LÝ THUYẾT MẬT MÃ

Cryptography Theory

ET3310

NCM. Lý thuyết Thông tin

Mục tiêu học phần

Cung cấp kiến thức cơ bản về mật mã đảm bảo an toàn và bảo mật thông tin:

- ✓ Các phương pháp mật mã khóa đối xứng; Phương pháp mật mã khóa công khai;
- ✓ Các hệ mật dòng và vấn đề tạo dãy giả ngẫu nhiên;
- ✓ Lược đồ chữ ký số và các chuẩn chữ ký số;
- ✓ Độ phức tạp xử lý và độ phức tạp dữ liệu của một tấn công cụ thể vào hệ thống mật mã;
- ✓ Đặc trưng an toàn của phương thức mã hóa;
- ✓ Thám mã tuyến tính, thám mã vi sai và các vấn đề về xây dựng hệ mã bảo mật cho các ứng dụng.

Nội dung môn học

- Chương 1. Giới thiệu
- Chương 2. Toán học của mật mã
  - *Phần I: Số học theo mô-đun, đồng nhất, và Ma trận*
- Chương 3. Các hệ mật mã đối xứng cổ điển
- Chương 4. Các hệ mật mã khoá đối xứng hiện đại
  - *Phần II: Cấu trúc Đại số: Nhóm, vành trường*
- Chương 5. Chuẩn mã hóa dữ liệu (DES)
- Chương 6. Chuẩn mã hóa nâng cao (AES)
- Chương 7. Hàm băm và chữ ký số
- Chương 8. Dãy giả ngẫu nhiên và hệ mật dòng
- Chương 9. Kỹ thuật quản lý khóa.

Tài liệu tham khảo

1. A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, *Handbook of applied cryptography*, CRC Press 1998.
2. B. Schneier, *Applied Cryptography*. John Wiley Press 1996.
3. M. R. A. Huth, *Secure Communicating Systems*, Cambridge University Press 2001.
4. W. Stallings, *Network Security Essentials, Applications and Standards*, Prentice Hall. 2000.

Nhiệm vụ của Sinh viên

1. Chấp hành nội quy lớp học
2. Thực hiện đầy đủ bài tập
3. Nắm vững 01 ngôn ngữ lập trình Python, Matlab …

Chương 1. Tổng quan

1.1. Giới thiệu sơ lược lịch sử khoa học mật mã

1.2. Khái niệm, mô hình của hệ mật

1.3. Một số hệ mật ban đầu

1.4. Các bài toán an toàn thông tin

1.5. Thám mã

1.6. Tính an toàn của các hệ mật mã

1.7. Cơ sở toán học của hệ mật mã

1.8. Tính bí mật của các hệ mật

1.1. Giới thiệu sơ lược lịch sử khoa học mật mã

Caesar cipher

- Trong cuốn Cuộc đời của Caesar VI của Suetonius có mô tả chi tiết về một số mật mã của Caesar. Caesar thay thế một cách đơn giản từng chữ cái trong thư bằng chữ cái cách đó ba vị trí trong bảng chữ cái. Sau này được gọi là mã dịch chuyển Caesar.

DVH Oderudwrub=

1.1. Giới thiệu sơ lược lịch sử khoa học mật mã

- Người Ai Cập cổ đại bắt đầu sử dụng mật mã hạn chế khoảng 4000 năm về trước.
- Thuật ngữ "mật mã - **cryptography**" dịch từ tiếng Hy Lạp có nghĩa là "chữ viết bí mật" (Kryptósgráfo "hidden" và grafo "to write" or legein "to speak").
- Sự khởi đầu cho kỷ nguyên **mật mã hiện đại** được đánh dấu bởi các công bố của của Claude E. Shannon: "A Mathematical Theory of Cryptography"[1)]-1948, "Communication Theory of Secrecy Systems" [2)]-1949. Khái niệm về các tính chất Confusion và Diffusion cũng do C.E. Shannon đưa ra, và sau này được dùng phổ biến để đánh giá cho mật mã nói chung.
- Sự phát triển và ngày càng phổ biến của máy tính và hệ thống thông tin liên lạc trong những năm 1960 đã tạo ra nhu cầu bảo vệ thông tin dưới dạng số và cung cấp dịch vụ an ninh thông tin.
- DES (Data Encryption Standard): Tiêu chuẩn bảo mật dữ liệu được Horst Feistel thiết kế bởi vào năm **1970** tại IBM và chấp thuận thành chuẩn vào năm **1977** bởi Chuẩn xử lý thông tin của Liên bang Hoa Kỳ (Federal Information Processing Standard - FIPS). DES là cơ chế mã hóa nổi tiếng nhất trong lịch sử.

[1)] Claude E. Shannon, "A Mathematical Theory of Cryptography", The Bell System Technical Journal, vol. 27, pp. 379–423, 623–656, July, October, 1948.
[2)] Claude E. Shannon, "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, vol. 28(**4**), page 656–715, 1949.

1.1. Giới thiệu sơ lược lịch sử khoa học mật mã

- Whitefield Diffie và Martin E. Hellman xuất bản bài báo "New Directions in Cryptography" [1] năm **1976** về Mật mã khóa công khai (public-key cryptography) hoặc mật mã hóa bất đối xứng.
- Năm **1978** thuật toán mật mã và chữ ký khóa công khai đầu tiên, RSA, ra đời.
- Trước đó, vào năm **1973**, Clifford Cocks, một nhà toán học người Anh đã mô tả một thuật toán tương tự. Với khả năng tính toán tại thời điểm đó thì thuật toán này không khả thi và chưa bao giờ được thực nghiệm. Tuy nhiên, phát minh này chỉ được công bố vào năm **1997** vì được xếp vào loại tuyệt mật.
- Năm **1985** ElGamal phát triển một lớp thuật toán khóa công khai khác dựa trên bài toán logarit rời rạc.

[1] W. Diffie and M. Hellman, " New Directions in Cryptography," in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, 1976.

