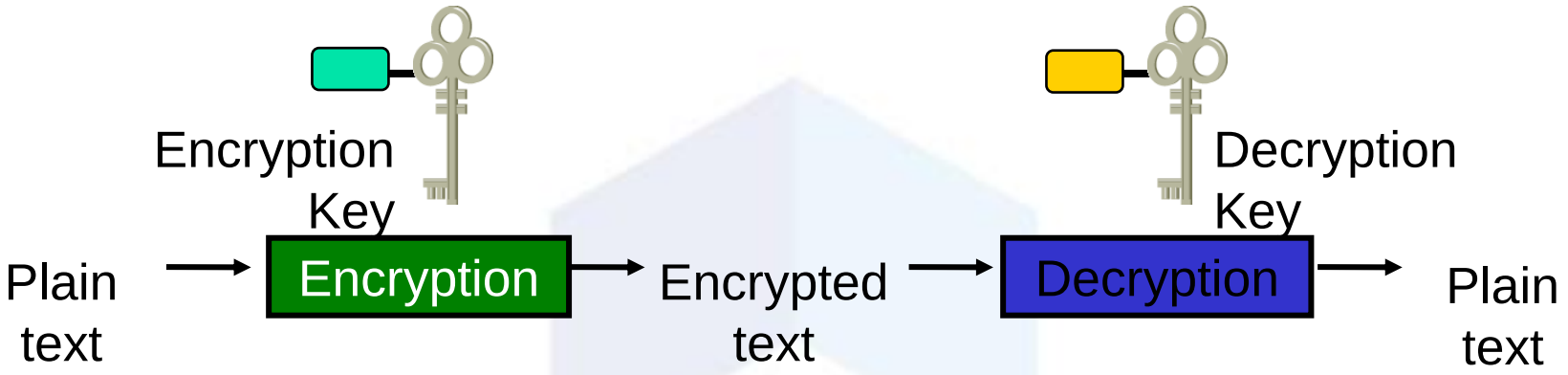
	DES	3DES	AES
Thuật toán được cộng đồng mật mã tin tưởng	Không	Đúng	Vẫn còn đang kiểm chứng
Thuật toán chống lại được tấn công vét cạn (brute-force attack)	Không	Đúng	Đúng

KHI BUỘC PHẢI SỬ DỤNG DES

- Thay đổi khóa thường xuyên để chống tấn công brute-force.
- Dùng một kênh an toàn để gởi khóa đến bên nhận.
- Xem xét dùng DES trong chế độ hoạt động CBC.
- Thử một khóa có yếu hay không trước khi sử dụng



LƯU Ý KHI DÙNG MÃ HÓA KHÓA CÔNG KHAI



- Khóa có chiều dài lớn hơn hay bằng 1024 bits là có thể tin tưởng.
- Khóa có chiều dài nhỏ hơn 1024 bits là không đáng tin cậy cho hầu hết các thuật toán.

NỘI DUNG TRÌNH BÀY

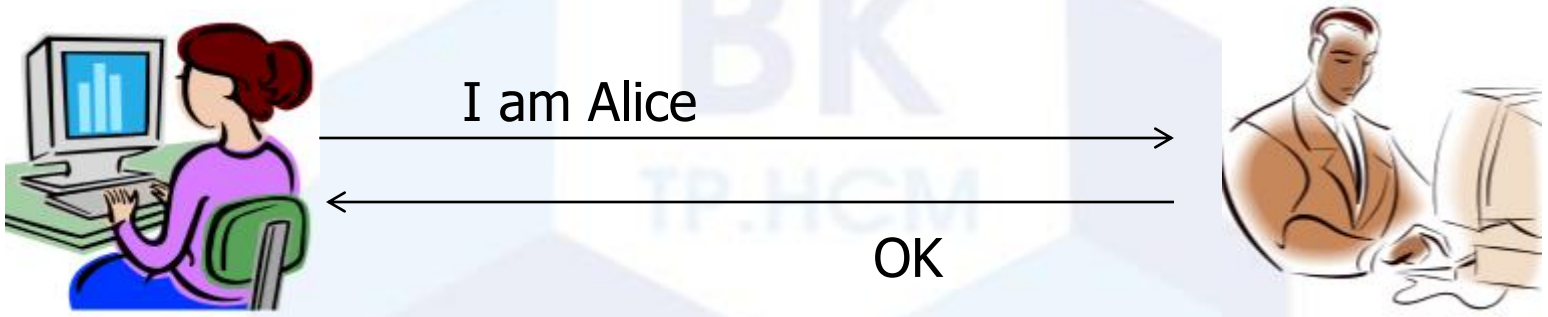
- Truyền thông an toàn
- Giao thức xác thực an toàn

GIAO THỨC XÁC THỰC

- **Xác thực là quá trình một thực thể cung cấp thông tin để chứng minh mình là ai.**
- **Phương pháp xác thực**
  - Những gì bạn biết
  - Những gì bạn có
  - Những gì là chính bạn
- **Một phương pháp xác thực tốt là phương pháp mà không dễ bị đoán hoặc bị làm giả.**

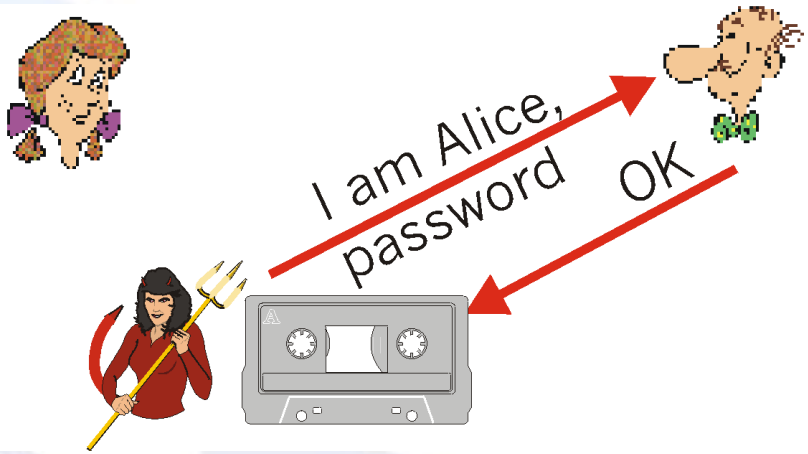
GIAO THỨC XÁC THỰC

- **Giao thức xác thực**
  - Cách thức một đối tác xác thực đối tác còn lại khi hai bên thực hiện trao đổi thông tin trên mạng.
  - Quá trình xác thực chỉ dựa duy nhất vào những thông điệp và dữ liệu được trao đổi.



