Mật mã và An ninh mạng

- **Giờ học**: 07h00 ~ 09h25; 12h30 ~ 14h55 ; 15h00 ~ 17h25
- **Phòng học**: H.A10-1003; H.A9-303; H.A9-305
- **Tín chỉ**: 3
- **Giảng viên**: Hoàng Đắc Thắng
- **ĐT**: 0965148378

Mô tả học phần

Học phần cung cấp các kiến thức, nguyên lý cơ sở về:

- Khái niệm mang tính chất cơ sở của lĩnh vực an toàn thông tin và mạng.
- Mật mã đối xứng hiện đại và sơ đồ mã hóa khối tổng quát Feistel.
- Mật mã liên hợp nhiều khối và cách thức chung quản lý các khóa bí mật.
- Bảo mật, chữ ký số, và trao đổi khóa bí mật của mật mã khóa công khai.
- Các cơ chế xác thực thông báo và tác giả của thông báo.
- Các ứng dụng của mật mã, xác thực và chữ ký số.

Quy định về tham dự lớp học

- ✓ Tham dự đầy đủ các buổi học. Trong trường hợp nghỉ học do lý do bất khả kháng thì phải có giấy tờ chứng minh đầy đủ và hợp lý.
- ✓ Vắng quá 50% buổi học dù có lý do hay không có lý do đều bị coi như không hoàn thành khóa học và phải đăng ký học lại vào học kỳ sau.
- ✓ Vào trễ quá 15 phút sau khi giờ học bắt đầu sẽ không được tham dự buổi học.
- ✓ Tuyệt đối không làm ồn, gây ảnh hưởng đến người khác.
- ✓ Tuyệt đối không được ăn uống, nhai kẹo cao su, sử dụng các thiết bị như điện thoại, máy nghe nhạc trong giờ học.

Cách tính điểm

✓ Điểm quá trình: 40%

- Kiểm tra thường xuyên: Hệ số 1
- Kiểm tra định kỳ lần 1: Hệ số 2
- Kiểm tra định kỳ lần 2: Hệ số 2
- Kiểm tra định kỳ lần 3: Hệ số 2
- Kiểm tra chuyên cần: Hệ số 3

✓ Điểm thi kết thúc học phần: 60%

Tài liệu

1. Tài liệu học tập:

[1]. Nguyễn Thu Hiền, Đào Thụy Ánh, Phạm Minh Thái, Ngô Quang Trí, Tài liệu học tập An toàn thông tin, Khoa CNTT, Trường Đại học Kinh tế - Kỹ thuật Công nghiệp, 2023. (Lưu hành nội bộ).

2. Tài liệu tham khảo:

[2]. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education, Inc, 2014.