1.1. Giới thiệu sơ lược lịch sử khoa học mật mã

- Đóng góp quan trọng của cơ chế khóa công khai là chữ ký số (Digital Signature). Năm **1991** tiêu chuẩn chữ ký số đầu tiên ISO/IEC 9796 dựa trên thuật toán RSA
- Năm **1994** chính phủ Mỹ công bố chuẩn Digital Signature Standard dựa trên cơ chế ElGamal.
- Hàng thế kỷ qua, mật mã là nghệ thuật viết mã và giải mã
- **Trước kia**: Chủ yếu trong thông tin quân sự và tình báo
- **Ngày nay**: Dùng phổ biến trên mọi lĩnh vực…

1.1. Giới thiệu sơ lược lịch sử khoa học mật mã

- Ngày nay, các ứng dụng mã hóa và bảo mật thông tin đang được sử dụng ngày càng phổ biến trong các lĩnh vực khác nhau trên thế giới, từ các lĩnh vực an ninh, quân sự, quốc phòng…, cho đến các lĩnh vực dân sự như thương mại điện tử, ngân hàng.
- Trong đời sống – xã hội: Các ứng dụng mã hóa thông tin cá nhân, trao đổi thông tin kinh doanh, thực hiện các giao dịch điện tử qua mạng... đã trở nên gần gũi và quen thuộc với mọi người.
- Ứng dụng của khoa học mật mã không chỉ đơn thuần là mã hóa và giải mã thông tin mà còn bao gồm nhiều vấn đề khác nhau cần được nghiên cứu và giải quyết như chứng thực nguồn gốc nội dung thông tin (kỹ thuật chữ ký điện tử), chứng nhận tính xác thực về người sở hữu mã khóa (chứng nhận khóa công cộng), các quy trình giúp trao đổi thông tin và thực hiện giao dịch điện tử an toàn trên mạng...
- Những kết quả nghiên cứu về mật mã cũng đã được đưa vào trong các hệ thống phức tạp hơn, kết hợp với những kỹ thuật khác để đáp ứng yêu cầu đa dạng của các hệ thống ứng dụng khác nhau trong thực tế.

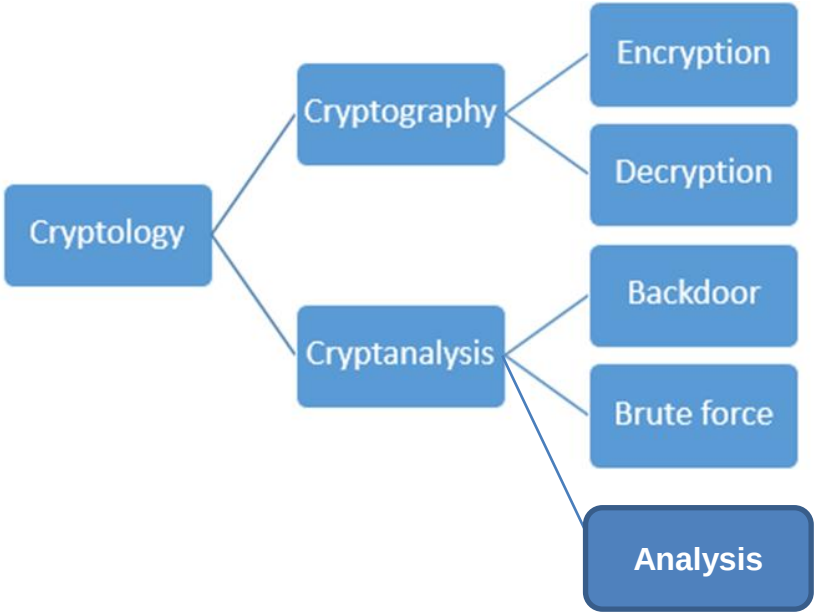
1.2. Khái niệm, mô hình của hệ mật

- Ngược lại của mật mã là ***thám mã***
  - Thực hiện bài toán: ***"Tìm chìa khóa mật mã"*** hay ***"khôi phục nội dung thông tin"***
- Không thể xây dựng một hệ mật (Cryptosystem) tốt nếu không hiểu biết sâu về thám mã.
- Một giải pháp mật mã là bảo đảm bí mật, nếu mọi thuật toán thám mã đều phải được thực hiện với độ phức tạp tính toán cực lớn *(ngoài khả năng của máy tính hoặc thời gian rất dài)*.

Mật mã học (Cryptology)

=

Mật mã (Cryptography) + Thám mã (Cryptanalysis)

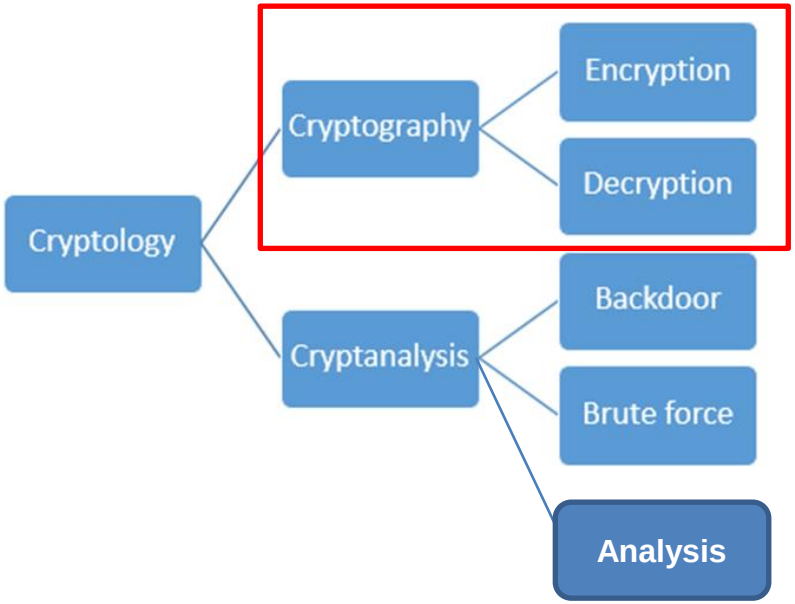


1.2. Khái niệm, mô hình của hệ mật

Mật mã học (Cryptology)

=

Mật mã (Cryptography) + Thám mã (Cryptanalysis)