GIAO THỨC XÁC THỰC

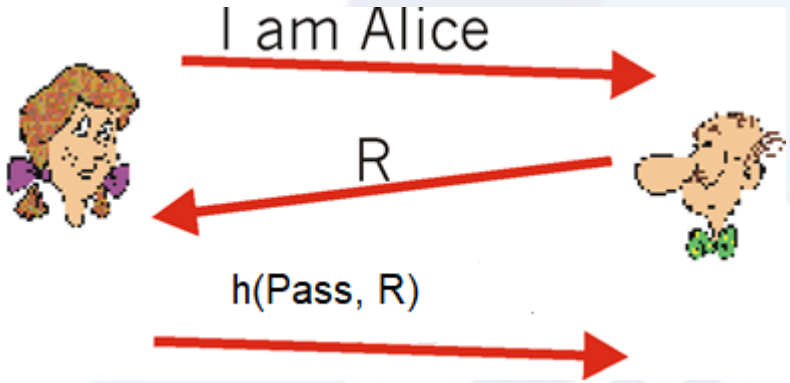
- **Giao thức xác thực dựa trên mật khẩu**
  - PAP – Password Authetication Protocol



  - Nghe lén mật khẩu của Alice.
  - Giả mạo Alice.
- **Mật khẩu được hash hay mã hóa trước khi gửi cũng không an toàn**
  - Tấn công lặp lại (replay attack).

GIAO THỨC XÁC THỰC

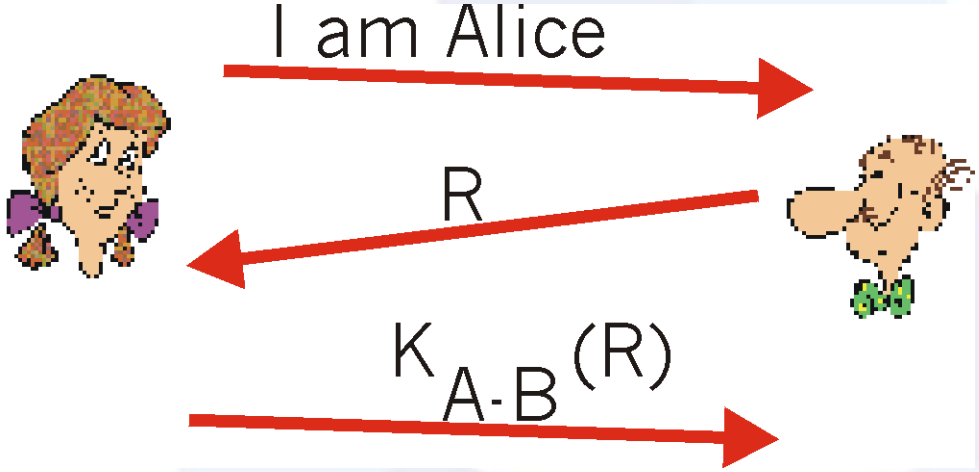
- **Giao thức xác thực thách thức và đáp ứng**
  - Dùng một số Nonce (Number used Once in-a-lifetime)
  - Số Nonce sẽ được sử dụng để tạo mã xác thực của mật khẩu



  - Nhược điểm: Bob phải biết mật khẩu của Alice
  - Không an toàn vì tấn công xen giữa(MITM - man in the midle attack)

GIAO THỨC XÁC THỰC

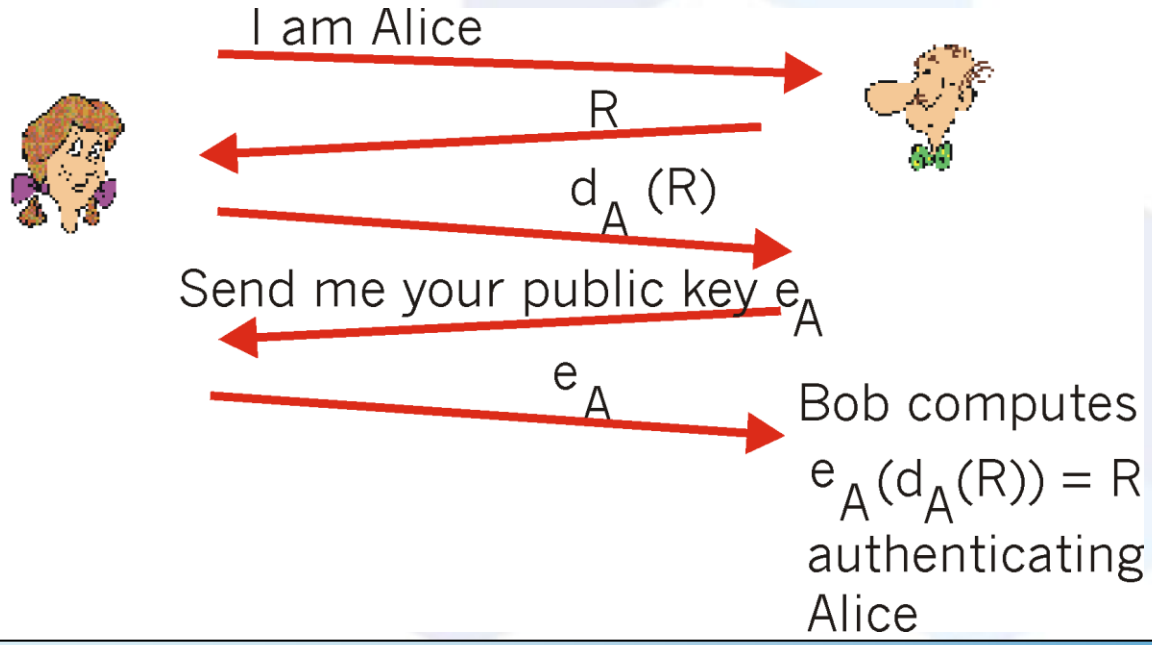
- **Giao thức xác thực dùng mã hóa đối xứng**
  - Dùng một số Nonce
  - Có một khóa K được chia xẻ giữa hai bên
  - Số Nonce sẽ được mã hóa đối xứng bằng khóa K