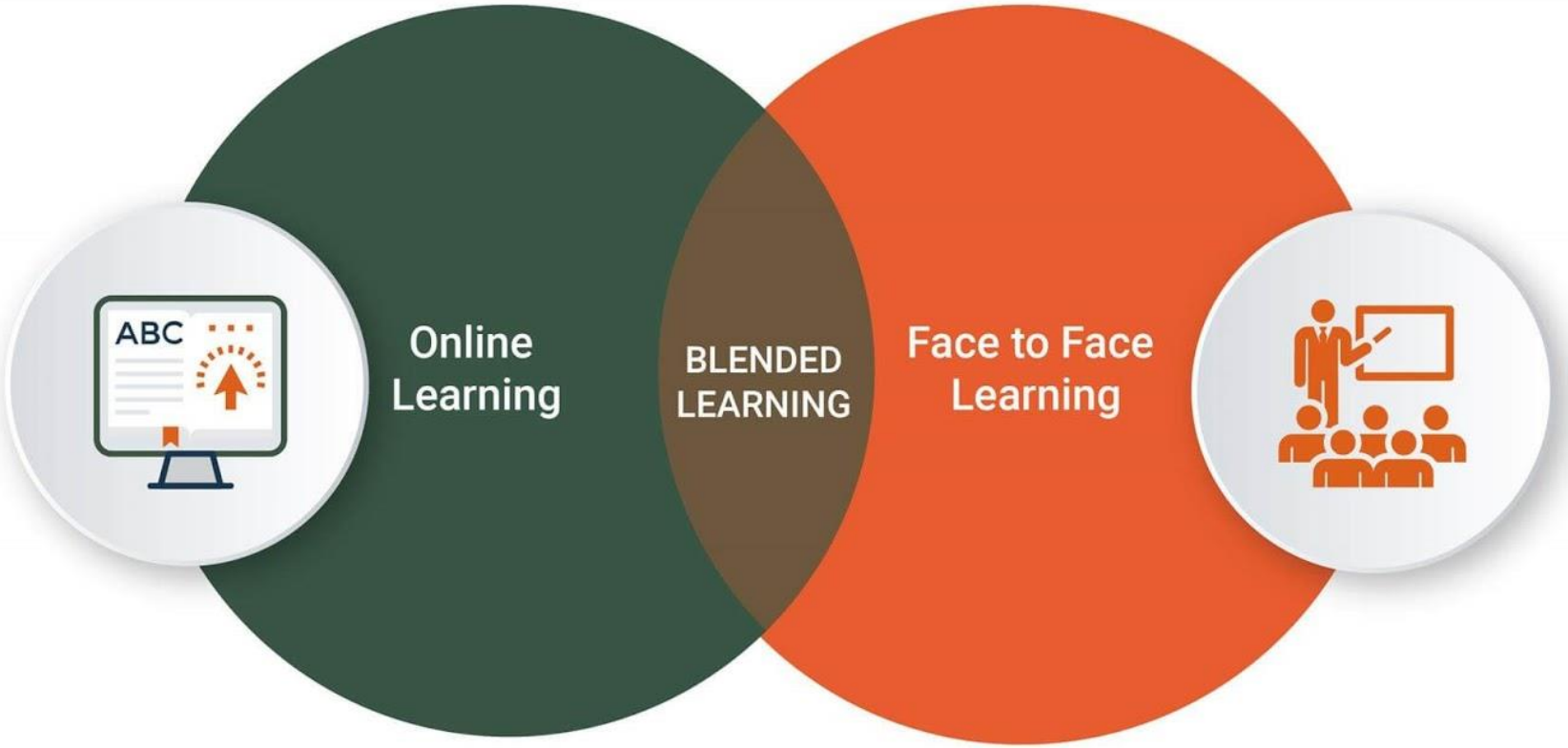
[3]. TS Lê Văn Phùng, *An toàn thông tin*, NXB TT & Truyền Thông, 2018.

[4]. Nguyễn Khanh Văn, *Giáo trình cơ sở An toàn thông tin*, NXB Bách Khoa, 2015.

