



TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN ĐIỆN TỬ - VIỄN THÔNG

BỘ MÔN ĐIỆN TỬ HÀNG KHÔNG VŨ TRỤ


Môn học:

LÝ THUYẾT MẬT MÃ

Giảng viên: TS. Hán Trọng Thanh
 Email: httbkhn@gmail.com

1/23/2016

1



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 Elgamal và chuẩn chữ ký số ECDSA;
- ✓ 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;
- ✓ Thăm mã tuyến tính, thăm mã vi sai và các vấn đề về xây dựng hệ mã bảo mật cho các ứng dụng.

2



Nội Dung

1. Chương 1. Tổng quan
 2. Chương 2. Mật mã khóa đối xứng
 3. Chương 3. Mật mã khóa công khai
 4. Chương 4. Hàm băm và chữ ký số
 5. Chương 5. Dây giả ngẫu nhiên và hệ mật dòng
 6. Chương 6. Kỹ thuật quản lý khóa
-

1/23/2016

3



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.
-

4



Nhiệm vụ của Sinh viên

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



5



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

6



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 gráfo “to write” or legein “to speak”).
- Sự phổ biến của máy tính và hệ thống thông tin liên lạc trong những năm 1960 đã tạo ra nhu cầu từ khu vực tư nhân bảo vệ thông tin dưới dạng số và cung cấp dịch vụ an ninh thông tin.
- DES: Tiêu chuẩn bảo mật dữ liệu được Feistel bắt đầu từ năm 1970 tại IBM và chấp thuận vào năm 1977 là một tiêu chuẩn xử lý thông tin liên bang Hoa Kỳ để bảo mật thông tin không được phân loại. DES là cơ chế mã hóa nổi tiếng nhất trong lịch sử.

7



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

- Diffie và Hellman xuất bản bài báo New Directions in Cryptography năm 1976: Mật mã khóa công cộng public-key cryptography; cơ chế trao đổi khóa mới; các tác giả chưa đề nghị phương án thực tế.
- 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 cộng khác dựa trên bài toán logarit rời rạc.

8



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

- Đóng góp quan trọng trong khóa công cộng là chữ ký số . Năm 1991 tiêu chuẩn chữ ký số đầu tiên ISO/IEC 9796 dựa trên thuật toán RSA
- Năm 1994 chính phủ Mỹ xuất bản Digital Signature Standard dựa trên cơ chế ElGamal.
- Hàng thế kỷ qua, mật mã là nghệ thuật viết mã và giải mã
- Trước: Chủ yếu trong thông tin quân sự và tình báo

9



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.

10



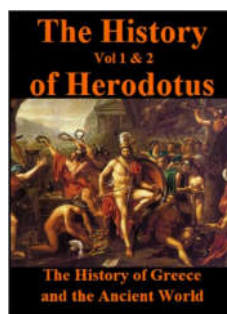
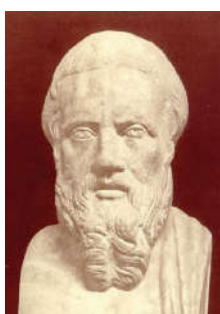
1.1. Giới thiệu sơ lược lịch sử khoa học mật mã

- 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.

11



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



Herodotos xứ Halikarnasseus, là một nhà sử học người Hy Lạp sống ở thế kỷ 5 trước Công nguyên (khoảng 484 TCN - 425 TCN), ông được coi là "người cha của môn sử học" trong văn hóa phương Tây.

12



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

Hy Lạp cổ xưa



Trong cuốn The Histories, Herodotus miêu tả về cuộc chiến giữa Hy Lạp và Ba Tư vào khoảng thế kỷ 5th B.C.

- ❑ Xerxes (Vua Ba Tư) đang thiết lập quân đội và lên kế hoạch tấn công bất ngờ Hy Lạp
- ❑ Demaratus, một người Hy Lạp bị trục xuất khỏi quê hương; đang sống ở Ba Tư đã gửi cảnh báo tới Hy Lạp:

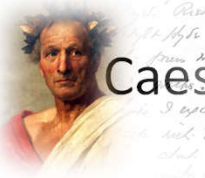
Ông đã cạo lớp sáp trên hai thanh gỗ dầy, viết lên đó lời cảnh báo, cuối cùng phủ một lớp sáp ra ngoài.