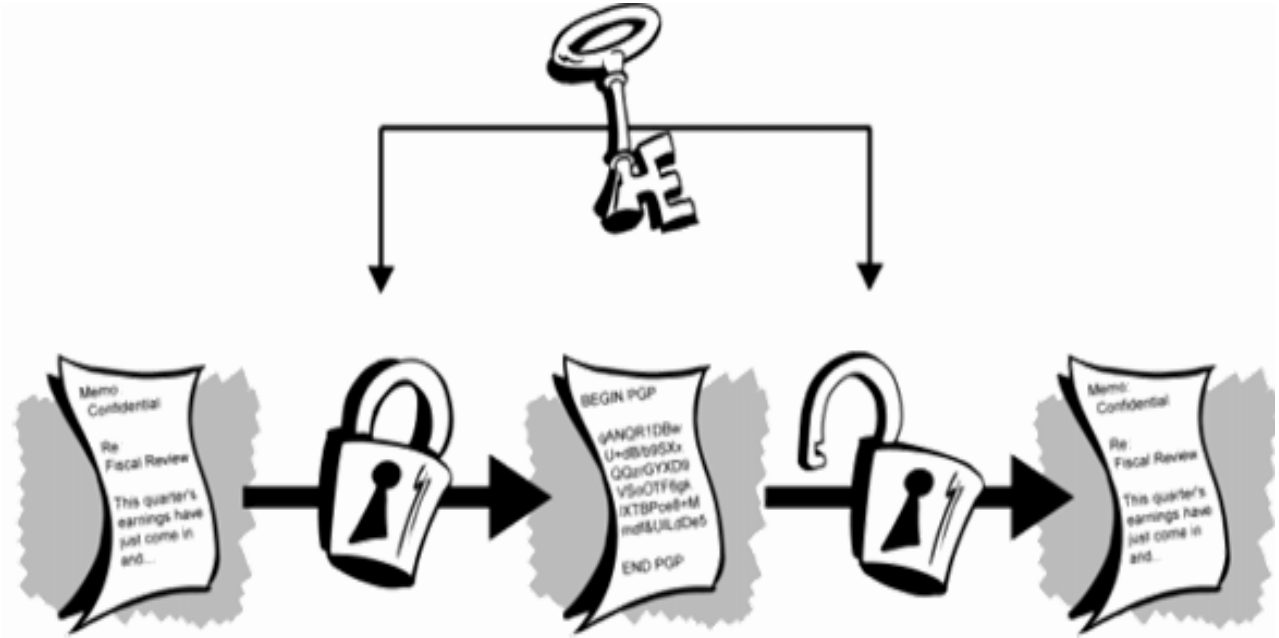


1.2. Khái niệm, mô hình của hệ mật

- Mật mã nhằm là để giữ bí mật thông tin. Ví dụ: văn bản của A gửi đến B muốn giữ bí mật (giấu nội dung).
  - A phải tạo cho văn bản đó một bản mã mật tương ứng.
  - B nhận được bản mã mật và sẽ có cách từ đó khôi phục lại văn bản rõ để hiểu được thông tin mà A muốn gửi cho mình.
  - A và B phải có một ***"chìa khóa chung"*** được gọi là ***"Khóa mật mã"***

1.2. Khái niệm, mô hình của hệ mật

Khóa mật mã



Bản tin rõ (**P**laintext)

Mật mã hóa (**E**ncryption)

Bản tin mật (**C**iphertext)

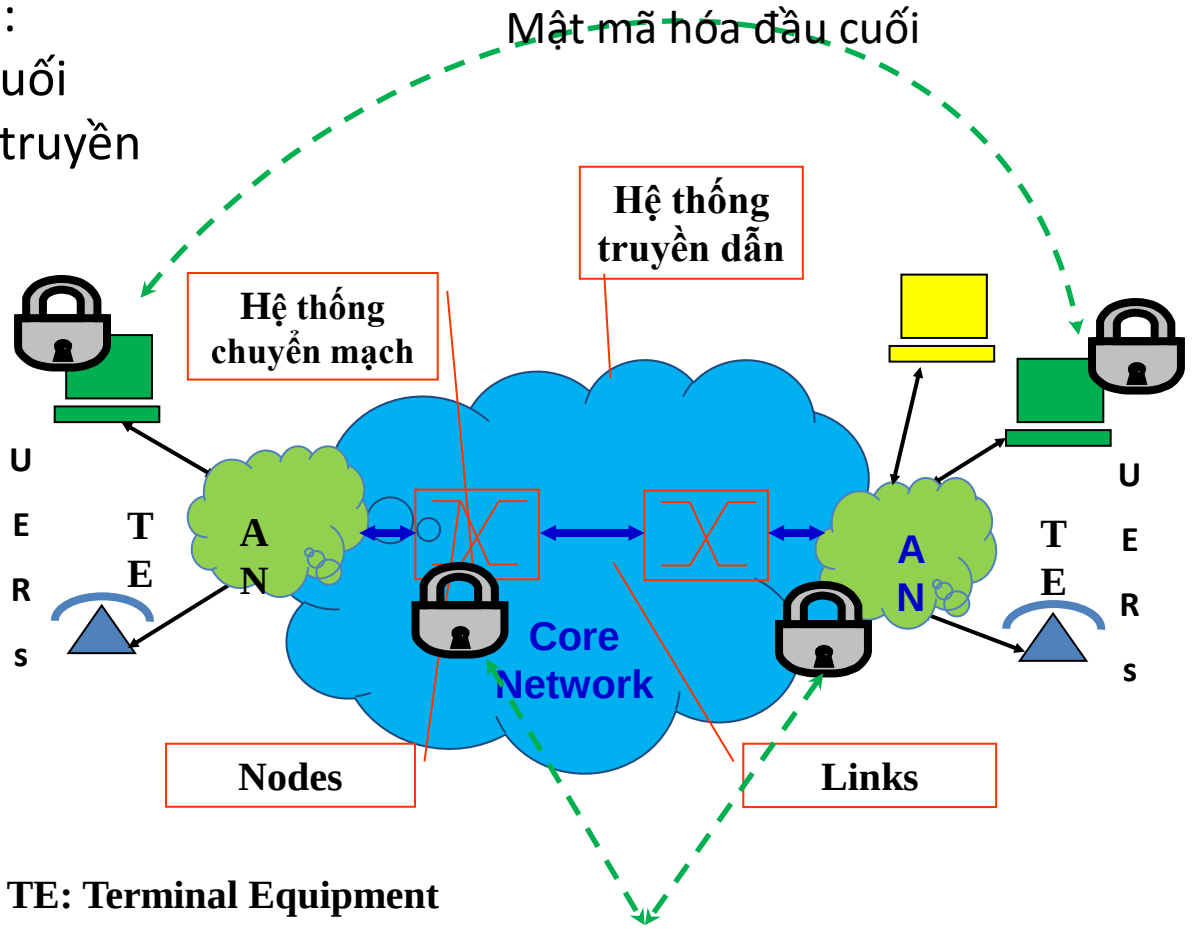
Giải mã mật (**D**ecryption)

Bản tin rõ (**R**ecovered Plaintext)

1.2. Khái niệm, mô hình của hệ mật

Trong hệ thống truyền tin:

- Mật mã hóa đầu cuối
- Mật mã hóa kênh truyền



AN: Access Network ; TE: Terminal Equipment

1.2. Khái niệm, mô hình của hệ mật

- Thuật toán lập (mật mã hóa)/giải mật mã: là thuật toán biến bản rõ, cùng với khóa mật mã, thành bản mã mật và ngược lại.
- Trong khoa học mật mã:
  - Thuật toán lập/giải mật mã có thể không cần giữ bí mật.
  - Giữ tuyệt mật: khóa mật mã

1.2. Khái niệm, mô hình của hệ mật

Hệ thống mật mã (Cryptosystem)

- Một hệ thống mật mã là một bộ năm:

$$\boldsymbol{S = (P, C, K, E, D)}$$

Thỏa mãn các điều kiện sau đây:

- Tập nguồn ***P*** (**plaintext**) là tập hữu hạn tất cả các bản tin nguồn cần mã hóa có thể có.
- ***C*** (**ciphertext**) là một tập hữu hạn các ký tự bản mã
- ***K*** (**key**)là tập hữu hạn các khóa có thể được sử dụng
- ***E*** (**encryption**) là một ánh xạ từ ***(K,P)*** vào ***C***, được gọi là phép lập mật mã
- ***D*** (**decryption**)**là** một ánh xạ từ ***(K,C)*** vào ***P*** , được gọi là phép giải mã.