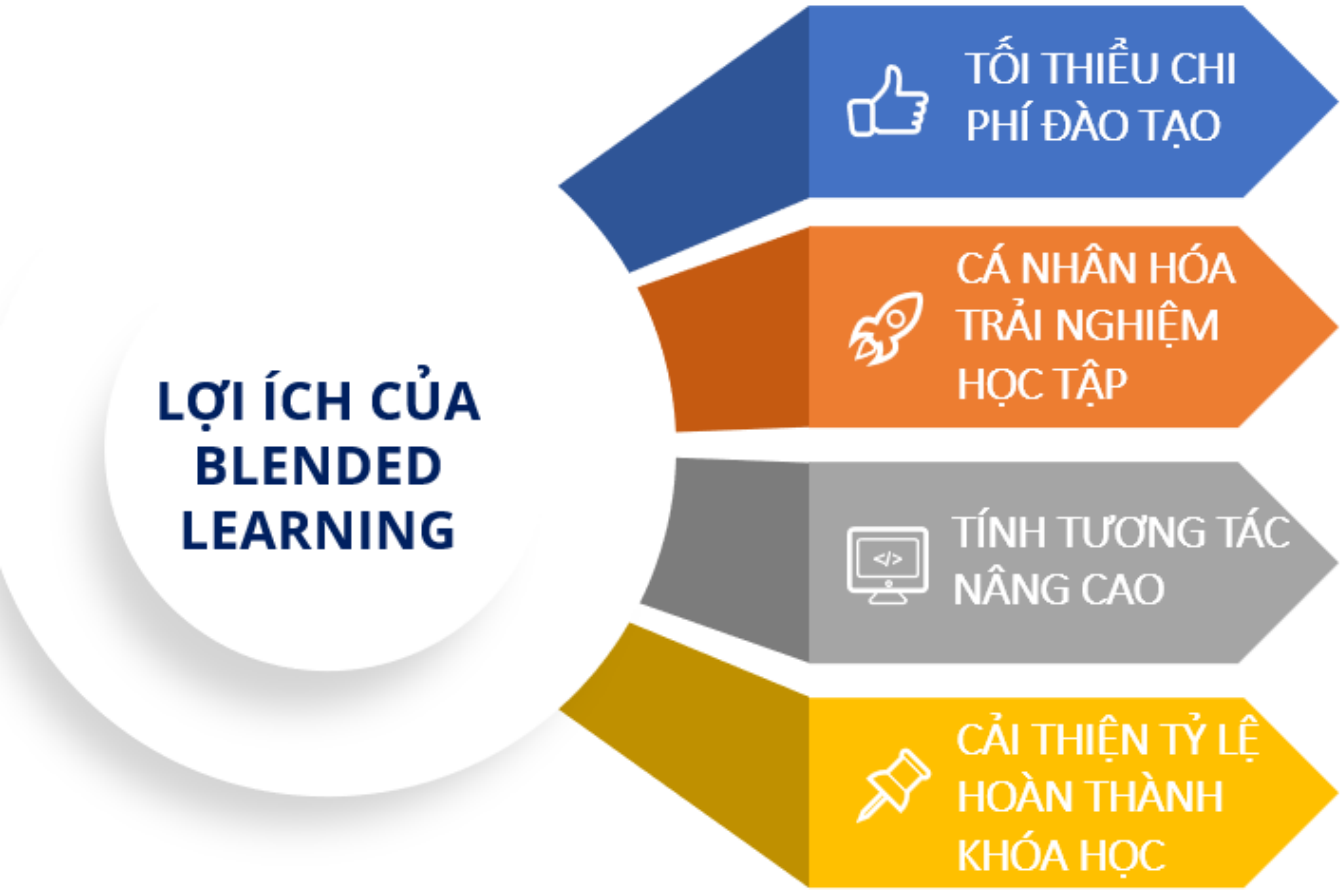
[5]. Thái Hồng Nhị, Phạm Minh Việt, *An toàn TT MMT, truyền tin số và truyền DL*, NXB KH&KT, 2004.

Phương pháp

Phương pháp học tập hỗn hợp (Blended-Learning)



Phương pháp



- Chi phí quản lý vận hành
- Cơ sở vật chất
- Lương giảng viên
- Bài giảng tái sử dụng

- Cập nhật thường xuyên hệ thống kiến thức thông tin
- Chủ động với lộ trình học tập
- Chủ động các nguồn tài liệu tham khảo

- Đa dạng hóa các công cụ hỗ trợ công nghệ cao
- Tương tác nâng cao giữa giảng viên và học viên
- Dễ dàng kiểm tra định kỳ, kiểm soát chất lượng và kiến thức

- Nâng cao tỷ lệ hoàn thành khóa học nhờ vào khả năng tạo ra sự liên kết chặt chẽ giữa người học, giảng viên và người quản lý
- Chủ động và nâng cao tinh thần trách nhiệm của học viên

Phương pháp

Học tập hỗn hợp: Kết hợp Offline và Online

- **Tuần lẻ sẽ dạy/học offline**
- **Tuần chẵn sẽ dạy/học online**

Hệ thống học trực tuyến

- egov.uneti.edu.vn
- lms.uneti.edu.vn
- Nhóm Zalo
- https://meet.google.com/zvj-sndz-vse

Nội dung chính

Chương 1: Tổng quan về mật mã và an ninh mạng.

Chương 2: Mật mã khóa đối xứng (Mật mã khóa bí mật)

Chương 3: Mật mã khóa bất đối xứng (Mật mã khoá công khai)

Chương 4: Các thuật toán tích hợp dữ liệu mật mã

Chương 5: Quản lý khóa và giao thức xác thực

Chương 6: An toàn Internet

Chương 7: An toàn mạng máy tính

Chương 8: An toàn cơ sở dữ liệu

Chương 1: Tổng quan

1.1 Tầm quan trọng

1.2 Hệ thống thông tin và tài sản

1.3 Các mối đe dọa và biện pháp ngăn chặn

1.4 Các yêu cầu

1.5 Các chiến lược an toàn hệ thống

1.6 Các mức bảo vệ trên mạng

1.7 Các kỹ thuật bảo đảm ATTT

1.8 Mật mã

1.1 Tầm quan trọng

Trước khi có máy tính, vấn đề an toàn bảo mật thông tin:

- Đóng dấu và ký niêm phong một bức thư hoặc tài liệu.
- Dùng các phương pháp mật mã.
- Lưu giữ tài liệu mật trong các két sắt có khóa, tại các nơi được bảo vệ nghiêm ngặt.