  - Nhược điểm: Bob xác minh được Alice nhưng Alice không xác minh được Bob.

GIAO THỨC XÁC THỰC

- **Giao thức xác thực dùng mã hóa khóa công khai**
  - Dùng một số Nonce
  - Số Nonce sẽ được mã hóa bằng khóa riêng của Alice

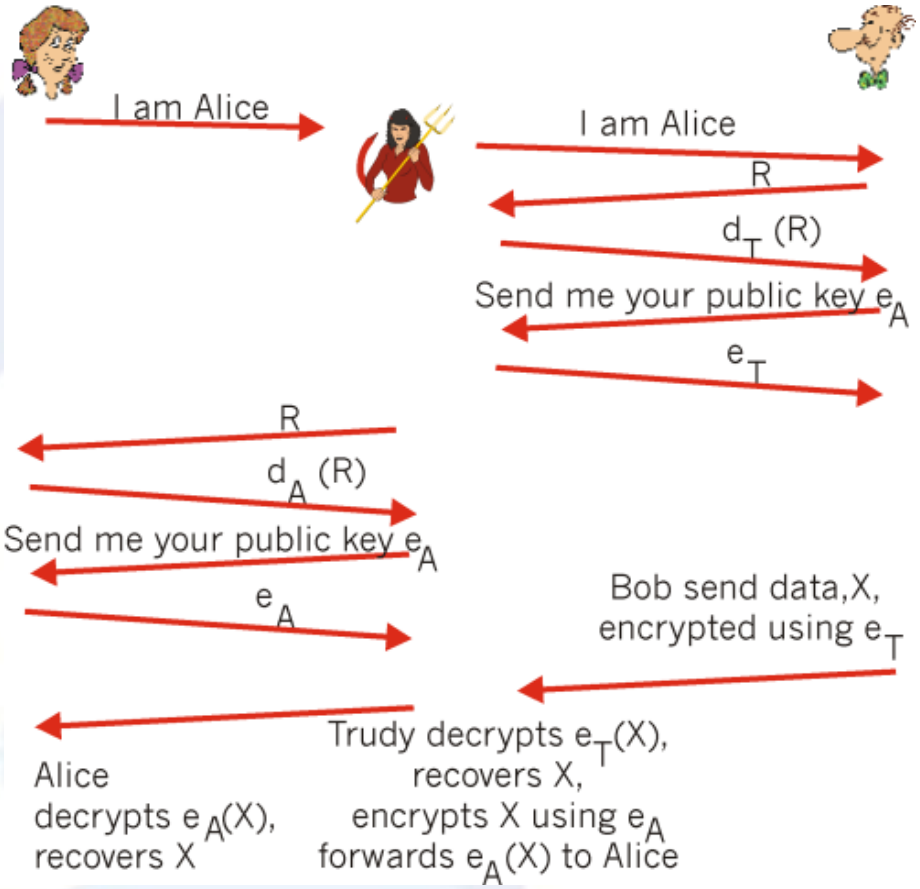


GIAO THỨC XÁC THỰC

- **Giao thức xác thực dùng mã hóa khóa công khai**
  - 

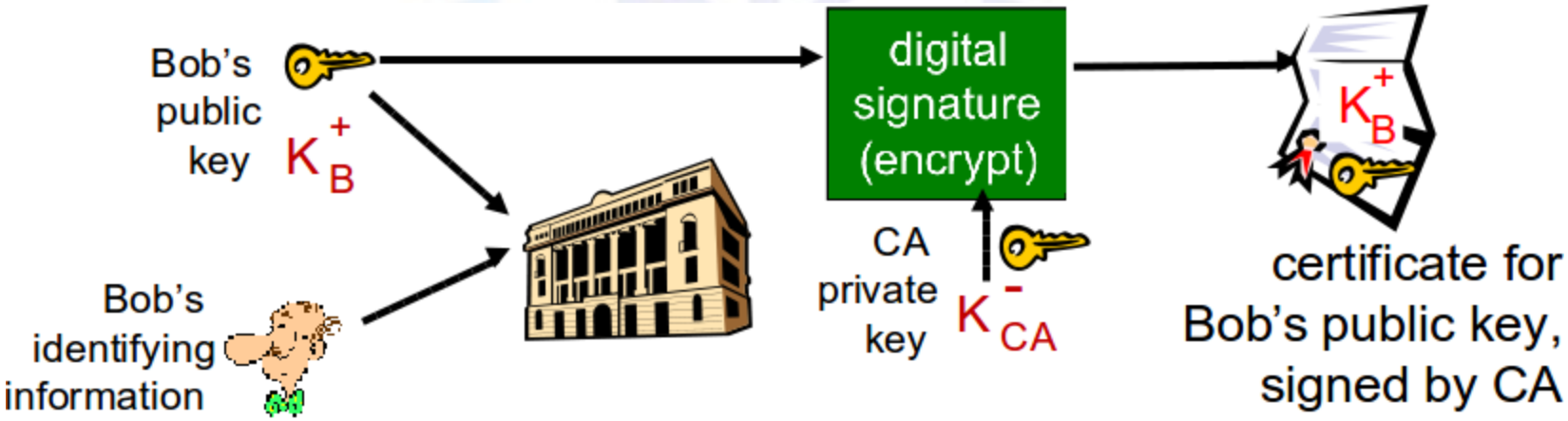
GIAO THỨC XÁC THỰC

- **Giao thức xác thực dùng mã hóa khóa công khai**
  - Không an toàn vì tấn công xen giữa



