BG Chương I. Giới thiệu về Mật mã và An toàn thông tin

Trong chương này, tổng quan một cách ngắn gọn về mật mã và các kỹ thuật mật mã được giới thiệu. Phần trình bày chi tiết và chặt chẽ các công cụ và kỹ thuật mật mã sẽ ở các chương sau. Phần giới thiệu này chỉ là bản tóm tắt, phi kỹ thuật, phi toán học về mật mã.

1.1 Cryptosystems and Basic Cryptographic Tools

Các hệ mật và các công cụ mật mã cơ bản

Trong phần nay, các khái niệm cơ bản về mật mã được thảo luận:

- Mật mã khóa bí mật
- Mật mã khóa công khai
- Mã khối
- Mã dòng
- Mã lai

1.1.1Secret-key Cryptosystems

Mật mã đã được sử dụng hàng ngàn năm để đảm bảo liên lạc bí mật. Ở dạng cơ bản nhất đó là sự liên lạc giữa hai người, thường được ký hiệu là A (Alice) và B (Bob), đã thống nhất một khóa bí mật. . Sau đó, Alice có thể muốn gửi một tin nhắn bí mật cho Bob (hoặc Bob có thể muốn gửi một tin nhắn cho Alice). Khóa được sử dụng để chuyển đổi thông điệp gốc (thường được gọi là văn bản gốc) thành dạng xáo trộn mà bất kỳ ai không có khóa đều không thể hiểu được. Quá trình này được gọi là mã hóa và thông điệp được mã hóa được gọi là bản mã. Khi Bob nhận được bản mã, anh ta có thể sử dụng khóa để chuyển đổi bản mã trở lại bản rõ ban đầu; đây là quá trình giải mã. Một hệ mật bao gồm một đặc tả đầy đủ về các khóa và cách chúng được sử dụng để mã hóa và giải mã thông tin.

Trong suốt chiều dài lịch sử đã có nhiều hệ mật với độ phức tạp ngày càng tăng. Các ứng dụng mật mã bao gồm đảm bảo an toàn cho sự liên lạc giuaz các nhà lãnh đạo chính trị hoặc hàng gia, các cuộc diễn tập quan sự, … tuy nhiên, với sự phát triển của Internet và các ứng dụng khác như thương mại điện từ, nhiều ứng dụng đa dạng khác của Mật mã đã xuất hiện. Trong đó bao gồm các ứng dụng: mã hóa mật khẩu, số thẻ tín dụng, email, tài liệu, các files và các phương tiện kỹ thuật số.

Các kỹ thuật mã hóa được sử dụng rộng rãi để bảo vệ dữ liệu được lưu trữ bên cạnh dữ liệu được truyền từ nơi này đến nơi khác. Ví dụ, người dùng có thể muốn mã hóa dữ liệu được lưu trữ trên máy tính xách tay, trên đĩa cứng ngoài, trên đám mây, trong cơ sở dữ liệu, … Ngoài ra, rất hữu ích nếu có thể thực hện tính toán trên các dữ liệu đã được mã hóa (mà không cần giải mã dữ liệu trước).

Việc phát triển và triển khai một hệ mật phải đảm bảo sự bảo mật. Theo truyền thống, mối đe dọa mà mật mã phải giải quyết là kẻ địch có thể chặn bắt bản mã và tìm cách giải nó. Nếu kẻ địch tình cờ sở hữu được khóa mã thì không có cách nào khắc phục được. Do đó, việc xem xét bảo mật với giả thiết kẻ tấn công không sở hữu khóa, nhưng vẫn cố gắng giải mã. Các kỹ thuật mà kẻ tấn công sử dụng để cố gắng “phá vỡ” hệ mật được gọi là phân tích mật mã. Dạng phân tích mật mã thường gặp nhất là đoán khóa mã. Kẻ tấn công cố giải mã bằng tất cả các khóa có thể, gọi là phương pháp vét cạn. Khi kẻ tấn công thử đúng khóa, bản rõ được tìm thấy, nhưng khi thử bằng khóa khác thì chỉ nhận được văn bản vô nghĩa. Vì vậy, bước đầu tiên thiết kế một hệ mật an toàn là cần phải tạo ra số khóa có thể lớn đến mức không thể kiểm tra hết tất cả các khóa trong một khoảng thời gian hợp lý.

Mô hình mật mã được mô tả ở trên thường được gọi là mật mã khóa bí mật. Điều này chỉ ra rằng có một khóa bí mật mà cả Alice và Bob đều biết. Nghĩa là, khóa mã là một “Bí mật” cả hai đề biết. Khóa mã này được dùng cả để mã hóa bnar rõ và giải mã bản mã. Do đó, hàm mã hóa và hàm giải mã là nghịch đảo của nhau. Một số hệ mật khóa bí mật được giới thiệu và thám mã trong chương 2 và 3.

Hạn chế của mật mã khóa bí mật là Alice và Bob bằng cách nào đó phải có khả năng thỏa thuận trước về khóa bí mật (trước khi họ muốn gửi bất kỳ tin nhắn nào cho nhau). Điều này có thể đơn giản nếu Alice và Bob ở cùng một nơi khi họ chọn khóa bí mật. Nhưng điều gì sẽ xảy ra nếu Alice và Bob ở xa nhau, chẳng hạn như ở các châu lục khác nhau? Khi đó, một giải pháp khả thi là Alice và Bob sử dụng hệ thống mật mã khóa công khai.