- ❑ *Người Hy Lạp, được cảnh báo, đã đảo ngược tình thế. Yếu tố bất ngờ của người Ba Tư đã mất, cuộc chiến của quân đội Ba Tư đã thất bại.*

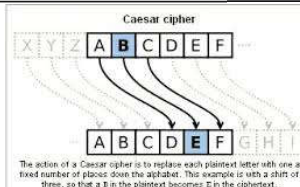
13



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



Caesar cipher



- ❑ Trong cuốn “Chiến tranh xứ Gaul”, Julius Caesar có miêu tả cách ông gửi thư cho Cicero – người bị vây hãm và đang ngập ngừng đầu hàng như thế nào
- ❑ Trong bức thư gửi Cicero, Caesar đã thay thế một số ký tự Roma bằng ký tự Hy Lạp để bức thư không thể đọc được bởi đối thủ.

14



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.

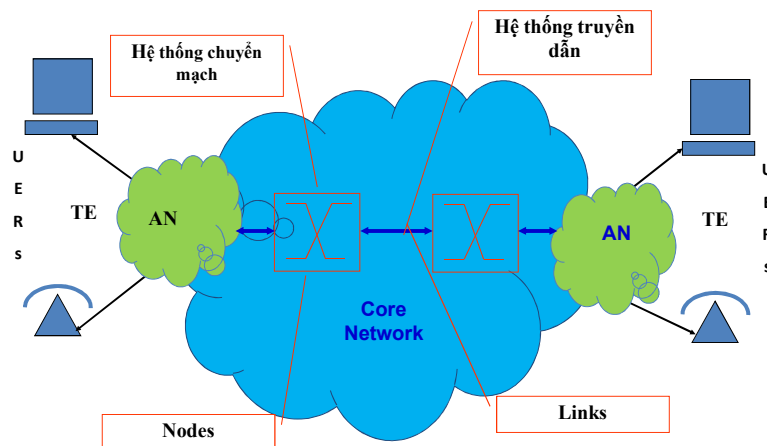
DVH Oderudwrub=



15



1.2. Khái niệm, mô hình của hệ mật



AN: Access Network ; TE: Terminal Equipment

16



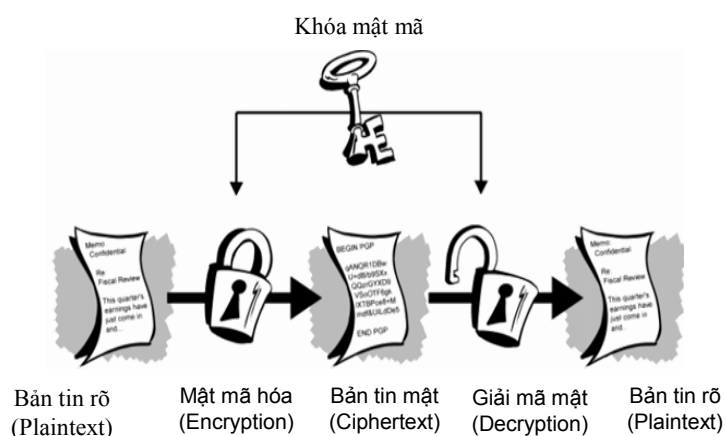
1.2. Khái niệm, mô hình của hệ mật

- Mật mã trước hết là một loại hoạt động thực tiễn, nội dung chính của nó là để giữ bí mật thông tin (chẳng hạn dưới dạng một văn bản) từ một người gửi A đến một người nhận B.
- 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”**

17



1.2. Khái niệm, mô hình của hệ mật



18



1.2. Khái niệm, mô hình của hệ mật

- Thuật toán lập/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

```

03003802 996CB7BA 08G0161B G0021C06
BA7CE203 G0030200 01208600 37D14D00
1B7125G0 024FG002 53D03C00 AD722500
1BD03C00 887525C1 01A07700 37D14D00
B7125G0 024FG002 53D03C00 AD722500
BD03C00 887525C1 4F5531 53414241
F4F3D41 4242434E 3D4A0 6469204
16C2F4F 553D4553 414A0 4F3D414
425604 00310230 042424 0003424
003042 4C000000 024E4E4F 00B1D3
1254F1 21000009 8B33B0CC 2957EE
3ECAA CB3E88EF DF038D7F A14217
2AA4D 04143B75 4F571C83 535C00
7DED9 B57C659E C820EE07 FA49F
96DB 7D7F743D 9A36DD29 454E0
014D 410800C8 9A54E072 5A140