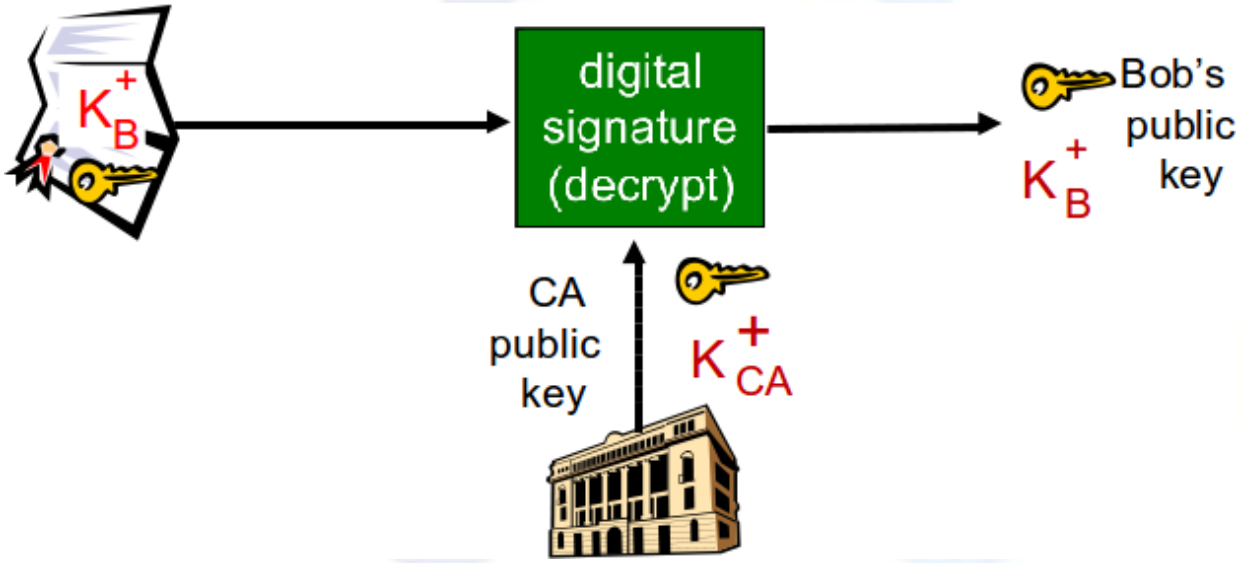
CHỐNG TẤN CÔNG XEN GIỮA

- **Dùng chứng chỉ khóa công khai**
  - Bob cung cấp "bằng chứng về định danh" đến CA(**certification authority)**.
  - CA tạo chứng chi ràng buộc với khóa công khai của Bob.
  - Chứng chỉ chứa khóa công khai của Bob được ký bởi CA, tương ứng CA nói rằng đây là khóa công khai của Bob



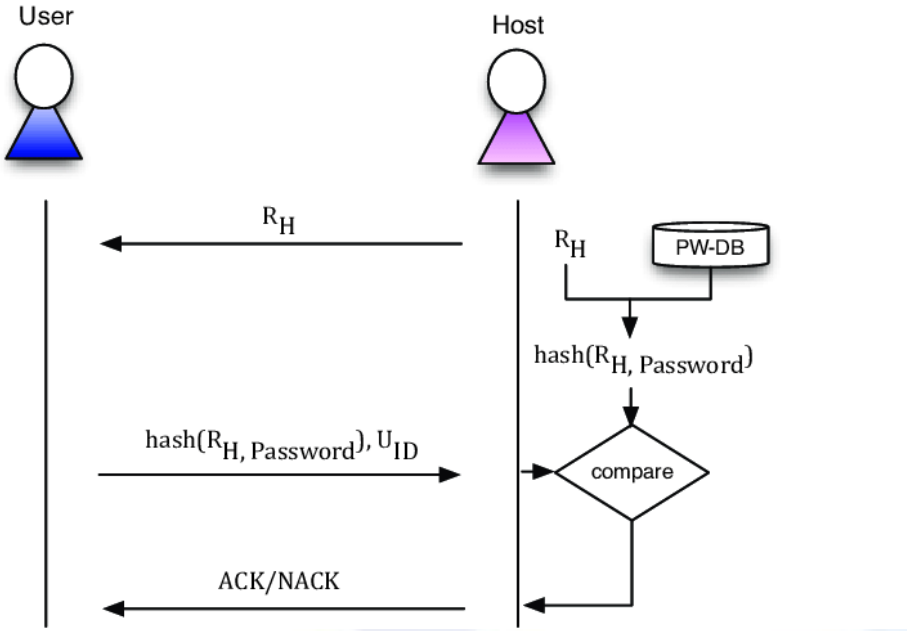
CHỐNG TẤN CÔNG XEN GIỮA

- **Khi Alice muốn khóa công khai của Bob**
  - Lấy chứng chỉ của Bob (từ bất cứ nơi đâu hoặc là Bob gửi)
  - Dùng khóa công khai của CA để giải mã và lấy ra khóa công khai của Bob