1.1.2 Public-key Cryptosystems
Hệ mật khóa công khai

Ý tưởng mang tính cách mạng về mật mã khóa công khai được Diffie và Hellman đưa ra vào những năm 1970. Ý tưởng của họ là có thể tạo ra một hệ mật mã trong đó có hai khóa riêng biệt. Khóa chung sẽ được sử dụng để mã hóa bản rõ và khóa riêng sẽ cho phép giải mã bản mã. Lưu ý rằng "tất cả mọi người" có thể biết khóa chung, trong khi khóa riêng chỉ được biết bởi một người (cụ thể là người nhận tin nhắn được mã hóa). Vì vậy, một hệ mật mã khóa công khai sẽ cho phép bất kỳ ai mã hóa một tin nhắn để truyền tới Bob, và chỉ Bob mới có thể giải mã được tin nhắn đó. Ví dụ đầu tiên và nổi tiếng nhất về hệ mật mã khóa công khai là Hệ mật mã RSA được phát minh bởi Rivest, Shamir và Adleman. Nhiều loại hệ mật mã khóa công khai khác nhau được trình bày trong Chương 6, 7 và 9.

Mật mã khóa công khai giúp hai bên không cần phải thống nhất về khóa bí mật chung trước đó. Tuy nhiên, vẫn cần phải đưa ra một phương pháp phân phối khóa công khai một cách an toàn. Nhưng đây không hẳn là một mục tiêu tầm thường cần đạt được, vấn đề chính là tính chính xác hoặc tính xác thực của các khóa công khai có mục đích. Chứng chỉ, mà chúng ta sẽ thảo luận sau, là một phương pháp phổ biến để giải quyết vấn đề này.

1.1.3 Block and Stream Ciphers
Mã khối và mã dòng

Các hệ mật mã thường được phân loại thành mật mã khối hoặc mật mã dòng. Trong mật mã khối, bản rõ được chia thành các khối có kích thước cố định gọi là khối. Một khối được chỉ định là một chuỗi bit (tức là chuỗi 0 và 1) có độ dài cố định nào đó (ví dụ: 64 hoặc 128 bit). Mật mã khối sẽ mã hóa (hoặc giải mã) từng khối một. Ngược lại, mật mã dòng trước tiên sử dụng khóa để xây dựng dòng khóa, là chuỗi bit có độ dài chính xác bằng văn bản gốc (văn bản gốc là chuỗi bit có độ dài tùy ý). Hoạt động mã hóa xây dựng văn bản mã hóa là văn bản độc quyền hoặc của văn bản gốc và dòng khóa. Việc giải mã được thực hiện bằng cách tính toán độc quyền hoặc của bản mã và dòng khóa. Hệ mật mã khóa công khai luôn là mật mã khối, trong khi hệ thống mật mã khóa bí mật có thể là mật mã khối hoặc mật mã dòng. Mật mã khối được nghiên cứu chi tiết ở Chương 4.

1.1.4 Hybrid Cryptography
Mật mã lai

Một trong những nhược điểm của hệ mật mã khóa công khai là chúng chậm hơn nhiều so với hệ mật mã khóa bí mật. Do đó, hệ mật mã khóa công khai chủ yếu được sử dụng để mã hóa một lượng nhỏ dữ liệu, ví dụ: số thẻ tín dụng. Tuy nhiên, có một cách hay để kết hợp mật mã khóa bí mật và khóa công khai để đạt được lợi ích của cả hai. Kỹ thuật này được gọi là mật mã lai. Giả sử Alice muốn mã hóa một tin nhắn “dài” và gửi nó cho Bob. Giả sử Alice và Bob không có khóa bí mật chung trước đó. Alice có thể chọn một khóa bí mật ngẫu nhiên và mã hóa bản rõ bằng cách sử dụng hệ mật mã khóa bí mật (nhanh). Sau đó Alice mã hóa khóa bí mật này bằng khóa chung của Bob. Alice gửi bản mã và khóa mã hóa cho Bob. Đầu tiên Bob sử dụng khóa giải mã riêng của mình để giải mã khóa bí mật, sau đó anh ấy sử dụng khóa bí mật này để giải mã bản mã

Lưu ý rằng hệ mật mã khóa công khai “chậm” chỉ được sử dụng để mã hóa khóa bí mật ngắn. Hệ mật mã khóa bí mật nhanh hơn nhiều được sử dụng để mã hóa bản rõ dài hơn. Do đó, mật mã lai (gần như) đạt được hiệu quả của mật mã khóa bí mật, nhưng nó có thể được sử dụng trong trường hợp Alice và Bob không có khóa bí mật được thỏa thuận trước đó.

1.2 Message Integrity
Tính toàn vẹn Dữ liệu

Phần này thảo luận về các công cụ khác nhau giúp đạt được tính toàn vẹn của dữ liệu, bao gồm mã xác thực tin nhắn (MAC), sơ đồ chữ ký và hàm băm.

Các hệ mật mã cung cấp tính bí mật (tương đương, tính bảo mật) chống lại kẻ địch nghe lén, thường được gọi là kẻ địch thụ động. Kẻ địch thụ động được cho là có thể truy cập bất kỳ thông tin nào đang được gửi từ Alice đến Bob; xem Hình 1.1. Tuy nhiên, có nhiều mối đe dọa khác mà chúng ta muốn chống lại, đặc biệt khi có sự hiện diện của một đối thủ đang hoạt động tích cực. Kẻ địch tích cực là kẻ có thể thay đổi thông tin được truyền từ Alice sang Bob.

Hình 1.2 mô tả một số hành động có thể xảy ra của một đối thủ tích cực. Một kẻ địch tích cực có thể

• thay đổi thông tin được gửi từ Alice tới Bob,

• gửi thông tin cho Bob theo cách mà Bob cho rằng thông tin đó có nguồn gốc từ Alice, hoặc

• chuyển hướng thông tin được gửi từ Alice đến Bob theo cách mà bên thứ ba (Charlie) nhận được thông tin này thay vì Bob.