1.1 Tầm quan trọng

Ngày nay có máy tính, mạng máy tính, Internet, Intranet, điện toán đám mây:

- Rò rỉ thông tin
- Đánh cắp thông tin
- Khai thác dữ liệu
- Phá hoại hệ thống thông tin

→ An toàn thông tin và an ninh mạng

1.2 Hệ thống thông tin và tài sản

Hệ thống thông tin là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng được tích lũy theo thời gian.

1.2 Hệ thống thông tin và tài sản

Tài sản của hệ thống bao gồm các thành phần sau:

- Phần cứng
- Phần mềm
- Dữ liệu
- Các truyền thông giữa các máy tính của hệ thống
- Môi trường làm việc
- Con người

1.3 Các mối đe dọa và biện pháp ngăn chặn

Có 3 hình thức chủ yếu đe dọa đến hệ thống:

- Phá hoại: Kẻ thù phá hỏng thiết bị phần cứng hoặc phần mềm hoạt động trên hệ thống.
- Sửa đổi: Tài sản của hệ thống bị sửa đổi trái phép.
- Can thiệp: Tài sản bị truy cập bởi những người không có thẩm quyền. Các truyền thông thực hiện trên hệ thống bị ngăn chặn, sửa đổi.

1.3 Các mối đe dọa và biện pháp ngăn chặn

Các đe dọa đối với một hệ thống thông tin có thể đến từ ba loại đối tượng:

- Các đối tượng từ ngay bên trong hệ thống (insider), đây là những người có quyền truy cập hợp pháp đối với hệ thống.
- Những đối tượng bên ngoài hệ thống (hacker, cracker), thường các đối tượng này tấn công qua những đường kết nối với hệ thống như Internet chẳng hạn.
- Các phần mềm độc hại (chẳng hạn spyware, adware …) chạy trên hệ thống.

1.3 Các mối đe dọa và biện pháp ngăn chặn

Các biện pháp ngăn chặn:

- Điều khiển thông qua phần mềm: Dựa vào các cơ chế an toàn bảo mật của hệ thống nền (hệ điều hành), các thuật toán mật mã học.
- Điều khiển thông qua phần cứng: Các cơ chế bảo mật, các thuật toán mật mã học được cứng hóa để sử dụng.
- Điều khiển thông qua các chính sách của tổ chức: Ban hành các qui định của tổ chức nhằm đảm bảo tính an toàn bảo mật của hệ thống.

1.4 Các yêu cầu

1. Tính bí mật/ riêng tư (Confidentiality/Privacy)
2. Tính toàn vẹn (Integrity)
3. Tính xác thực (Authenticity)
4. Tính không thể chối bỏ (Non repudiation)
5. Tính nhận dạng (Identification)

1. Tính bí mật/ riêng tư (Confidentiality/Privacy)

- Chỉ có người gửi và người nhận mới biết nội dung của tin.
- Nếu có kẻ thứ 3 là tên trộm có thể tiếp cận được tin thì cũng không thể hiểu được nội dung của tin.

2. Tính toàn vẹn (Integrity)

- Đảm bảo rằng thông tin không bị sửa đổi bất hợp pháp.
- Thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi.
- Nội dung tin có thể bị mất hoặc bị sửa đổi trên đường truyền. Lúc đó cần đảm bảo rằng người gửi và người nhận sẽ phát hiện được.

3. Tính xác thực (Authenticity)

- Người nhận tin (có thể cả người gửi) có biện pháp để chứng minh với đối tác rằng "họ chính là họ" chứ không phải là người thứ 3 khác.
- Sự xác nhận này có thể 1 chiều: người nhận phải xác thực mình với người gửi
- Có thể là 2 chiều: Người nhận với người gửi và ngược lại.