Chú ý: các ánh xạ này là ánh xạ 1-1

1.2. Khái niệm, mô hình của hệ mật

Hệ thống mật mã (Cryptosystem)

- Một sơ đồ hệ thống mật mã là một bộ năm tham số

$$\boldsymbol{S = (P, C, K, E, D)}$$

- ✓ Với mỗi khóa $\boldsymbol{k \in K}$, tồn tại luật mật mã $\boldsymbol{e_k \in E}$ và luật giải mật mã $\boldsymbol{d_k \in D}$ tương ứng.
- ✓ Luật mật mã $\boldsymbol{e_k}$: $\boldsymbol{P \rightarrow C}$ và luật giải mật mã $\boldsymbol{d_k}$: $\boldsymbol{C \rightarrow P}$ là hai ánh xạ thỏa mãn: $\boldsymbol{d_k(e_k(x)) = x, \forall x \in P}$

1.3. Phân loại hệ mật

- Theo cách thức quản lý và sử dụng khóa mật:
  - Khóa công khai (**public-key**) hay còn gọi là mật mã hóa bất đối xứng (asymetric)
  - Khóa bí mật (**private-key**) hay mật mã hóa đối xứng (symmetric-key)
- Theo cách đối xử với dữ liệu:
  - Mật mã khối bit (**block cipher**)
  - Mật mã luồng bit (**stream cipher**)

1.3. Phân loại hệ mật - Mật mã khối bit

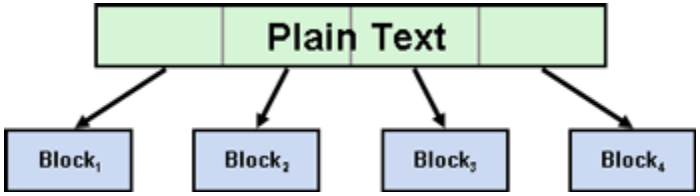
➢ *Mã theo khối (Block cipher)*

- Độ dài khối (N bít)
- Không gian khóa k được mở rộng từ $K \rightarrow K^k$ (key scheduling)
- Mỗi $K = K_1 \dots K_k \in K^k$, các thuật toán e_k và d_k được mở rộng: e_k: $P^k \rightarrow C^k$ và d_k: $C^k \rightarrow P^k$ như sau:

Với mọi bản rõ $x_1 \dots x_k \in P^k$ ***và bản mã*** $y_1 \dots y_k \in C^k$ ***ta có***

$$e_K(x_1 \dots x_k) = e_{K_1}(x_1) \dots e_{K_k}(x_k)$$
$$d_K(y_1 \dots y_k) = d_{K_1}(y_1) \dots d_{K_k}(y_k)$$

Thực tế là chia ra thành từng khối bit để mật mã hóa và giải mã rồi ghép lại



1.3. Phân loại hệ mật - Mật mã dòng bit

➢ *Mã theo dòng (Stream cipher)*

- Đầu tiên xác định 1 ***dòng khóa***: $K = K_1 \dots K_m \in K^*$ nào đó
- Bản mã tương ứng với mọi bản rõ $X = x_1 \dots x_m \in P^*$ với dòng khóa K được xác định: $Y = e_K(X)$

  $e_K(X) = e_K(x_1 \dots x_m) = e_{K_1}(x_1) \dots e_{K_m}(x_m)$
- Giải mã $X = d_K(Y) = d_K\left(e_K(X)\right)$ ta được:

$$d_K(Y) = d_{K_1}\left(e_{K_1}(x_1)\right) \dots d_{K_m}\left(e_{K_m}(x_m)\right) = x_1 \dots x_m = X$$

1.3. Phân loại hệ mật - Mật mã dòng bit

➢ *Mã theo dòng (Stream cipher)*

- Trong các ứng dụng thực tế, người ta thường dùng cách mã theo dòng có sơ đồ mật mã gốc là sơ đồ Vernam với:

$$P = C = K = \{0, 1\}$$

- Các hàm lập mã và giải mã theo từng bit được xác định bởi:

$$e_K(x) = x + K \bmod(2)$$
$$d_K(y) = y + K \bmod(2)$$
$$K = 0 \; hoặc \; 1$$

Thực tế là phép XOR các bit

- Dòng khóa là dãy bit ngẫu nhiên được sinh ra bởi một bộ tạo dãy bit ngẫu nhiên nào đó.

1.3. Phân loại hệ mật – Khóa đối xứng

➢ *Mật mã khóa đối xứng (khóa bí mật)*

- Trong một giao dịch truyền tin bảo mật:
  - ✓ Người A gửi cho người B bản tin đã được mật mật mã với quy ước trước một khóa chung K.
    - A dùng e_K để lập mật mã
    - B dùng d_K đề giải mã bản mật
- Nhận xét: *sinh viên tự tìm hiểu chi tiết trên Wikipedia*

1.3. Phân loại hệ mật – Khóa công khai

➢ ***Mật mã khóa bất đối xứng (khóa công khai)***

- Trong khoa học mật mã, về nguyên tắc hai hàm lập mã và giải mã là khác nhau, không nhất thiết phải phụ thuộc cùng một khóa.