Các mục tiêu có thể có của một kẻ địch tích cực có thể bao gồm việc đánh lừa Bob (ví dụ) chấp nhận thông tin "không có thật" hoặc đánh lừa Bob về việc ai đã gửi thông tin cho anh ta ngay từ đầu.

Chúng ta nên lưu ý rằng bản thân mã hóa không thể bảo vệ khỏi các kiểu tấn công tích cực này. Ví dụ: mật mã dòng dễ bị tấn công lật bit. Nếu một số bit bản mã bị “lật” (tức là số 0 được thay thế bằng số 1 và ngược lại), thì hiệu ứng là lật các bit văn bản gốc tương ứng. Do đó, kẻ tấn công có thể

sửa đổi bản rõ theo cách có thể dự đoán được, mặc dù kẻ tấn công không biết các bit bản rõ là gì.

Có nhiều cách đảm bảo “tính toàn vẹn” khác nhau mà chúng ta có thể tìm cách cung cấp để bảo vệ trước các hành động có thể xảy ra của một kẻ địch tích cực. Kẻ địch như vậy có thể thay đổi thông tin đang được truyền từ Alice sang Bob (và lưu ý rằng thông tin này có thể được mã hóa hoặc không). Ngoài ra, kẻ địch có thể cố gắng “giả mạo” một tin nhắn và gửi nó cho Bob với hy vọng rằng anh ta sẽ nghĩ rằng nó có nguồn gốc từ Alice. Các công cụ mật mã bảo vệ chống lại những mối đe dọa này và các loại mối đe dọa liên quan có thể được xây dựng trong cả cài đặt khóa bí mật và khóa chung. Trong cài đặt khóa bí mật, chúng ta sẽ thảo luận ngắn gọn về khái niệm mã xác thực tin nhắn (hoặc MAC). Trong cài đặt khóa công khai, công cụ phục vụ mục đích gần giống nhau là sơ đồ chữ ký.

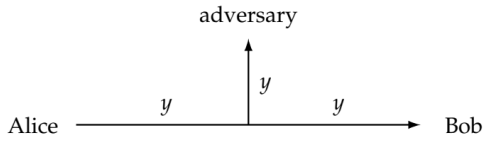
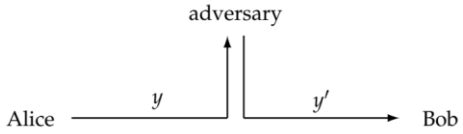
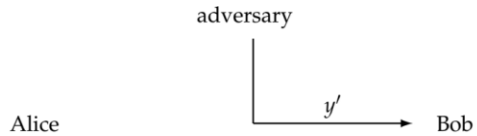


FIGURE 1.1: A passive adversary



or



or

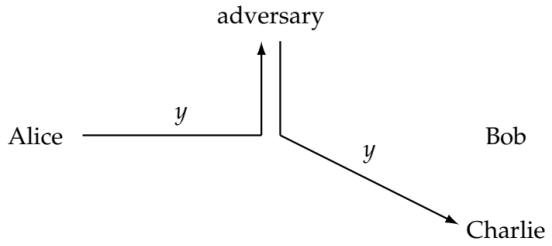


FIGURE 1.2: Active adversaries

1.2.1Message Authentication Codes (MAC) Mã hóa xác thực thông điệp (MAC)

Mã xác thực tin nhắn yêu cầu Alice và Bob chia sẻ khóa bí mật. Khi Alice muốn gửi tin nhắn cho Bob, cô ấy sử dụng khóa bí mật để tạo một thẻ mà cô ấy gắn vào tin nhắn (thẻ này phụ thuộc vào cả khóa và tin nhắn). Khi Bob nhận được tin nhắn và thẻ, anh ta dùng chìa khóa để tính lại thẻ và kiểm tra xem nó có giống với thẻ mà anh ta nhận được hay không. Nếu vậy, Bob chấp nhận tin nhắn này như một tin nhắn xác thực từ Alice; nếu không thì Bob sẽ từ chối tin nhắn vì tin nhắn đó không hợp lệ. Chúng tôi lưu ý rằng tin nhắn có thể được mã hóa hoặc không. MAC được thảo luận trong Chương 5.

Nếu không cần bảo mật thì tin nhắn có thể được gửi dưới dạng bản rõ. Tuy nhiên, nếu muốn bảo mật thì bản rõ sẽ được mã hóa và sau đó thẻ sẽ được tính toán trên bản mã. Đầu tiên Bob sẽ xác minh tính chính xác của thẻ. Nếu thẻ đúng thì Bob sẽ giải mã bản mã. Quá trình này thường được gọi là mã hóa-sau đó-MAC (xem Phần 5.5.3 để thảo luận chi tiết hơn về chủ đề này).

Để một MAC được coi là an toàn, kẻ tấn công sẽ không thể tính toán được thẻ chính xác cho bất kỳ tin nhắn nào mà chúng chưa thấy thẻ hợp lệ. Giả

sử chúng ta giả sử rằng Alice và Bob đang sử dụng một MAC an toàn (và giả sử rằng đối phương không biết khóa bí mật mà họ đang sử dụng). Sau đó, nếu Bob nhận được một tin nhắn và một thẻ hợp lệ, anh ta có thể tin tưởng rằng Alice đã tạo thẻ trên tin nhắn đã cho (với điều kiện Bob không tự tạo ra nó) và cả tin nhắn lẫn thẻ đều không bị kẻ địch thay đổi. Bob có thể đưa ra kết luận tương tự khi nhận được tin nhắn từ Alice, cùng với một thẻ chính xác.