4. Tính không thể chối bỏ (Non repudiation)

- Khi quá trình truyền tin kết thúc, người gửi không thể chối bỏ rằng thông tin đó không phải do mình gửi
- Người nhận cũng không thể chối bỏ rằng mình chưa nhận tin.

5. Tính nhận dạng (Identification)

Phải có biện pháp để hệ thống có thể nhận dạng (định danh) được các người sử dụng với quyền hạn kèm theo của họ.

1.5 Các chiến lược an toàn hệ thống

- Giới hạn quyền hạn tối thiểu (Last Privilege)
- Bảo vệ theo chiều sâu (Defence In Depth)
- Nút thắt (Choke Point)
- Điểm nối yếu nhất (Weakest Link)
- Tính toàn cục
- Tính đa dạng bảo vệ

Giới hạn quyền hạn tối thiểu (Last Privilege)

- Chiến lược cơ bản nhất.
- Bất kỳ một đối tượng nào cũng chỉ có những quyền hạn nhất định đối với tài nguyên mạng.
- Khi thâm nhập mạng, một đối tượng chỉ được sử dụng một số tài nguyên nhất định.

Bảo vệ theo chiều sâu (Defence In Depth)

- Không nên dựa vào một chế độ an toàn nào dù cho chúng rất mạnh
- Nên tạo nhiều cơ chế an toàn để tương hỗ lẫn nhau.

Nút thắt (Choke Point)

- Tạo ra một "cửa khẩu" hẹp, và chỉ cho phép thông tin đi vào hệ thống của mình bằng con đường duy nhất chính là "cửa khẩu" này.
- Phải tổ chức một cơ chế kiểm soát và điều khiển thông tin đi qua cửa này.

Điểm nối yếu nhất (Weakest Link)

- "Một dây xích chỉ chắc tại mắt duy nhất, một bức tường chỉ cứng tại điểm yếu nhất"
- Kẻ phá hoại thường tìm điểm yếu nhất của hệ thống để tấn công. Do đó cần gia cố các điểm yếu của hệ thống.
- Thông thường chúng ta chỉ quan tâm đến kẻ tấn công trên mạng hơn là kẻ tiếp cận hệ thống. Do đó an toàn vật lý được coi là điểm yếu của hệ thống.

Tính toàn cục

- Các hệ thống an toàn đòi hỏi phải có tính toàn cục của các hệ thống cục bộ.
- Nếu một kẻ có thể bẻ gãy được một cơ chế an toàn thì chúng có thể thành công bằng cách tấn công hệ thống tự do của ai đó sau đó tấn công hệ thống từ nội bộ bên trong.

Tính đa dạng bảo vệ

- Cần phải sử dụng nhiều biện pháp bảo vệ khác nhau cho hệ thống khác nhau, nếu không có kẻ tấn công vào được một hệ thống thì chúng cũng dễ dàng tấn công vào các hệ thống khác.

1.6 Các mức bảo vệ trên mạng

- Quyền truy cập (Access rights)
- Đăng ký tên và mật khẩu (Login/password)
- Mã hóa dữ liệu (Data encryption)
- Bảo vệ vật lý (Physical protection)
- Tường lửa (Protection Firewall)

Quyền truy cập (Access rights)

- Là lớp bảo vệ trong cùng nhằm kiểm soát các tài nguyên của mạng và quyền hạn trên tài nguyên đó.
- Kiểm soát cấu trúc dữ liệu càng chi tiết càng tốt.
- Thường ở mức tệp

Đăng ký tên và mật khẩu (Login/password)

- Kiểm soát truy cập mức hệ thống
- Mỗi User đều phải đăng ký tên và mật khẩu
- Người quản trị mạng kiểm soát mọi hành động của mạng, xác định quyền truy cập của các User theo không gian và thời gian.

Mã hóa dữ liệu (Data encryption)

- Dữ liệu bị biến đổi từ dạng nhận thức được sang dạng không nhận thức được theo một thuật toán nào đó và sẽ được biến đổi ngược lại ở nơi nhận (giải mã).