- Nhận xét: *sinh viên tự tìm hiểu chi tiết trên Wikipedia*

1.3. Phân loại hệ mật – mã hóa đối xứng

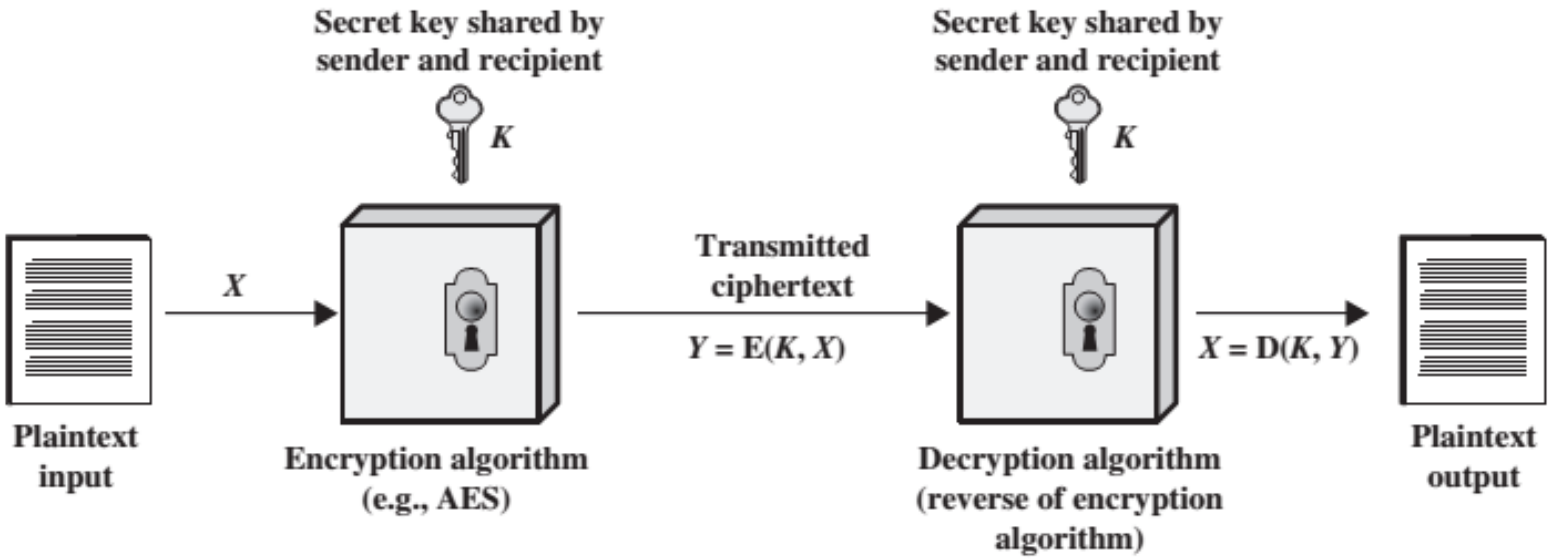
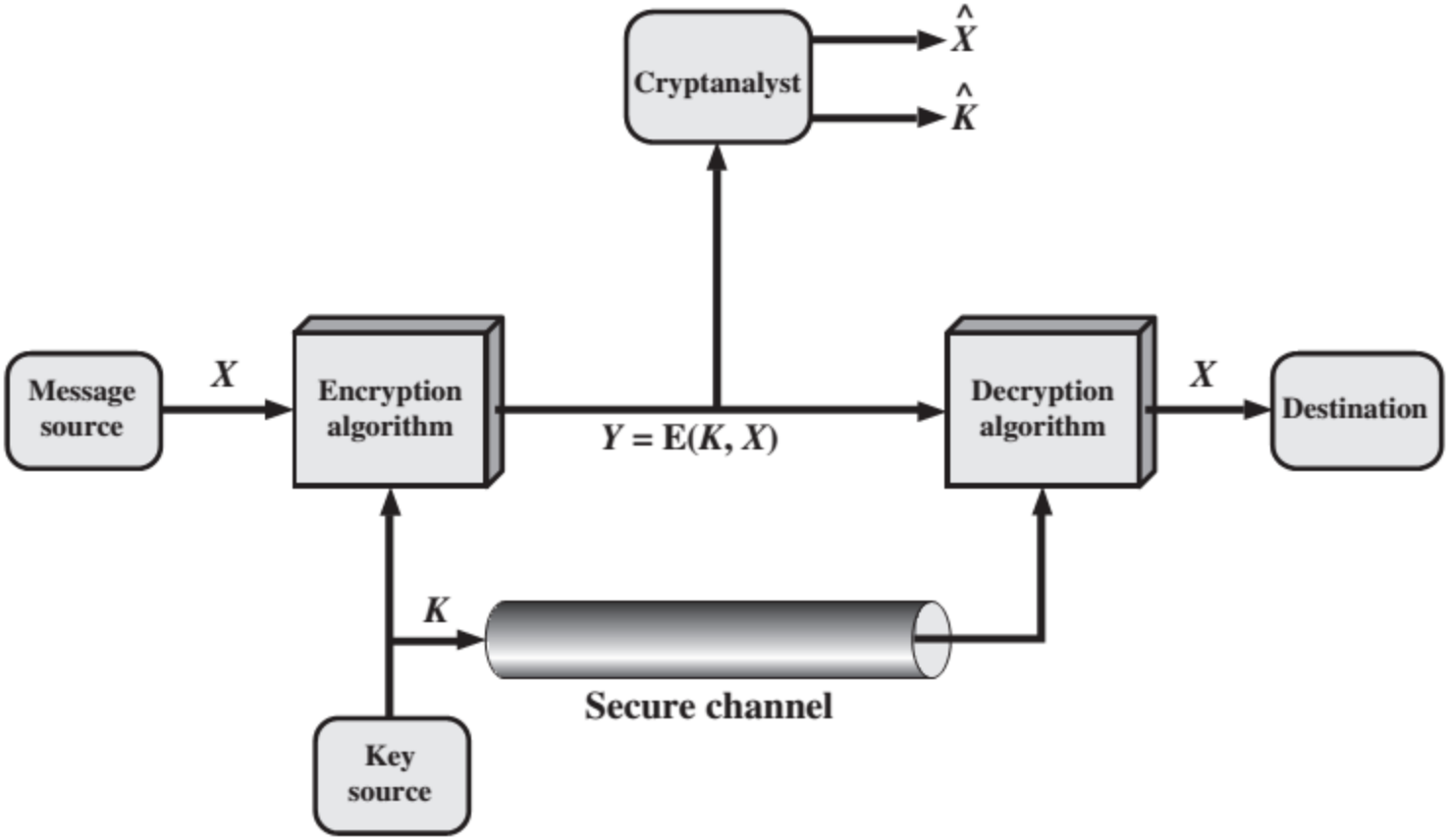


Figure 2.1 Simplified Model of Symmetric Encryption

1.3. Phân loại hệ mật – mã hóa đối xứng



1.4. Các vấn đề liên quan đến anh ninh và an toàn thông tin

- Tính kín đáo (**confidentiality**): 2 khái niệm
  - Giữ kín dữ liệu
  - Tính riêng tư (privacy)
- Toàn vẹn thông tin (**integrity**): 2 khái niệm
  - Toàn vẹn dữ liệu
  - Toàn vẹn hệ thống
- Tính sẵn sàng
- Tính chính xác: đảm bảo tin tức đúng nguồn gốc và có thể kiểm tra được tính chính xác
- Tính giải trình: đảm bảo không bị chối cãi…

1.4. Các vấn đề liên quan đến anh ninh và an toàn thông tin

- Từ đó có các dịch vụ:
  - Nhận thực một thực thể
  - Nhận thực một thông báo
  - Ủy quyền
  - Cấp chứng chỉ
  - Báo nhận
  - Làm chứng
  - Không chối bỏ được
  - Ẩn danh
  - Thu hồi
  - Chữ ký