1.2.2Signature Schemes
Các sơ đồ chữ ký

Trong cài đặt khóa công khai, sơ đồ chữ ký cung cấp sự đảm bảo tương tự như sơ đồ do MAC cung cấp. Trong sơ đồ chữ ký, khóa riêng chỉ định thuật toán ký mà Alice có thể sử dụng để ký tin nhắn. Tương tự như MAC, thuật toán ký tạo ra một đầu ra, trong trường hợp này được gọi là chữ ký, phụ thuộc vào thông báo được ký cũng như khóa. Chữ ký sau đó sẽ được thêm vào tin nhắn. Lưu ý rằng thuật toán ký chỉ có Alice biết. Mặt khác, có một thuật toán xác minh là khóa chung (được mọi người biết đến). Thuật toán xác minh lấy đầu vào là một thông báo và chữ ký, sau đó đưa ra giá trị đúng hoặc sai để cho biết liệu chữ ký có được chấp nhận là hợp lệ hay không. Một tính năng hay của sơ đồ chữ ký là bất kỳ ai cũng có thể xác minh chữ ký của Alice trên các tin nhắn, miễn là họ có bản sao xác thực khóa xác minh của Alice. Ngược lại, trong cài đặt MAC, chỉ Bob mới có thể xác minh các thẻ do Alice tạo (khi Alice và Bob chia sẻ khóa bí mật). Lược đồ chữ ký được nghiên cứu trong Chương 8.

Các yêu cầu bảo mật đối với sơ đồ chữ ký cũng tương tự như MAC. Kẻ địch sẽ không thể tạo được chữ ký hợp lệ trên bất kỳ tin nhắn nào chưa được Alice ký trước đó. Do đó, nếu Bob (hoặc bất kỳ ai khác) nhận được một tin nhắn và một thẻ hợp lệ (tức là thẻ có thể được xác minh bằng thuật toán xác minh công khai của Alice), thì người nhận có thể tin tưởng rằng chữ ký đó được tạo bởi Alice chứ không phải tin nhắn cũng như chữ ký đã bị kẻ địch sửa đổi.

Một ứng dụng phổ biến của chữ ký là tạo điều kiện thuận lợi cho việc cập nhật phần mềm an toàn. Khi người dùng mua phần mềm từ một trang web trực tuyến, phần mềm đó thường bao gồm thuật toán xác minh sơ đồ chữ ký. Sau này, khi tải xuống phiên bản cập nhật của phần mềm, nó sẽ bao gồm chữ ký (trên phần mềm đã cập nhật). Chữ ký này có thể được xác

minh bằng thuật toán xác minh đã được tải xuống khi mua phiên bản gốc của phần mềm. Điều này cho phép máy tính của người dùng xác minh rằng bản cập nhật đến từ cùng một nguồn với phiên bản gốc của phần mềm.

Lược đồ chữ ký có thể được kết hợp với lược đồ mã hóa khóa công khai để cung cấp tính bảo mật cùng với sự đảm bảo tính toàn vẹn của lược đồ chữ ký. Giả sử Alice muốn gửi một tin nhắn (ngắn) có chữ ký, mã hóa cho Bob. Trong tình huống này, kỹ thuật được sử dụng phổ biến nhất là trước tiên Alice tạo chữ ký trên bản rõ bằng thuật toán ký riêng của mình, sau đó mã hóa bản rõ và chữ ký bằng khóa mã hóa công khai của Bob. Khi Bob nhận được tin nhắn, trước tiên anh ấy sẽ giải mã nó và sau đó kiểm tra tính hợp lệ của chữ ký. Quá trình này được gọi là đăng nhập rồi mã hóa; lưu ý rằng theo một nghĩa nào đó, đây là sự đảo ngược của quy trình “mã hóa-sau-MAC” được sử dụng trong cài đặt khóa bí mật.

1.2.3Nonrepudiation
Chống chối bỏ

Có một sự khác biệt hơi khó nhận thấy giữa MAC và sơ đồ chữ ký. Trong sơ đồ chữ ký, thuật toán xác minh là công khai. Điều này có nghĩa là chữ ký có thể được xác minh bởi bất kỳ ai. Vì vậy, nếu Bob nhận được tin nhắn từ Alice có chữ ký hợp lệ của cô ấy trên tin nhắn, anh ấy có thể hiển thị tin nhắn và chữ ký cho bất kỳ ai khác và tin tưởng rằng bên thứ ba cũng sẽ chấp nhận chữ ký là hợp lệ. Do đó, Alice không thể ký vào một tin nhắn và sau đó cố gắng khẳng định rằng cô ấy không ký vào tin nhắn đó, một đặc tính được gọi là tính không chối bỏ. Điều này rất hữu ích trong việc thiết lập các hợp đồng, trong đó chúng tôi không muốn ai đó có thể từ bỏ hợp đồng đã ký bằng cách tuyên bố (sai) rằng họ chữ ký đã bị "giả mạo", ví dụ

Tuy nhiên, đối với MAC, không có khả năng xác minh của bên thứ ba vì khóa bí mật được yêu cầu để xác minh tính chính xác của thẻ và khóa này chỉ có Alice và Bob biết. Ngay cả khi khóa bí mật được tiết lộ cho bên thứ ba (ví dụ: do lệnh của tòa án), không có cách nào để xác định xem thẻ được tạo bởi Alice hay Bob, bởi vì bất cứ điều gì Bob có thể làm, Alice cũng có thể làm như được và ngược lại. Vì vậy, MAC không cung cấp khả năng chống chối bỏ và vì lý do này, MAC đôi khi được gọi là có thể từ chối.” Tuy nhiên, điều thú vị cần lưu ý là có những tình huống mong muốn sự phủ nhận. Đây có thể là trường hợp trong giao tiếp thời gian thực, trong

đó Alice và Bob muốn được đảm bảo về tính xác thực của giao tiếp của họ khi chúng diễn ra, nhưng họ không muốn tồn tại một bản ghi vĩnh viễn, có thể kiểm chứng được về giao tiếp này. Sự giao tiếp như vậy tương tự như một cuộc trò chuyện "không được ghi lại", ví dụ, giữa một nhà báo và một nguồn ẩn danh. MAC rất hữu ích trong bối cảnh các cuộc trò chuyện kiểu này, đặc biệt nếu bạn cẩn thận sau cuộc trò chuyện đã xong, hãy xóa các khóa bí mật được sử dụng trong quá trình liên lạc.