```

19



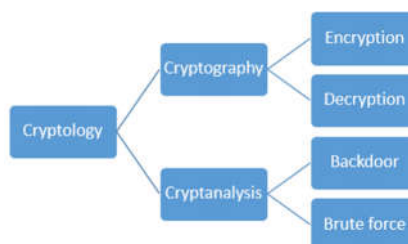
1.2. Khái niệm, mô hình của hệ mật

- Ngược lại của mật mã là **thăm mã**
 - Thực hiện bài toán: “**Tìm chìa khóa mật mã**”
- Không thể xây dựng một hệ mật (Cryptosystem) tốt nếu không hiểu biết sâu về thăm mã.
- Một giải pháp mật mã là bảo đảm bí mật, nếu mọi thuật toán thăm mã, nếu có, đều phải được thực hiện với độ phức tạp tính toán cực lớn.

Mật mã học (Cryptography)

=

**Mật mã (Cryptography) +
Thăm mã (Cryptanalysis)**



20



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

$$S = (P, C, K, E, D)$$

Thỏa mãn các điều kiện sau đây:

- Tập nguồn P là tập hữu hạn tất cả các bản tin nguồn cần mã hóa có thể có.
- C là một tập hữu hạn các ký tự bản mã
- K là tập hữu hạn các khóa có thể được sử dụng
- E là một ánh xạ từ $K \times P$ vào C , được gọi là phép lập mật mã
- D là một ánh xạ từ $K \times C$ vào P , được gọi là phép giải mã

21



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

$$S = (P, C, K, E, D)$$

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

22



1.3. Một số hệ mật ban đầu

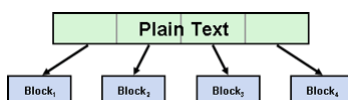
➤ Mã theo khối (Block cipher)

- Độ dài khối (k)
- Không gian khóa k được mở rộng từ $K \rightarrow K^k$
- 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 $x_1 \dots x_k \in P^k$ và $y_1 \dots y_k \in C^k$ ta có

$$e_K(x_1 \dots x_k) = e_{K_1}(x_1) \dots e_{K_k}(x_k)$$

$$d_K(y_1 \dots y_k) = d_{K_1}(y_1) \dots d_{K_k}(y_k)$$



23



1.3. Một số hệ mật ban đầu

➤ 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:

$$e_K(X) = e_K(x_1 \dots x_m) = e_{K_1}(x_1) \dots e_{K_m}(x_m)$$

- Giải mã $Y = e_K(X)$ ta được:

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

24



1.3. Một số hệ mật ban đầu

➤ 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 được xác định bởi:

$$e_K(x) = x + K \bmod (2)$$

$$d_K(y) = y + K \bmod (2)$$

$$K = 0 \text{ hoặc } 1$$

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

25



1.3. Một số hệ mật ban đầu

➤ Mật mã khóa đối xứng

- Trong một giao dịch truyền tin bảo mật:
 - ✓ Người A gửi cho người B bản tin bảo mật với quy ước trước một khóa chung K .
 - A dùng e_K để lập mật mã
 - B dùng d_K để giải mã bản mật
- Nhận xét:

26



1.3. Một số hệ mật ban đầu

➤ Mật mã 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.

27



1.3. Một số hệ mật ban đầu

➤ Mật mã khóa công khai

Hệ mật mã với cách sử dụng đó là
“Mật mã phi đối xứng”

Nhận xét:

Hệ mật mã với cách sử dụng đó là
“Hệ Mật mã khóa công khai”

28



1.4. Các bài toán an toàn thông tin

- *Bảo mật:*
 - *Toàn vẹn thông tin*
 - *Nhận thực một thực thể:*
 - *Nhận thực một thông báo:*
-