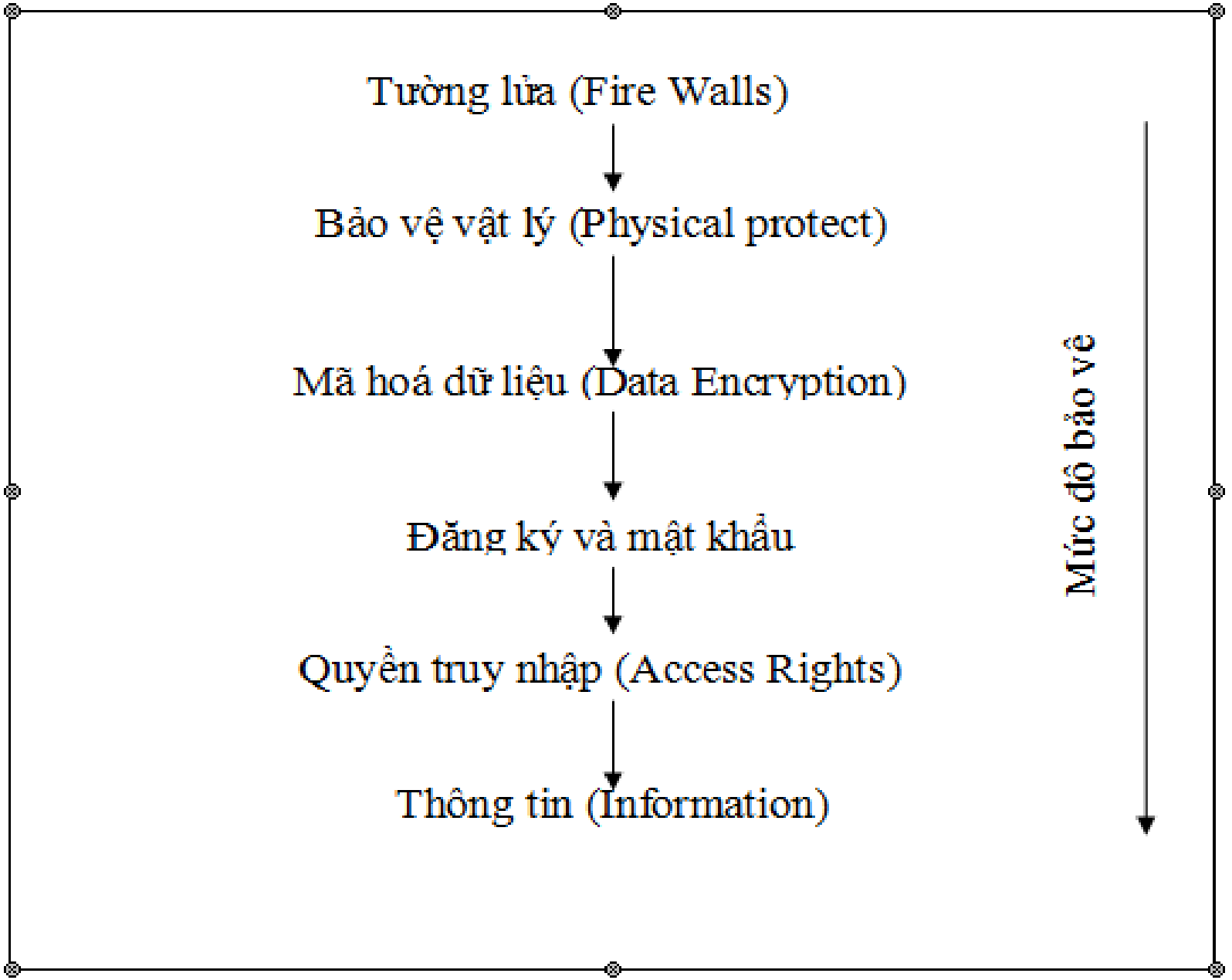
Bảo vệ vật lý (Physical protection)

- Ngăn cản các truy nhập vật lý vào hệ thống
- Không phận sự không vào phòng chứa hạ tầng cơ sở mạng
- Dùng ổ khóa, …

Tường lửa (Protection Firewall)

- Ngăn chặn thâm nhập trái phép và lọc bỏ các gói tin không muốn gửi hoặc nhận vì các lý do nào đó để bảo vệ một máy tính hoặc cả mạng nội bộ (intranet).

Các mức độ bảo vệ thông tin từ ngoài vào trong



Quản trị mạng

- Toàn bộ hệ thống hoạt động bình thường trong giờ làm việc.
- Có hệ thống dự phòng khi có sự cố về phần cứng hoặc phần mềm xảy ra.
- Backup dữ liệu quan trọng theo định kỳ.
- Bảo dưỡng mạng theo định kỳ.
- Bảo mật dữ liệu, phân quyền truy cập, tổ chức nhóm làm việc trên mạng.