1.2.4Certificates
Chứng chỉ

Ở trên chúng ta đã đề cập rằng việc xác minh tính xác thực của khóa công khai trước khi chúng được sử dụng là điều quan trọng. Chứng chỉ là một công cụ phổ biến giúp đạt được mục tiêu này. Chứng chỉ sẽ chứa thông tin về một người dùng cụ thể hoặc phổ biến hơn là một trang web, bao gồm cả khóa chung của trang web. Các khóa công khai này sẽ được ký bởi một cơ quan đáng tin cậy. Giả định rằng mọi người đều sở hữu khóa xác minh công khai của cơ quan đáng tin cậy, vì vậy bất kỳ ai cũng có thể xác minh khóa xác minh công khai của cơ quan đáng tin cậy đó với chữ ký trên giấy chứng nhận. Xem Phần 8.6 để biết thêm thông tin về chứng chỉ.

Kỹ thuật này được sử dụng trên internet trong Transport Layer Security (thường được gọi là TLS). Khi người dùng kết nối với một trang web an toàn, chẳng hạn như một trang web thuộc một doanh nghiệp tham gia thương mại điện tử, trang web của công ty sẽ gửi chứng chỉ cho người dùng để người dùng có thể xác minh tính xác thực của khóa công khai của trang web. Những khóa công khai này sau đó sẽ được sử dụng để thiết lập một kênh bảo mật giữa người dùng và trang web, trong đó tất cả thông tin đều được mã hóa. Lưu ý rằng khóa chung của cơ quan đáng tin cậy, được sử dụng để xác minh khóa chung của trang web, thường được mã hóa cứng vào trình duyệt web.

1.2.5Hash Functions
Hàm băm

Lược đồ chữ ký có xu hướng kém hiệu quả hơn nhiều so với MAC. Vì vậy không nên sử dụng sơ đồ chữ ký để ký các tin nhắn "dài". (Trên thực tế, hầu hết các sơ đồ chữ ký được thiết kế để chỉ ký các tin nhắn có độ dài

ngắn, cố định.) Trong thực tế, các tin nhắn được “băm” trước khi chúng được ký. Hàm băm mật mã được sử dụng để nén một thông điệp có độ dài tùy ý thành một bản tóm tắt thông báo ngắn, trông ngẫu nhiên, có độ dài cố định. Lưu ý rằng hàm băm là một hàm công khai được cho là mọi người đều biết. Hơn nữa, hàm băm không có khóa. Hàm băm được thảo luận trong Chương 5.

Sau khi Alice băm tin nhắn, cô ấy ký vào bản tóm tắt tin nhắn bằng thuật toán ký riêng của mình. Tin nhắn ban đầu, cùng với chữ ký trên tin nhắn, sau đó sẽ được truyền tới Bob. Quá trình này được gọi là băm-sau đó-ký. Để xác minh chữ ký, Bob sẽ tính toán thông báo bằng cách băm thông báo. Sau đó, anh ta sẽ sử dụng thuật toán xác minh công khai để kiểm tra tính hợp lệ của chữ ký trên bản tóm tắt thông báo. Khi chữ ký được sử dụng cùng với mã hóa khóa công khai, quy trình thực sự sẽ là băm-rồi-ký-rồi-mã hóa. Nghĩa là, tin nhắn được băm, bản tóm tắt tin nhắn sau đó được ký và cuối cùng, tin nhắn và chữ ký được mã hóa.

Ví dụ, hàm băm mật mã rất khác với hàm băm được sử dụng để xây dựng bảng băm. Trong bối cảnh của bảng băm, hàm băm thường chỉ được yêu cầu để tạo ra các xung đột với xác suất đủ nhỏ. Mặt khác, nếu sử dụng hàm băm mật mã thì việc tìm ra các xung đột sẽ không khả thi về mặt tính toán, mặc dù chúng phải tồn tại. Hàm băm mật mã thường được yêu cầu để đáp ứng các thuộc tính bảo mật bổ sung, như được thảo luận trong Phần 5.2.

Hàm băm mật mã còn có những ứng dụng khác, chẳng hạn như để lấy dẫn xuất khóa. Khi được sử dụng để lấy khóa, hàm băm sẽ được áp dụng cho một chuỗi ngẫu nhiên dài để tạo khóa ngẫu nhiên ngắn

Cuối cùng, cần nhấn mạnh rằng hàm băm không thể được sử dụng để mã hóa vì hai lý do cơ bản. Đầu tiên là thực tế là hàm băm không có khóa. Thứ hai là các hàm băm không thể đảo ngược (chúng không phải là các hàm nội xạ) nên thông báo tóm tắt không thể được “giải mã” để mang lại một giá trị văn bản gốc duy nhất.

1.3 Cryptographic Protocols
Giao thức mật mã

Các công cụ mật mã như hệ thống mật mã, sơ đồ chữ ký, hàm băm, v.v., có thể được sử dụng riêng để đạt được các mục tiêu bảo mật cụ thể. Tuy

nhiên, những công cụ này cũng được sử dụng làm thành phần trong các giao thức phức tạp hơn. (Tất nhiên, các giao thức cũng có thể được thiết kế "từ đầu" mà không cần sử dụng các giao thức gốc trước đó.)