29



1.4. Các bài toán an toàn thông tin

- *Ủy quyền:*
 - *Cấp chứng chỉ:*
 - *Báo nhận:*
 - *Làm chứng:*
-

30



1.4. Các bài toán an toàn thông tin

- *Không chối bỏ được:*
- *Ẩn danh:*
- *Thu hồi:*
- *Chữ ký:*

31



1.4. Các bài toán an toàn thông tin

privacy or confidentiality	Tính riêng tư hoặc tính bí mật	keeping information secret from all but those who are authorized to see it.
Data integrity	Tính toàn vẹn dữ liệu	ensuring information has not been altered by unauthorized or unknown means.
Entity authentication or identification	Nhận thực thực thể hoặc định danh	corroboration of the identity of an entity (e.g., a person, a computer terminal, a credit card, etc.).
Message authentication	Nhận thực bản tin	corroborating the source of information; also known as data origin authentication.
Signature	Chữ ký	a means to bind information to an entity
Authorization	Tác quyền	conveyance, to another entity, of official sanction to do or be something.

32



1.4. Các bài toán an toàn thông tin

Validation	Tính hợp lệ	a means to provide timeliness of authorization to use or manipulate information or resources.
Access control	Điều khiển truy nhập	restricting access to resources to privileged entities
Certification	Chứng nhận	endorsement of information by a trusted entity
timestamping	Nhãn thời gian	recording the time of creation or existence of information
Witnessing	Chứng thực	verifying the creation or existence of information by an entity other than the creator
Receipt	Biên nhận	acknowledgement that information has been received
Confirmation	Xác nhận	acknowledgement that services have been provided

33



1.4. Các bài toán an toàn thông tin

Ownership	Quyền sở hữu	a means to provide an entity with the legal right to use or transfer a resource to others
Anonymity	Nặc danh	concealing the identity of an entity involved in some process
Non-repudiation	Chống sự từ chối	preventing the denial of previous commitments or actions
Revocation	Thu hồi	retraction of certification or authorization



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.
- 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.

35

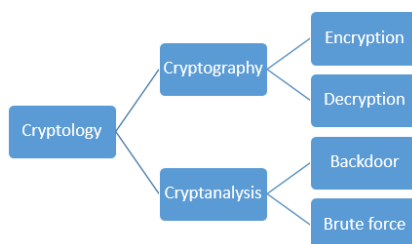


1.5. Thám mã

Mật mã học (Cryptology)

=

Mật mã (Cryptography) + Thám mã (Cryptanalysis)



36



1.5. Thám mã

- Các bài toán thám mã:
 - *Thám mã chỉ biết bản mã :*
 - *Thám mã khi biết cả bản rõ:*
 - *Thám mã khi có bản rõ được chọn:*
 - *Thám mã khi có bản mã được chọn:*

37



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:

38



1.6. Tính an toàn của các hệ mật mã

- An toàn vô điều kiện:
- An toàn được chứng minh:
- An toàn tính toán:

39



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, $Z^+ = \{0, 1, 2, ..., \infty\}$
- Tập hợp Z là đóng kín đối với các phép cộng, trừ và nhân, nhưng không đóng kín đối với phép chia.

40



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 , $b > 1$

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

41



1.7. Cơ sở toán học của lý thuyết mật mã

1.7.1. SỐ HỌC CÁC SỐ NGUYÊN

➤ Ước số chung lớn nhất:

$$d = \text{GCD}(a, b)$$

42



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 được gọi là hợp số, nếu không phải là số nguyên tố.

➤ Hai số a và b được gọi là nguyên tố với nhau.

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

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 $b \nmid a$ thì $\gcd(a, b) = b$; Nếu $a = bq + r$ thì $\gcd(a, b) = \gcd(b, r)$.

➤ **Bội số chung bé nhất:** m là bội số chung của a và b , và mọi bội số chung của a và b đều là bội của m . $m = \text{lcm}(a, b)$

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

$$\text{lcm}(a, b) \cdot \gcd(a, b) = a \cdot b$$



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 với nhau theo môđun n , và viết $a \equiv b \pmod{n}$, nếu $(a-b)$ chia hết cho n .
- Hai số nguyên thuộc cùng một lớp tương đương khi và chỉ khi chúng cho cùng một số dư nếu chia cho n .
- Mỗi lớp tương đương được đại diện bởi một số duy nhất trong tập hợp: $Z_n = \{0, 1, 2, 3, \dots, n-1\}$ là số dư chung khi chia các số trong lớp đó cho n .
- Ví dụ: với $Z_{25} = \{0, 1, 2, \dots, 24\}$,

45



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

$$a : b \pmod{n} = a \cdot b^{-1} \pmod{n}$$
- Phép chia chỉ thực hiện được khi b là khả nghịch theo \pmod{n} .