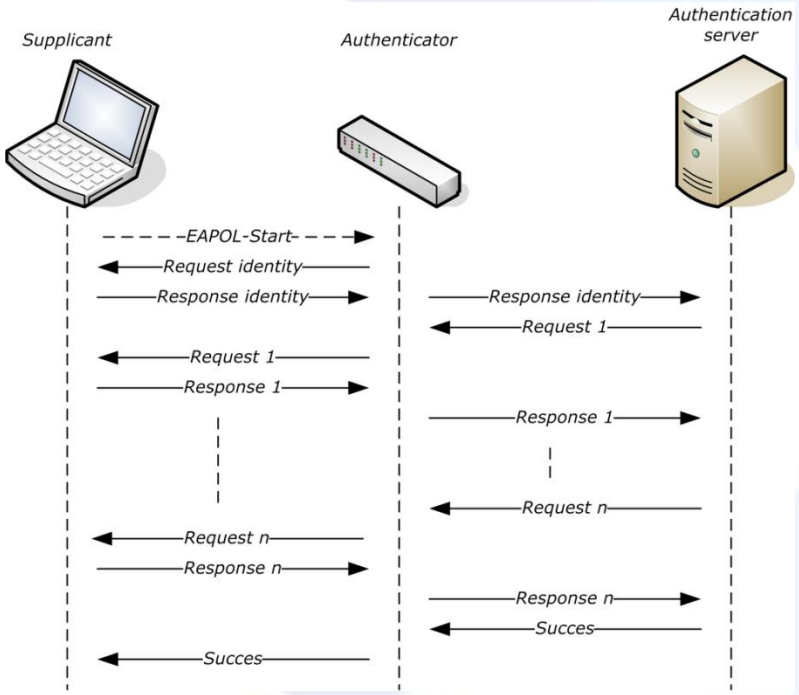
GIAO THỨC XÁC THỰC AN TOÀN

- **CHAP**
  - Challenge-handshake authentication protocol
  - Dùng giao thức xác thực mã hóa đối xứng
  - Số nonce thường có chiều dài 128 bits.



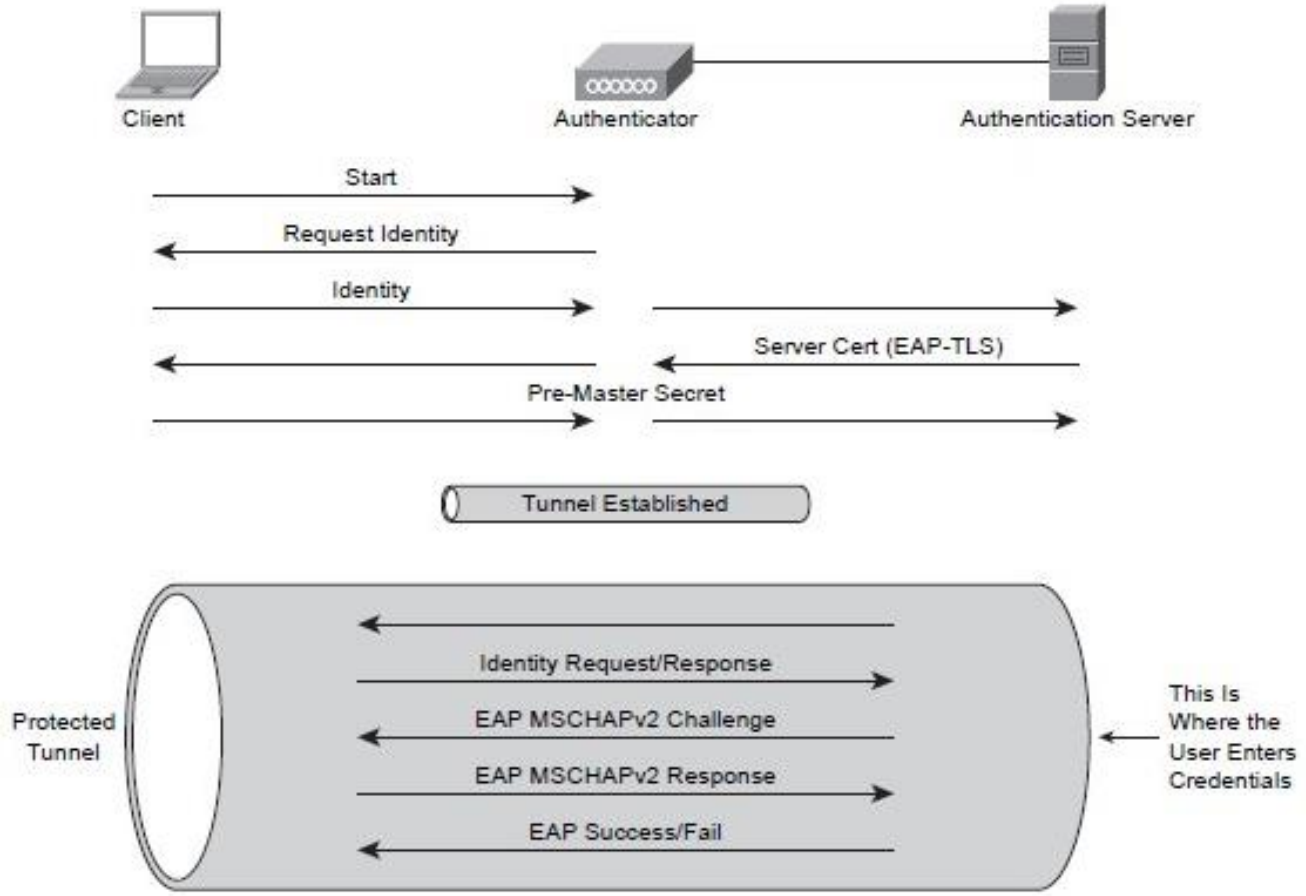
GIAO THỨC XÁC THỰC AN TOÀN

- **EAP**
  - Extensible Authentication Protocol
  - Được sử dụng rộng rãi vì nó là một khung làm việc tổng quát
  - EAP-MD5, EAP-TLS, EAP-FAST, EAP-PEAP, ..