1.4. Các vấn đề liên quan đến anh ninh và an toàn thông tin

privacy or confidentiality	Tính riêng tư hoặc tính bí mật	Giữ thông tin bí mật đối với những người không có quyền được biết
Data integrity	Tính toàn vẹn dữ liệu	Đảm bảo thông tin không bị sửa đổi, thay đổi bởi những người không được quyền thực hiện với bất cứ lý do gì không được biết.
Entity authentication or identification	Nhận thực thực thể hoặc định danh	Xác nhận đối tượng được quyền (chủ quyền) như máy tính, thẻ master card …
Message authentication	Nhận thực bản tin	Xác nhận nguồn thông tin đúng nguồn gốc
Signature	Chữ ký	Đánh dấu xác nhận
Authorization	Tác quyền	Thành phần có quyền thực hiện việc gì đó

1.4. Các vấn đề liên quan đến anh ninh và an toàn thông tin-các từ khóa

Validation	Tính hợp lệ	Xác nhận thời gian, tính hợp lệ của thông tin và nguồn tin
Access control	Điều khiển truy nhập	Giới hạn quyền truy nhập vào tài nguyên ở mức độ nào đó
Certification	Chứng nhận	Xác nhận sự trung thực hay đúng đắn

timestamping	**Nhãn thời gian**	**Ghi lại thời gian**
Witnessing	Chứng thực	Chứng kiến sự tồn tại của thông tin
Receipt	Biên nhận	Phúc đáp/xác nhận việc đã nhận được thông tin
Confirmation	Xác nhận	Khẳng định điều gì đó chắc chắn

1.4. Các bài toán an toàn thông tin

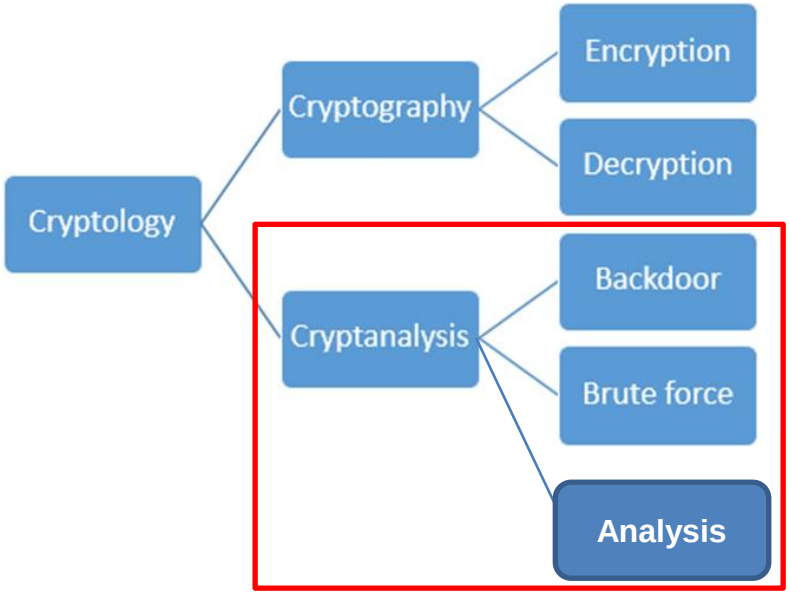
Ownership	Quyền sơ hữu	Cách cung cấp quyền hợp pháp hoặc quyền chuyển tài nguyên đến các thành phần khác
Anonymity	Nặc danh	Giấu kín danh tính khi thực hiện một điều/quá trình gì đó
Non-repudiation	Chống sự từ chối	Ngăn chặn sự từ chối những cam kết hoặc từ chối các hành động
Revocation	Thu hồi	Thu hồi chứng chỉ hay tác quyền

1.5. Thám mã

Mật mã học (Cryptology)

=

Mật mã (Cryptography) + Thám mã (Cryptanalysis)



1.5. Thám mã

- ***Mật mã học hiện đại*** – Modern Cryptography: Là ngành khoa học nghiên cứu các kỹ thuật đảm bảo an toàn thông tin, giao dịch và các tính toán phân bố.
- ***Thám mã (Cryptanalysis):*** Là ngành khoa học nghiên cứu các điểm yếu của hệ mật từ đó đưa ra phương pháp tấn công hệ mật đó (tin tặc-black hat) hoặc giúp cải thiện phương pháp mật mã (white hat).
  - Mật mã và thám mã là hai lĩnh vực đối lập nhau nhưng gắn bó mật thiết với nhau.
  - Không thể xây dựng một hệ mật (Cryptosystem) tốt nếu không hiểu biết sâu về thám mã.
  - Một giải pháp mật mã là bảo đảm bí mật, nếu mọi thuật toán thám mã, nếu có, đều phải được thực hiện với độ phức tạp tính toán cực lớn hoặc thời gian tính toàn rất dài.

1.5. Thám mã

- **Các giả thiết của bài toán thám mã:**
  - ***Thám mã khi có bản rõ được chọn*** (chosen-plaintext attack): cho phép có thể thực hiện mật mã nhiều lần với các bản rõ khác nhau➔ can thiệp bên mật mã hóa (encryptor)
  - ***Thám mã khi có bản mã được chọn*** (chosen-ciphertext attack): cho phép thực hiện giải mã hóa nhiều lần với các bản mã khác nhau ➔ Can thiệp bên giải mã (decryptor)
  - ***Thám mã khi biết bản rõ*** (known-plaintext attack): chỉ có bản rõ được dùng nhận được bản mã➔ hiểu được cách thức mật mã
  - ***Thám mã chỉ biết bản mã*** (ciphertext-only attack): chỉ có bản mã để phân tích và tìm ra khóa mật hoặc thông tin.

1.5. Thám mã

Type of Attack	Known to Cryptanalyst
Ciphertext only	• Encryption algorithm • Ciphertext to be decoded
Known plaintext	• Encryption algorithm • Ciphertext to be decoded • One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	• Encryption algorithm • Ciphertext to be decoded • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	• Encryption algorithm • Ciphertext to be decoded • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	• Encryption algorithm • Ciphertext to be decoded • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

1.6. Tính an toàn của các hệ mật mã

- Tính an toàn của một hệ thống mật mã phụ thuộc vào độ khó khăn của bài toán thám mã khi sử dụng hệ mật mã đó.
- Tính an toàn **theo nghĩa được chứng minh hay tính toán được** sử dụng nhiều trong việc nghiên cứu các hệ thống mật mã hiện đại, đặc biệt là các hệ thống mật mã khóa công khai.
- Các vấn đề an toàn của hệ mật mã bao gồm:

1.6. Tính an toàn của các hệ mật mã

- *An toàn vô điều kiện*: Tính toán được sác xuất mất an toàn bằng 0
- *An toàn được chứng minh*: áp dụng cho giải thuật
- *An toàn tính toán*: áp dụng cho nền tảng tính toán

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.1. SỐ HỌC CÁC SỐ NGUYÊN

- ***Z là tập hợp các số nguyên: Z = {.....,-2,-1,0,1,2,....}***
- ***Z^+ là tập hợp các số nguyên không âm, Z^+= {0,1,2,.....}***
- Tập hợp Z là đóng kín đối với các phép cộng, trừ và nhân, nhưng không đóng kín đối với phép chia.