1.7 Các kỹ thuật bảo đảm ATTT

- Diệt trừ: Xóa Virus, chương trình trái phép
- Tường lửa: Ngăn chặn truy cập trái phép, lọc thông tin không hợp pháp
- Mạng riêng ảo: Tạo hành lang riêng cho thông tin
- Mật mã: Mật mã hóa, ký số, giao thức, chống chối cãi, hàm băm, …
- Giấu tin: Che dấu thông tin trong môi trường dữ liệu khác.
- Thủy ký: Bảo vệ bản quyền tài liệu số hóa
- Truy tìm dấu vết kẻ trộm tin

1.8 Mật mã

- Mật mã (Cryptography) là một ngành khoa học nghiên cứu cách viết mã và giữ thông tin một cách bí mật.
- Đảm bảo sự bí mật thông tin tại nơi lưu trữ cũng như khi truyền thông tin trên mạng.
- Che dấu thông tin là thay đổi hình dạng thông tin gốc làm cho người đọc khó biết được thông tin gốc.

1.8 Mật mã

Mật mã bao gồm: Lập mã và phá mã.

- Lập mã bao gồm hai quá trình: Mã hóa và giải mã. Các sản phẩm của lĩnh vực này là các hệ mã mật, các hàm băm, các hệ chữ ký điện tử, các cơ chế phân phối, quản lý khóa và các giao thức mật mã.

- Phá mã (thám mã): Nghiên cứu các phương pháp phá mã hoặc tạo mã giả. Sản phẩm của lĩnh vực này là các phương pháp phá mã, các phương pháp giả mạo chữ ký, các phương pháp tấn công các hàm băm và các giao thức mật mã

1.8 Mật mã

Có 2 phương thức mã hoá cơ bản: Thay thế và hoán vị:

- Thay thế: từng ký tự gốc hay một nhóm ký tự gốc của bản rõ được thay thế bởi các từ, các ký hiệu khác hay kết hợp với nhau cho phù hợp với một phương thức nhất định và khoá.
- Hoán vị: các từ mã của bản rõ được sắp xếp lại theo một phương thức nhất định.

1.8 Mật mã

Hệ mật mã và vai trò của hệ mật mã:

- Hệ mật mã phải che dấu được nội dung của văn bản rõ (PlainText).
- Tạo các yếu tố xác thực thông tin, đảm bảo thông tin lưu hành trong hệ thống đến người nhận hợp pháp là xác thực (Authenticity).
- Tổ chức các sơ đồ chữ ký điện tử, đảm bảo không có hiện tượng giả mạo, mạo danh để gửi thông tin trên mạng.

Hệ mật mã

- Bản rõ X được gọi là là bản tin gốc. Bản rõ có thể được chia nhỏ để có kích thước phù hợp với các thuật toán mã hóa.
- Bản mã Y là bản tin thu được sau khi bản tin gốc đã được mã hoá. Ở đây ta thường xét phương pháp mã hóa mà không làm thay đổi kích thước của bản rõ, tức là chúng có cùng độ dài.
- Mã là thuật toán E chuyển bản rõ thành bản mã. Thông thường chúng ta cần thuật toán mã hóa mạnh, cho dù thám mã biết được thuật toán, nhưng không biết thông tin về khóa cũng không tìm được bản rõ.

Hệ mật mã

Một hệ mã mật là bộ 5 thành phần (*P, C, K, E, D*):

***P*:** không gian bản rõ (Plaintext): là tập hữu hạn các bản rõ có thể có.

***C*:** không gian bản mã (Ciphertext): là tập hữu hạn các bản mã có thể có.

***K*:** không gian khoá (Key): là tập hữu hạn các khoá có thể có.

***E*:** thuật toán mã hóa (Encryption algorithm)

***D*:** thuật toán giải mã (Decryption algorithm)

Hệ mật mã

Một hệ mã mật là bộ 5 thành phần (P, C, K, E, D):