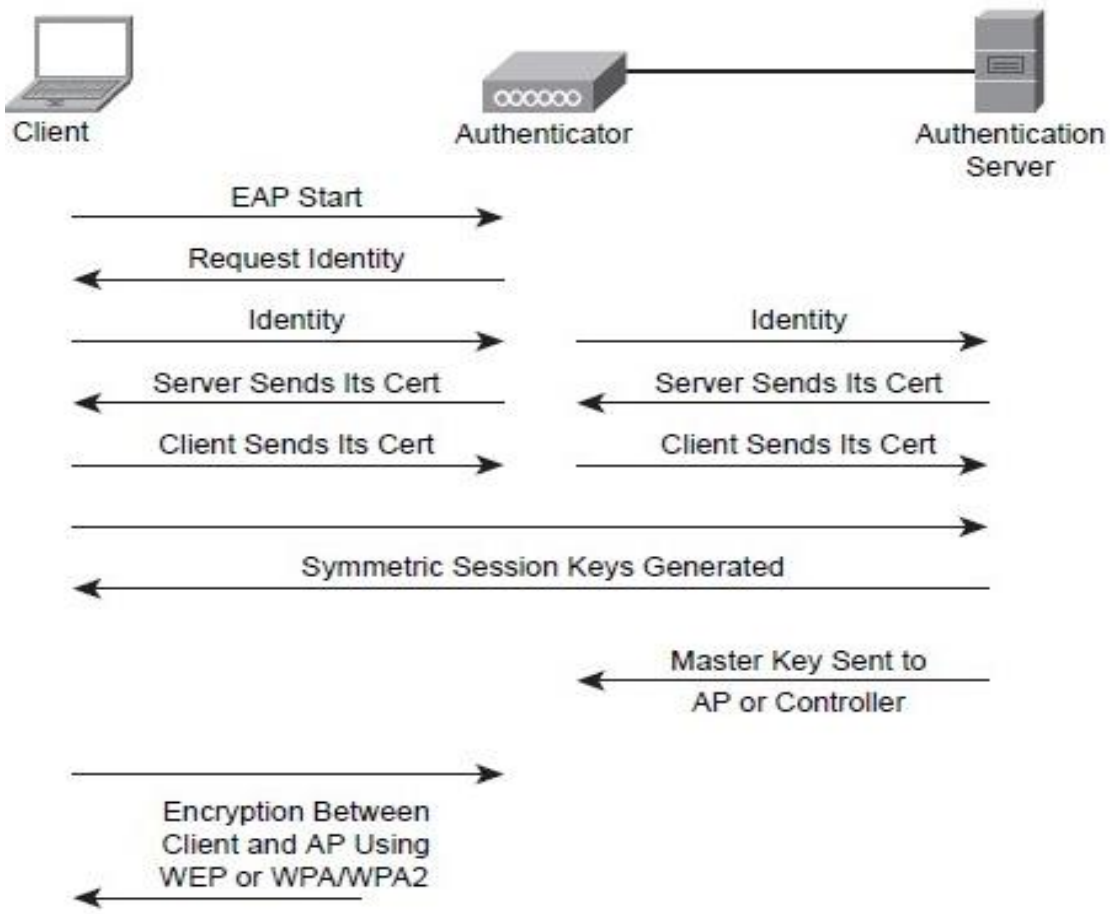
PEAP

- **Protected Extensible Authentication Protocol**



EAP-TLS

- **EAP - Transport Layer Security**



PEAP, EAP-TLS, EAP-TTL

Feature	TLS	TTLS	PEAP
Server-side certificate	Required	Required	Required
Client-side certificate	Required	Not required	Not required
Deployment difficulty	Very difficult (due to client certificate deployment)	Moderate	Moderate
Wi-Fi security	Very high	High	High