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.1. SỐ HỌC CÁC SỐ NGUYÊN

- Cho hai số nguyên bất kỳ a và b , b > 1, ta luôn xác định được ***q*** và ***r*** sao cho (***r*** là phần dư)

$$a = b.q + r,\ 0 < r < b.$$

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.1. SỐ HỌC CÁC SỐ NGUYÊN

- *Ước số chung lớn nhất*:

$$d = GCD(a, b)$$

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.1. SỐ HỌC CÁC SỐ NGUYÊN

- *số nguyên tố:*

Một số nguyên a > 1 được gọi là số **nguyên tố**, nếu *a* không có ước số nào ngoài 1 và chính *a*; và *a* được gọi là **hợp số** nếu không phải là số nguyên tố.

- Một số nguyên n > 1 bất kỳ đều có thể viết dưới dạng:

$$n = p_1^{\alpha_1} . p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

Trong đó $p_1 , p_2 , \dots , p_k$ là các số nguyên tố khác nhau, $\alpha_1, \alpha_2 , \dots , \alpha_k$ là các số mũ nguyên dương.

- **Đây là dạng khai triển chính tắc của n**

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.1. SỐ HỌC CÁC SỐ NGUYÊN

- ***Định lý (1.7.1.1):*** *Nếu b > 0 và b | a thì gcd(a ,b) = b; Nếu a = bq + r thì gcd(a,b) = gcd(b,r).*

Ví dụ: với số a=27, b=6 thì a=b.4+3 và *gcd(27,6)=3 và gcd(6,3)=3*

- ***Bội số chung bé nhất:*** *m là bội số chung nhỏ nhất của a và b, và mọi bội số chung của a và b đều là bội của m.*

$$m = \mathbf{lcm(a\ ,b)}$$

- Với hai số nguyên dương a và b bất kỳ ta có quan hệ:

$$\boldsymbol{lcm(a,b).gcd(a,b) = a.b}$$

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.2. Đồng dư và phương trình đồng dư tuyến tính

- Hai số nguyên a và b là đồng dư (*congruent modulo*) với nhau theo môđun n, và viết a ≡ b (mod n), nếu (a−b) chia hết cho n. ➔ đồng dư ở đây được hiểu là a *mod* n dư b. ví dụ: 27≡9 (mod 6) tức 27-9=18 chia hết cho 6.

Cho dù không phải số nguyên ta có

If

$$a_1 \equiv b_1 \pmod{n}$$

and

$$a_2 \equiv b_2 \pmod{n},$$

then:

- $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$
- $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}$.

Phải là số nguyên mới có

$$a_1 a_2 \equiv b_1 b_2 \pmod{n}.$$

Hơn nữa,

$$(a \bmod n)(b \bmod n) \equiv ab \pmod{n},$$

or, equivalently,

$$((a \bmod n)(b \bmod n)) \bmod n = (ab) \bmod n.$$

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.2. Đồng dư và phương trình đồng dư tuyến tính

- Hai số nguyên thuộc cùng một lớp tương đương khi và chỉ khi chúng cho cùng một số dư nếu chia cho n. Ví dụ: 23 và 5 là những số cùng lớp vì khi chia cho 3 đều dư 2.
- Mỗi lớp tương đương được đại diện bởi một số duy nhất trong tập hợp: $Z_n = \{0, 1, 2, 3,...., n -1\}$ là số dư chung khi chia các số trong lớp đó cho n.
- Ví dụ: với n=25 thì $Z_{25} = \{0, 1, 2, ..., 24\}$,

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.2. Đồng dư và phương trình đồng dư tuyến tính

- Cho $a \in Z_n$. Một số nguyên $x \in Z_n$ được gọi là nghịch đảo của a theo mod n , nếu a.x ≡ 1 (mod n).

Ví dụ: a=5 và x=3 với n=7 vì 5.3 ≡ 1 (mod 7)

- Nếu có số x như vậy thì ta nói *a* là khả nghịch, và ký hiệu *x* là $a^{-1} \bmod n$
- Phép chia trong Z_n được định nghĩa như sau:

$$a : b \ (mod\ n) \ = \ a . b^{-1} \ (mod\ n)$$

- Phép chia chỉ thực hiện được khi b là khả nghịch theo $(mod\ n)$

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.2. Đồng dư và phương trình đồng dư tuyến tính

- Phương trình đồng dư tuyến tính: là phương trình có dạng

$$a.x \equiv b(mod\ n)$$

trong đó a, b, n là các số nguyên, n > 0, x là ẩn số.

- Phương trình đó có nghiệm khi và chỉ khi $b \equiv 0(mod\ d)$ (tức b chia hết cho d) và với $d = \gcd(a,n)$, và khi đó có đúng d nghiệm theo $(mod\ n)$, với $x_0 < d/n$, có $x = x_0, x_0 + \frac{d}{n}, x_0 + \frac{2d}{n}, x_0 + \frac{3d}{n}.., x_0 + \frac{d-1}{n}$

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.2. Đồng dư và phương trình đồng dư tuyến tính

- ***Định lý***: Giả sử các số nguyên $n_1, n_2, \ldots, n_k$ là từng cặp nguyên tố với nhau. Khi đó, hệ phương trình đồng dư tuyến tính sau có một nghiệm duy nhất theo $(mod\ n)$.

$$\begin{cases} x_1 \equiv a_1 \pmod{n_1} \\ x_2 \equiv a_2 \pmod{n_2} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_k \equiv a_k \pmod{n_k} \end{cases}$$

Với $n = n_1.n_2 \ldots . n_k$, $Ni = \frac{n}{ni}$.