46



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

$$a.x \equiv b(\text{mod } n)$$

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

- Phương trình đó có nghiệm khi và chỉ khi $d = \text{gcd}(a, n) | b$, và khi đó nó có đúng d nghiệm theo $(\text{mod } n)$

47



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, \dots, 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 $(\text{mod } n)$.

$$\begin{cases} x_1 \equiv a_1 (\text{mod } n_1) \\ x_2 \equiv a_2 (\text{mod } n_2) \\ \dots\dots\dots \\ x_k \equiv a_k (\text{mod } n_k) \end{cases} \quad \text{Với } n = n_1 \cdot n_2 \dots n_k, N_i = \frac{n}{n_i}.$$

48



1.7. Cơ sở toán học của lý thuyết mật mã

1.7.3. Thặng dư thu gọn và phân tử nguyên thủy

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

49



1.7. Cơ sở toán học của lý thuyết mật mã

1.7.3. Thặng dư thu gọn và phân tử nguyên thủy

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

50



1.7. Cơ sở toán học của lý thuyết mật mã

1.7.3. Thặng dư thu gọn và phần tử nguyên thủy

- Số các phần tử trong một nhóm là cấp $\varphi(n)$ của nhóm đó.
- Một phần tử $g \in \mathbf{Z}_n^*$ có cấp m , nếu m là số nguyên dương bé nhất sao cho $g^m = 1$ trong \mathbf{Z}_n^*
- Nhóm \mathbf{Z}_n^* có cấp $\varphi(n)$, và nếu p là số nguyên tố thì nhóm \mathbf{Z}_p^* có cấp $p - 1$. khi đó $\forall b \in \mathbf{Z}_p^* : b^{p-1} \equiv 1 \pmod{p}$
- 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 \pmod{p} , chúng lập thành \mathbf{Z}_p^* là một nhóm *cyclic* và b là một phần tử sinh, hay *phần tử nguyên thủy* của nhóm.

51



1.7. Cơ sở toán học của lý thuyết mật mã

1.7.3. Thặng dư thu gọn và phần tử nguyên thủy

Các tính chất của phần tử nguyên thủy:

52



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:

$$x^2 \equiv a \pmod{n}$$

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 \pmod{n}
 - Nếu phương trình vô nghiệm thì a là bất thặng dư bậc 2 \pmod{n}
- Tập các số nguyên nguyên tố với n được phân hoạch thành hai tập con: tập Q_n các thặng dư bậc hai \pmod{n} , và tập \overline{Q}_n các bất thặng dư \pmod{n}
- *Tiêu chuẩn Euler*: Số a là thặng dư bậc hai \pmod{p} nếu và chỉ nếu $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

53



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:

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

- a là thặng dư bậc hai \pmod{p} khi và chỉ khi $\left(\frac{a}{p}\right) = 1$
- Với mọi $a \geq 0$, ta có: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

54



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

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

- Tính chất:

- Nếu $m_1 \equiv m_2 \pmod{n}$ thì $\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right)$
- $\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{khi } n \equiv \pm 1 \pmod{8} \\ -1 & \text{khi } n \equiv \pm 3 \pmod{8} \end{cases}$
- $\left(\frac{m_1 \cdot m_2}{n}\right) = \left(\frac{m_1}{n}\right) \left(\frac{m_2}{n}\right)$
- Nếu m và n đều là số lẻ, thì $\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right), & \text{khi } m \equiv 3 \pmod{4} \text{ \& } n \equiv 3 \pmod{4}, \\ \left(\frac{n}{m}\right), & \text{khi } m \equiv 1 \pmod{4} \vee n \equiv 1 \pmod{4}. \end{cases}$

55



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

56



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 $K \in K$ được dùng với xác suất bằng nhau là $1/|K|$, và với mọi $x \in P, y \in C$ có một khoá duy nhất $K \in K$ sao cho $e_K(x) = y$