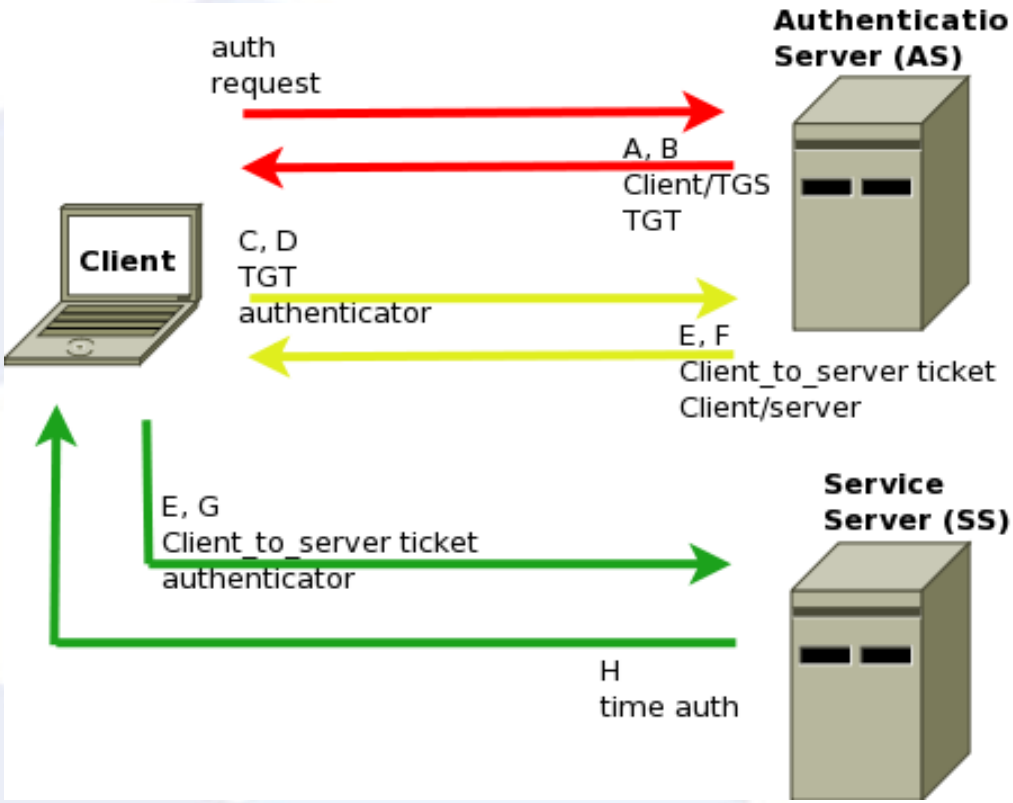
GIAO THỨC AN TOÀN VÀ MẬT KHẨU

	Clear-text	NT hash (ntlm_auth)	MD5 hash	Salted MD5 hash	SHA1 hash	Salted SHA1 hash	Unix Crypt
PAP	✓	✓	✓	✓	✓	✓	✓
CHAP	✓	x	x	x	x	x	x
Digest	✓	x	x	x	x	x	x
MS-CHAP	✓	✓	x	x	x	x	x
PEAP	✓	✓	x	x	x	x	x
EAP-MSCHAPv2	✓	✓	x	x	x	x	x
Cisco LEAP	✓	✓	x	x	x	x	x
EAP-GTC	✓	✓	✓	✓	✓	✓	✓
EAP-MD5	✓	x	x	x	x	x	x
EAP-SIM	✓	x	x	x	x	x	x
EAP-TLS	x	x	x	x	x	x	x

- Tham khảo: http://deployingradius.com/documents/protocols/compatibility.html

GIAO THỨC XÁC THỰC AN TOÀN KHÁC

- **Một số giao thức an toàn khác**
  - Radius (AAA)
  - Kerberos
  - OpenID
  - SAML
  - …



RADIUS

- Remote Authentication Dial-In User Service
- AAA(Authentication, Authorization, Accounting)

Kerberos

- **Một dịch vụ xác thực được phát triển như một phần trong dự án Athena ở MIT**
- **Một dịch vụ xác thực tập trung trong một môi trường mạng phân bố**
  - Xác thực người dùng trên các dịch vụ và ngược lại
  - Cho phép người dùng truy cập đến các dịch vụ được phân bố trên mạng
  - Hiện thực dựa trên mã hóa đối xứng, không dùng mã hóa khóa công khai
- **Hai phiên bản đang sử dụng là v.4 & v.5**

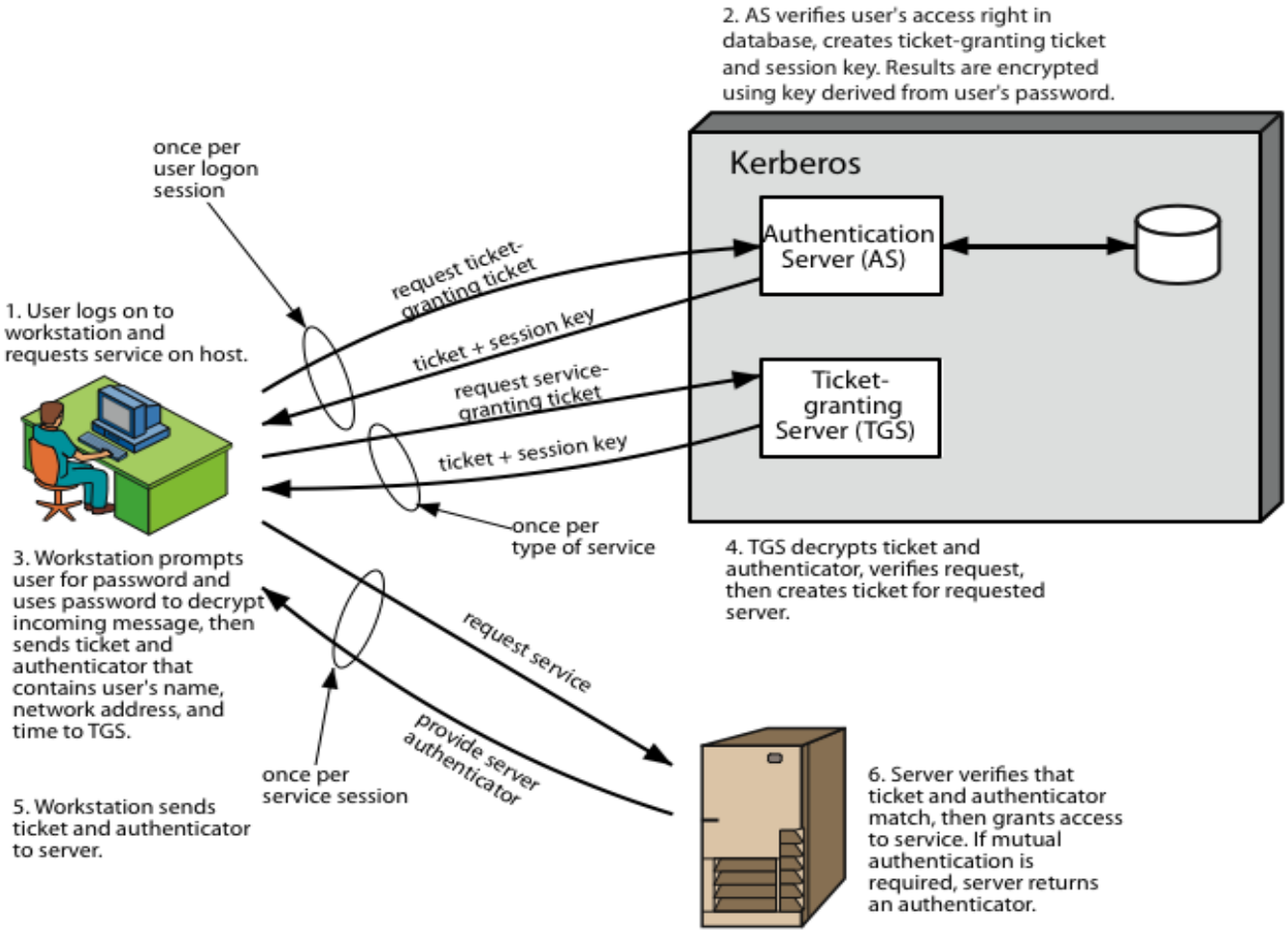
Sơ lược về phiên bản Kerberos 4

- **Một lược đồ xác thực dựa trên bên thứ ba**
- **Authentication Server (AS)**
  - Người dùng đàm phán với AS để xác định mình
  - Nếu thành công AS cấp một vé được gọi là TGT(Ticket Granting Ticket)
- **Ticket Granting Server (TGS)**
  - Sau đó người dùng có thể truy cập đến các dịch vụ khác từ TGS dựa trên TGT của người dùng.