Nói chung, một giao thức (hoặc giao thức tương tác) đề cập đến một chuỗi các thông điệp được chỉ định được trao đổi giữa hai (hoặc có thể nhiều) bên. Ví dụ: một phiên của giao thức giữa Alice và Bob sẽ bao gồm một hoặc nhiều luồng, trong đó mỗi luồng bao gồm một thông báo được gửi từ Alice đến Bob hoặc ngược lại. Vào cuối phiên, các bên liên quan có thể đã thiết lập một số thông tin chung được chia sẻ hoặc xác nhận quyền sở hữu một số thông tin được chia sẻ trước đó.

Một loại giao thức quan trọng là sơ đồ nhận dạng, trong đó một bên "chứng minh" danh tính của mình cho bên khác bằng cách chứng minh quyền sở hữu mật khẩu chẳng hạn. Thay vào đó, các giao thức xác nhân danh tính phức tạp hơn sẽ bao gồm hai (hoặc nhiều) luồng, ví dụ: một thử thách theo sau là một phản hồi, trong đó phản hồi được tính toán từ thử thách sử dụng một bí mật hoặc khóa riêng nhất định. Các sơ đồ xác nhận danh tính là chủ đề của Chương 10

Có nhiều loại giao thức liên quan đến các khía cạnh khác nhau của việc chọn khóa hoặc trao đổi khóa từ bên này sang bên khác. Trong sơ đồ phân phối khóa, khóa có thể được cơ quan đáng tin cậy chọn và truyền đạt tới một hoặc nhiều thành viên của một mạng nhất định. Một cách tiếp cận khác không yêu cầu sự tham gia của cơ quan có thẩm quyền đáng tin cậy đang hoạt động được gọi là thỏa thuận khóa. Trong sơ đồ thỏa thuận khóa, Alice và Bob (giả sử) có thể nhận được một khóa bí mật chung mà đối thủ không được biết. Những chủ đề này và các chủ đề liên quan sẽ được thảo luận trong Chương 11 và 12

Sơ đồ chia sẻ bí mật liên quan đến một cơ quan đáng tin cậy phân phối các "mảnh" thông tin (được gọi là "cổ phần") theo cách mà các tập hợp con chia sẻ nhất định có thể được kết hợp một cách phù hợp để tái tạo lại một bí mật nhất định được xác định trước. Một loại sơ đồ chia sẻ bí mật phổ biến là sơ đồ ngưỡng. Trong sơ đồ ngưỡng (k, n), có n phần chia sẻ và k phần chia sẻ bất kỳ đều cho phép tái tạo lại bí mật. Mặt khác, k - 1 cổ phiếu trở xuống không cung cấp thông tin về giá trị của bí mật. Các sơ đồ chia sẻ bí mật được nghiên cứu ở Chương 11.

1.4 Security
An toàn

Mục tiêu cơ bản của hệ thống mật mã, sơ đồ chữ ký, v.v. là để nó được "an toàn". Nhưng an toàn có nghĩa là gì và làm thế nào chúng ta có thể tin tưởng rằng thứ gì đó thực sự an toàn? Nói một cách đại khái, chẳng hạn, chúng tôi muốn nói rằng kẻ thù không thể thành công trong việc "phá vỡ" một hệ thống mật mã, nhưng chúng tôi phải làm cho khái niệm này trở nên chính xác. Bảo mật trong mật mã liên quan đến việc xem xét ba khía cạnh khác nhau: mô hình tấn công, mục tiêu đối nghịch và mức độ bảo mật. Chúng ta sẽ lần lượt thảo luận về từng điều này.

Mô hình tấn công chỉ định thông tin có sẵn cho kẻ thù. Chúng ta sẽ luôn cho rằng đối thủ biết sơ đồ hoặc giao thức đang được sử dụng (điều này được gọi là Nguyên tắc Kerckhoffs). Đối thủ cũng được cho là biết khóa công khai (nếu hệ thống là hệ thống khóa công khai). Mặt khác, kẻ tấn công được cho là không biết bất kỳ khóa bí mật hoặc khóa riêng nào đang được sử dụng. Thông tin bổ sung có thể được cung cấp cho đối thủ phải được chỉ định trong mô hình tấn công

Mục tiêu đối nghịch xác định chính xác ý nghĩa của việc "phá vỡ" hệ thống mật mã. Đối thủ đang cố gắng làm gì và họ đang cố gắng xác định thông tin gì? Vì vậy, mục tiêu của đối thủ xác định một "cuộc tấn công thành công".

Mức độ bảo mật cố gắng định lượng nỗ lực cần thiết để phá vỡ hệ thống mật mã. Tương tự, đối thủ có quyền truy cập vào những tài nguyên tính toán nào và sẽ mất bao nhiêu thời gian để thực hiện một cuộc tấn công bằng cách sử dụng những tài nguyên đó?

Tuyên bố về tính bảo mật của sơ đồ mật mã sẽ khẳng định rằng không thể đạt được mục tiêu đối nghịch cụ thể trong một mô hình tấn công cụ thể, với các tài nguyên tính toán cụ thể.

Bây giờ chúng ta minh họa một số khái niệm trên liên quan đến hệ thống mật mã. Có bốn mô hình tấn công thường được xét đến. Trong một cuộc tấn công bằng bản mã đã biết, kẻ tấn công có quyền truy cập vào một số lượng văn bản mã hóa được mã hóa bằng cùng một khóa không xác định. Trong một cuộc tấn công bằng văn bản gốc đã biết, kẻ tấn công có được quyền truy cập vào một số văn bản gốc cũng như văn bản mã hóa tương

ứng (tất cả đều được mã hóa bằng cùng một khóa). Trong một cuộc tấn công bằng văn bản gốc đã chọn, kẻ tấn công được phép chọn văn bản gốc và sau đó họ được cung cấp văn bản mã hóa tương ứng. Cuối cùng, trong một cuộc tấn công bằng bản mã đã chọn, kẻ tấn công chọn một số bản mã và sau đó chúng được cung cấp bản rõ tương ứng.