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.3. Thặng dư thu gọn và phần tử nguyên thuỷ

- Tập $\boldsymbol{Z_n} = \{0,1,2,\ldots,n-1\}$ thường được gọi là tập các thặng dư đầy đủ theo *mod n* (**complete residue system modulo *n*)**, vì mọi số nguyên bất kỳ đều có thể tìm được trong $\boldsymbol{Z_n}$ một số đồng dư với mình (theo $mod\ n$).
- Tập $\boldsymbol{Z_n}$ là đóng đối với các phép tính **cộng, trừ và nhân** theo $mod\ n$, nhưng **không** đóng đối với phép **chia**, vì phép chia cho a theo $mod\ n$ chỉ có thể thực hiện được khi a và n nguyên tố với nhau, tức khi $\gcd(a, n) = 1$.
- Tập các thặng dư thu gọn theo $mod\ n$ (**reduced residue system modulo *n*)** được định nghĩa là tập $Z_n^* = \{a \in \boldsymbol{Z_n}: \gcd(a, n) = 1\}$, tức $\boldsymbol{Z_n^*}$ là tập con của $\boldsymbol{Z_n}$ bao gồm tất cả các phần tử nguyên tố với n

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.3. Thặng dư thu gọn và phần tử nguyên thuỷ

- ***Thặng dư thu gọn (Reduced residue system)***
- ***Phần tử nguyên thuỷ (primitive)***

- Ví dụ:Tập thặng dự đầy đủ của modulo 12 là $\mathbf{Z_n}$={0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11}.
- Các số 1, 5, 7 và 11 là các số nguyên từ tập trên có tính nguyên tố với 12 (tức *gdc(,12)*=1), do vậy tập thặng dư rút gọn sẽ là {1,5,7,11}.
- Số phần tử của tập là $\{\varphi(12) = 4\}$ được gọi là cấp $\varphi(n)$ của nhóm. Và có các tập thặng dư modulo 12 khác nữa, như sau:

  {13,17,19,23}, {−11,−7,−5,−1}, {−7,−13,13,31}, {35,43,53,61}

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.3. Thặng dư thu gọn và phần tử nguyên thuỷ

- Nếu p là một số nguyên tố thì $\boldsymbol{Z_p^*} = \{1,2,\dots,p-1\}$. Và khi đó khi đó $\forall\, b \in Z_p^* \;:\; b^{p-1} \equiv 1(mod\ p)$
- Một phần tử $g \in \boldsymbol{Z_n^*}$ có cấp m, nếu m là số nguyên dương bé nhất sao cho $g^m = 1$ trong $\boldsymbol{Z_n^*}$
- Nếu b có cấp $p-1$, tức $p-1$ là số mũ bé nhất thoả mãn công thức trên, thì các phần tử $b, b^2, \dots., b^{P-1}$ đều khác nhau và theo $mod\ p$, chúng lập thành $\boldsymbol{Z_p^*}$ là một nhóm ***cyclic*** và b là một phần tử sinh, hay *phần tử nguyên thuỷ* của nhóm.

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.4. Phương trình đồng dư bậc hai và thặng dư bậc hai

- Phương trình đồng dư bậc 2 là phương trình có dạng:

$$x^2 \equiv a(mod\ n)$$

trong đó n là một số nguyên dương, a là số nguyên với $\gcd(a, n) = 1$,và x là ẩn số.

  - Nếu phương trình có nghiệm thì a là thặng dư bậc 2 $(mod\ n)$
  - Nếu phương trình vô nghiệm thì a là bất thặng dư bậc 2 $(mod\ n)$

- Tập các số nguyên nguyên tố với n được phân hoạch thành hai tập con: tập Q_n các thặng dư bậc hai $mod\ n$, và tập $\overline{Q_n}$ các bất thặng dư $mod\ n$
- *Tiêu chuẩn Euler*: Số a là thặng dư bậc hai $(mod\ p)$ nếu và chỉ nếu $a^{\frac{p-1}{2}}$.

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.4. Phương trình đồng dư bậc hai và thặng dư bậc hai

- *Ký hiệu Legendre:* p là một số nguyên tố lẻ, $\forall a > 0$, ký hiệu $Legendre\ \left(\frac{a}{p}\right)$ được định nghĩa như sau:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, khi\ a \equiv 0 (mod\ p) \\ 1, khi\ a \in Q_p \\ -1, khi\ a \notin Q_p \end{cases}$$

- a là thặng dư bậc hai $mod\ p$ khi và chỉ khi $\left(\frac{a}{p}\right) = 1$

- Với mọi a ≥ 0, ta có: $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} (mod\ p)$

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.4. Phương trình đồng dư bậc hai và thặng dư bậc hai

- *Ký hiệu Jacobi:* $\forall n$ là một số nguyên lẻ, $\forall a > 0$, ký hiệu *Jacobi* $\left(\frac{a}{n}\right)$ được định nghĩa như sau: Giả sử a có khai triển chính tắc thành thừa số nguyên tố là $n = p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_k^{\alpha_k}$ thì

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}.\left(\frac{a}{p_2}\right)^{\alpha_2}\dots\left(\frac{a}{p_k}\right)^{\alpha_k}$$

- Tính chất:
  - Nếu $m_1 \equiv m_2 \ (mod\ n)$ thì $\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right)$
  - $\left(\frac{2}{n}\right) = \begin{cases} 1\ khi\ n \equiv \pm 1 (mod\ 8) \\ -1 khi\ n \equiv \pm 3 (mod\ 8) \end{cases}$
  - $\left(\frac{m_1.m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$
  - Nếu m và n đều là số lẻ, thì

$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right), khi\ m \equiv 3 (\text{mod}\ 4)\ \&\ n \equiv 3 (\text{mod}\ 4), \\ \left(\frac{n}{m}\right), khi\ m \equiv 1 (\text{mod}\ 4) \vee n \equiv 1 (\text{mod}\ 4). \end{cases}$$

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.5. Xác suất thống kê

- ***Không gian các sự kiện sơ cấp*** (hay không gian mẫu) $\Omega = \{s_1, s_2 \dots s_n\}$

- Phân bố xác suất P trên Ω được định nghĩa là một tập các số thực không âm $P = \{p_1, p_2, \dots, p_n\}$ có tổng $\sum p_i = 1$.
  - Số p_i được coi là xác suất của sự kiện sơ cấp s_i.
- Tập con $E \subseteq \Omega$ được gọi là một sự kiện. Xác suất của sự kiện E được định nghĩa bởi $p(E) = \sum_{s \in E} p(s)$
- Cho E_1 và E_2 là hai sự kiện, với $p(E_2) > 0$, xác suất có điều kiện của E_1 khi có E_2 , $p(E_1|E_2)$ được định nghĩa là

Công thức Bayes

1.7. Cơ sở toán học của lý thuyết mật mã

1.7.6. Tính bí mật hoàn toàn của một hệ mật mã

- Giả sử $S = (P, C, K, E, D)$ là một hệ mật mã với điều kiện $|P| = |C| = |K|$, tức các tập P, C, K có số các phần tử bằng nhau. Khi đó, hệ là bí mật hoàn toàn nếu và chỉ nếu mỗi khoá $\boldsymbol{K} \in K$ được dùng với xác suất bằng nhau là $1/|K|$, và với mọi $x \in P, y \in C$ có một khoá duy nhất $\boldsymbol{K} \in K$ sao cho $e_K(x) = y$