Các pha trong Kerberos 4

- **Lấy TGT từ AS**
  - Một TGT trên một người
- **Lấy SGT(service granting ticket) từ TGT**
  - Cho từng dịch vụ riêng biệt
- **Trao đổi client/server để có được dịch vụ**
  - Trên tất cả yêu cầu dịch vụ

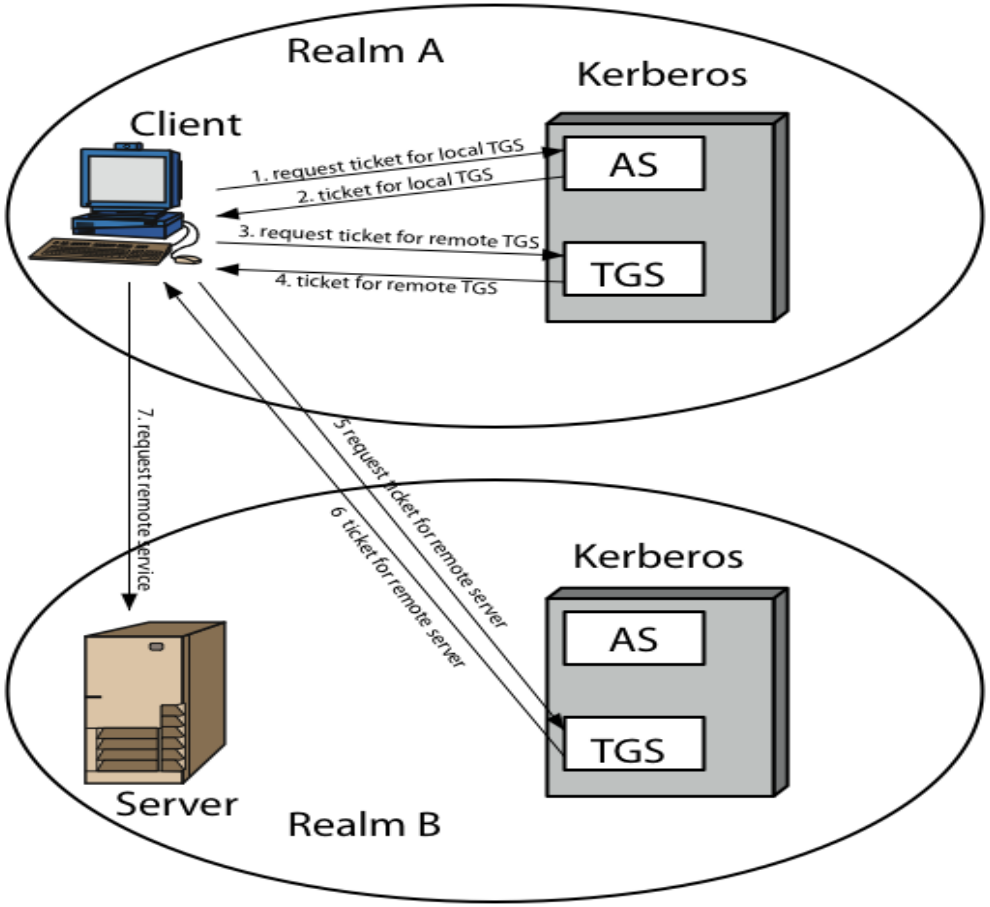
Các pha trong Kerberos 4



Miền quản trị Kerberos

- **Thuật ngữ sử dụng là Realm**
- **Môi trường Kerberos bao gồm**
  - Một Kerberos server
  - Một số lượng máy trạm, tất cả đều đăng ký với Kerberos server
  - Các máy chủ chia sẻ khóa với Kerberos server
- **Nếu có nhiều miền quản trị, các Kerberos server sẽ phải chia sẻ khóa và tin tưởng lẫn nhau**

Miền quản trị Kerberos



Phiên bản Kerberos 5

- **Đặc tả với chuẩn Internet RFC 1510**
- **Cung cấp các cải tiến dựa trên phiên bản 4**
  - Các hạn chế về môi trường
    - Thuật toán mã hóa, giao thức mạng, thứ tự byte trong thông điệp, thời gian sống của vé, chuyển tiếp xác thực, xác thực liên miền.
  - Các thiếu sót về kỹ thuật
    - Mã hóa hai lần, dùng chế độ mã hóa không chuẩn, khóa phiên, tấn công trên mật khẩu.

OpenID

- OpenID là một tiêu chuẩn mở (open standard) dùng cho việc xác thực người dùng không tập trung.
- Thông qua các nhà cung cấp dịch vụ OpenID còn được gọi là OpenID provider (như Google, Facebook, Twitter...).
- Tham khảo:
  - https://aita.gov.vn/tieu-chuan-loi-ket-noi-openid-phan-1
  - https://aita.gov.vn/tieu-chuan-loi-ket-noi-openid-phan-2

TÓM TẮT

- Truyền thông an toàn đảm bảo thông điệp trao đổi giữa các vị trí phải được bảo mật, không bị thay đổi, giả mạo hoặc giải mã khi bị chặn. Đòi hỏi phải dùng các thuật toán hiện đại và cập nhật thường xuyên.
- Giao thức xác thực là cách thức một đối tác xác thực đối tác còn lại khi hai bên thực hiện trao đổi thông tin trên mạng. Quá trình xác thực chỉ dựa duy nhất vào những thông điệp và dữ liệu được trao đổi. Giao thức xác thực đưa vào sử dụng phải là giao thức xác thực an toàn.