Rõ ràng một cuộc tấn công bằng văn bản gốc hoặc văn bản mã hóa được chọn sẽ cung cấp cho kẻ tấn công nhiều thông tin hơn một cuộc tấn công bằng văn bản mã hóa đã biết. Vì vậy, chúng sẽ được coi là các mô hình tấn công mạnh hơn so với tấn công bằng bản mã đã biết, vì chúng có khả năng khiến công việc của kẻ thù trở nên dễ dàng hơn.

Khía cạnh tiếp theo cần nghiên cứu là mục tiêu đối nghịch. Khi phá vỡ hoàn toàn hệ thống mật mã, kẻ tấn công sẽ xác định khóa riêng (hoặc bí mật). Tuy nhiên, có những mục tiêu khác yếu hơn mà đối thủ có thể đạt được, ngay cả khi không thể phá vỡ hoàn toàn. Ví dụ: kẻ tấn công có thể giải mã một bản mã chưa được nhìn thấy trước đó với một số xác suất khác 0 được chỉ định, mặc dù chúng không thể xác định được khóa. Hoặc, kẻ tấn công có thể xác định được một phần thông tin nào đó về bản rõ, với một bản mã chưa được nhìn thấy trước đó, với một số xác suất khác 0 được chỉ định. “Thông tin một phần” có thể bao gồm các giá trị của các bit văn bản gốc nhất định. Cuối cùng, như một ví dụ về mục tiêu yếu, kẻ tấn công có thể có khả năng phân biệt giữa các mã hóa của hai bản rõ nhất định.2

Các loại mật mã nguyên thủy khác sẽ có các mô hình tấn công và mục tiêu đối nghịch khác nhau. Trong sơ đồ chữ ký, mô hình tấn công sẽ chỉ định loại chữ ký (hợp lệ) mà đối thủ có quyền truy cập. Có lẽ đối phương chỉ nhìn thấy một số thông điệp đã được ký trước đó, hoặc có thể đối phương có thể yêu cầu người ký ký một số thông điệp cụ thể mà đối phương lựa chọn. Mục tiêu của đối thủ thường là ký một số tin nhắn “mới” (tức là một tin nhắn mà đối thủ chưa biết chữ ký hợp lệ). Có lẽ đối phương có thể tìm thấy chữ ký hợp lệ cho một số thông điệp cụ thể mà đối thủ chọn hoặc có thể họ có thể tìm thấy chữ ký hợp lệ cho bất kỳ thông điệp nào. Đây sẽ là những mục tiêu đối nghịch mạnh và yếu tương ứng.

Ba cấp độ bảo mật thường được nghiên cứu, được gọi là bảo mật tính toán, bảo mật có thể chứng minh được và bảo mật vô điều kiện.

Bảo mật tính toán có nghĩa là một thuật toán cụ thể để phá vỡ hệ thống là không khả thi về mặt tính toán, tức là không thể thực hiện được nó trong một khoảng thời gian hợp lý bằng cách sử dụng các tài nguyên tính toán hiện có. Tất nhiên, một hệ thống được bảo mật về mặt tính toán ngày nay có thể không được bảo mật về mặt tính toán một cách vô thời hạn. Ví dụ: các thuật toán mới có thể được phát hiện, máy tính có thể hoạt động nhanh hơn hoặc các mô hình điện toán cơ bản mới như điện toán lượng tử có thể trở thành hiện thực. Điện toán lượng tử, nếu trở thành hiện thực, có thể có tác động to lớn đến tính bảo mật của nhiều loại mật mã khóa công khai; vấn đề này được đề cập chi tiết hơn ở Phần 9.1.

Trên thực tế, rất khó để dự đoán một thứ được coi là an toàn ngày nay sẽ được an toàn trong bao lâu. Có nhiều ví dụ trong đó nhiều sơ đồ mật mã đã không tồn tại được lâu như mong đợi ban đầu vì những lý do nêu trên. Điều này dẫn đến việc thay thế tiêu chuẩn bằng tiêu chuẩn cải tiến khá thường xuyên. Ví dụ: trong trường hợp hàm băm, đã có một loạt các tiêu chuẩn được đề xuất và/hoặc phê duyệt, ký hiệu là SHA-0, SHA-1, SHA-2 và SHA-3, khi các cuộc tấn công mới được phát hiện và các tiêu chuẩn cũ được phát hiện. đã trở nên bất an.

Một ví dụ thú vị liên quan đến dự đoán sai được cung cấp bởi Hệ thống mật mã RSA khóa công khai. Trong số tháng 8 năm 1977 của tạp chí Scientific American, nhà giải thích toán học lỗi lạc Martin Gardner đã viết một chuyên mục về hệ thống mật mã khóa công khai RSA mới được phát triển có tựa đề “Một loại mật mã mới sẽ phải mất hàng triệu năm mới có thể giải mã được”. Trong bài viết có một bản mã thách thức, được mã hóa bằng khóa 512-bit. Tuy nhiên, thách thức đã được giải quyết 17 năm sau, vào ngày 26 tháng 4 năm 1994, bằng cách phân tích khóa công khai đã cho (văn bản gốc là “các từ ma thuật là mảnh vụn”). Tuyên bố rằng mật mã sẽ mất hàng triệu năm để phá vỡ có lẽ đề cập đến việc phải mất bao lâu để chạy thuật toán phân tích nhân tử tốt nhất được biết đến vào năm 1977 trên máy tính nhanh nhất hiện có vào năm 1977. Tuy nhiên, từ năm 1977 đến năm 1994, đã có một số phát triển, bao gồm sau đây:

• máy tính trở nên nhanh hơn nhiều,

• các thuật toán phân tích nhân tố cải tiến đã được tìm thấy, và

• sự phát triển của internet đã tạo điều kiện thuận lợi cho việc tính toán phân tán trên quy mô lớn.