Đối với mỗi $k \in K$ có một quy tắc mã $e_K: P \rightarrow C$

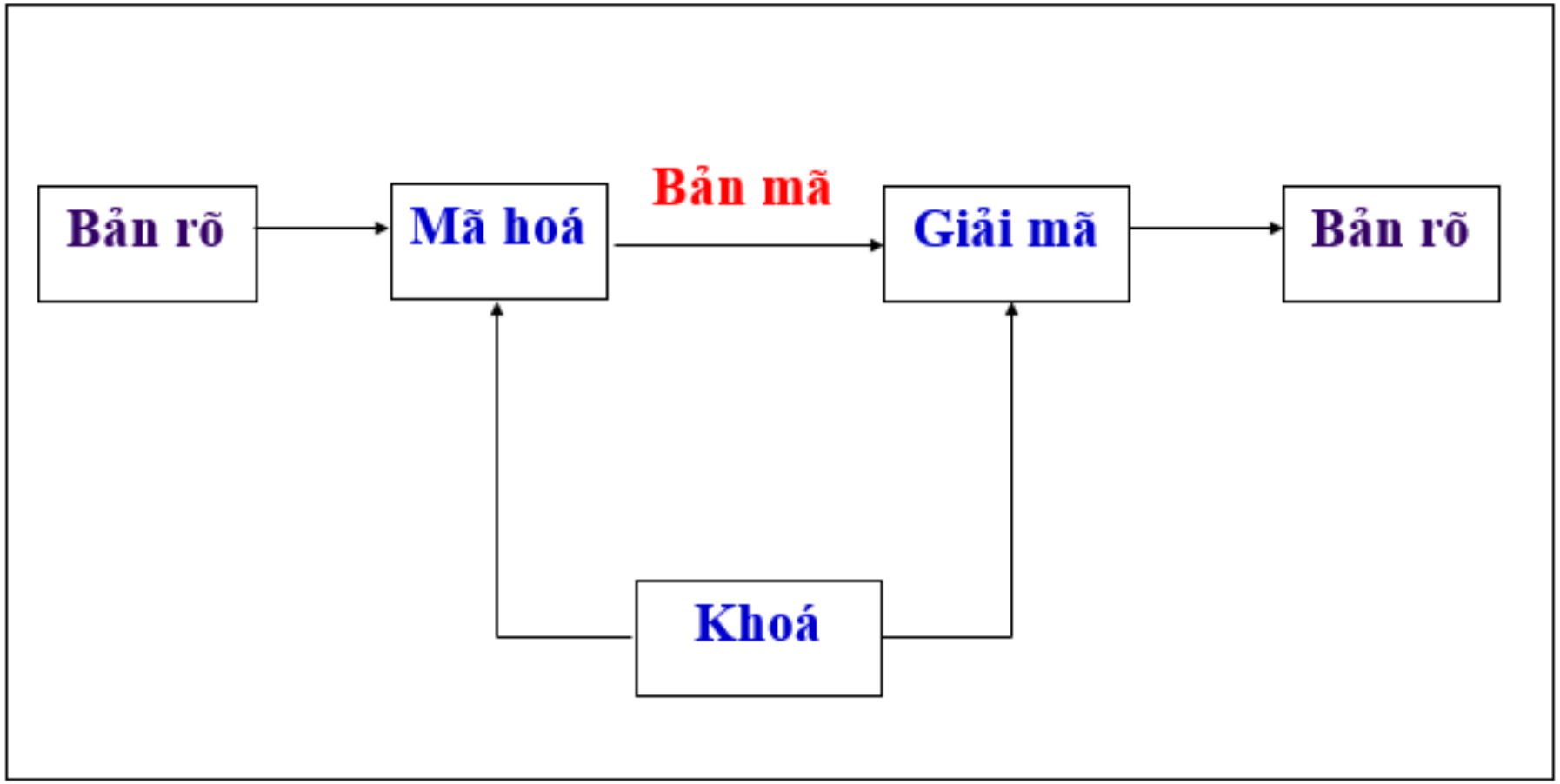
và một quy tắc giải mã tương ứng $d_K \in D: C \rightarrow P$

Với mỗi $e_K: P \rightarrow C$ và $d_K: C \rightarrow P$ là những hàm mà

$d_K(e_K(x)) = x$ với mọi bản rõ $x \in P$.

Hàm giải mã d_k chính là ánh xạ ngược của hàm mã hóa e_k

Hệ mật mã



Quá trình mã hóa và giải mã thông tin