Tất nhiên, về cơ bản là không thể dự đoán được khi nào các thuật toán mới sẽ được phát hiện. Ngoài ra, mục thứ ba được liệt kê ở trên có thể được coi là một "sự thay đổi mô hình" có lẽ không có ai để ý vào năm 1977.

"Cấp độ" bảo mật tiếp theo mà chúng tôi giải quyết là bảo mật có thể chứng minh được (còn được gọi là bảo mật rút gọn), đề cập đến tình huống phá vỡ hệ thống mật mã (tức là đạt được mục tiêu đối nghịch) có thể được giảm bớt theo nghĩa lý thuyết phức tạp để giải quyết một số vấn đề cơ bản. (được cho là khó) vấn đề toán học. Điều này cho thấy rằng việc phá vỡ hệ thống mật mã ít nhất cũng khó như giải một bài toán khó đã cho. Tính bảo mật có thể chứng minh được thường liên quan đến việc rút gọn bài toán phân tích nhân tử hoặc bài toán logarit rời rạc (những bài toán này được nghiên cứu lần lượt trong Phần 6.6 và 7.2)

Cuối cùng, bảo mật vô điều kiện có nghĩa là hệ thống mật mã không thể bị phá vỡ (nghĩa là mục tiêu của đối thủ không thể đạt được), ngay cả với nguồn lực tính toán không giới hạn, vì không có đủ thông tin có sẵn cho đối thủ (như được chỉ định trong mô hình tấn công) để họ có thể thực hiện được. có thể làm điều này Ví dụ nổi tiếng nhất về hệ thống mật mã an toàn vô điều kiện là One-time Pad. Trong hệ thống mật mã này, khóa là một chuỗi bit ngẫu nhiên có cùng độ dài với bản rõ. Bản mã được hình thành dưới dạng độc quyền hoặc của bản rõ và khóa. Đối với One-time Pad, có thể chứng minh bằng toán học rằng kẻ tấn công không thể thu được một phần thông tin nào về bản rõ (ngoài độ dài của nó), với bản mã đã cho, miễn là khóa được sử dụng để mã hóa chỉ một chuỗi bản rõ và khóa có cùng độ dài với bản rõ. Pad một lần được thảo luận trong Chương 3.

Khi chúng tôi phân tích sơ đồ mật mã, mục tiêu của chúng tôi là chỉ ra rằng kẻ địch không thể đạt được mục tiêu yếu ớt trong mô hình tấn công mạnh, với các tài nguyên tính toán lớn.

Cuộc thảo luận trước đây về bảo mật chủ yếu đề cập đến tình huống của mật mã nguyên thủy chẳng hạn như hệ thống mật mã. Tuy nhiên, các nguyên hàm mật mã thường được kết hợp theo những cách phức tạp khi các giao thức được xác định và triển khai cuối cùng. Ngay cả những quyết định triển khai tưởng chừng đơn giản cũng có thể dẫn đến những lỗ hổng

không mong muốn. Ví dụ: khi dữ liệu được mã hóa bằng mật mã khối, trước tiên nó cần được chia thành các đoạn có độ dài cố định, ví dụ: các khối 128 bit. Nếu dữ liệu không lấp đầy chính xác một số khối nguyên thì phải đưa vào một số phần đệm. Hóa ra là một kỹ thuật đệm tiêu chuẩn, khi được sử dụng với chế độ hoạt động chung của CBC, sẽ dễ bị tấn công được gọi là tấn công đệm oracle, được Vaudenay phát hiện vào năm 2002 (xem Phần 4.7.1 để biết mô tả về cuộc tấn công này).

Ngoài ra còn có nhiều loại tấn công khác nhau chống lại việc triển khai mật mã vật lý được gọi là tấn công kênh bên. Ví dụ về những điều này bao gồm các cuộc tấn công thời gian, các cuộc tấn công phân tích lỗi, các cuộc tấn công phân tích sức mạnh và các cuộc tấn công bộ đệm. Ý tưởng là thông tin về khóa bí mật hoặc khóa riêng có thể bị rò rỉ bằng cách quan sát hoặc thao tác vật lý trên một thiết bị (chẳng hạn như thẻ thông minh) có triển khai sơ đồ mật mã cụ thể. Một ví dụ là quan sát thời gian thiết bị thực hiện để thực hiện một số tính toán nhất định (cái gọi là “tấn công thời gian”). Việc rò rỉ thông tin này có thể xảy ra ngay cả khi chương trình này “an toàn”.

1.5 Notes and References
Chú thích và tài liệu tham khảo

Có rất nhiều chuyên khảo và sách giáo khoa về chủ đề mật mã. Chúng tôi sẽ đề cập ở đây một số phương pháp điều trị chung có thể hữu ích cho độc giả.

Để có cách xử lý dễ tiếp cận, không dùng toán học, chúng tôi khuyên bạn nên

• *Everyday Cryptography: Fundamental Principles and Applications, Second Edition* by Keith Martin [127].
For a more mathematical point of view, the following recent texts are helpful:
• *An Introduction to Mathematical Cryptography* by J. Hoffstein, J. Pipher, and J. Silverman [96]
• *Introduction to Modern Cryptography, Second Edition* by J. Katz and Y. Lindell [104]

• *Understanding Cryptography: A Textbook for Students and Practitioners* by C. Paar and J. Pelzl [157]
• *Cryptography Made Simple* by Nigel Smart [185]
• *A Classical Introduction to Cryptography: Applications for Communications Security* by Serge Vaudenay [196].