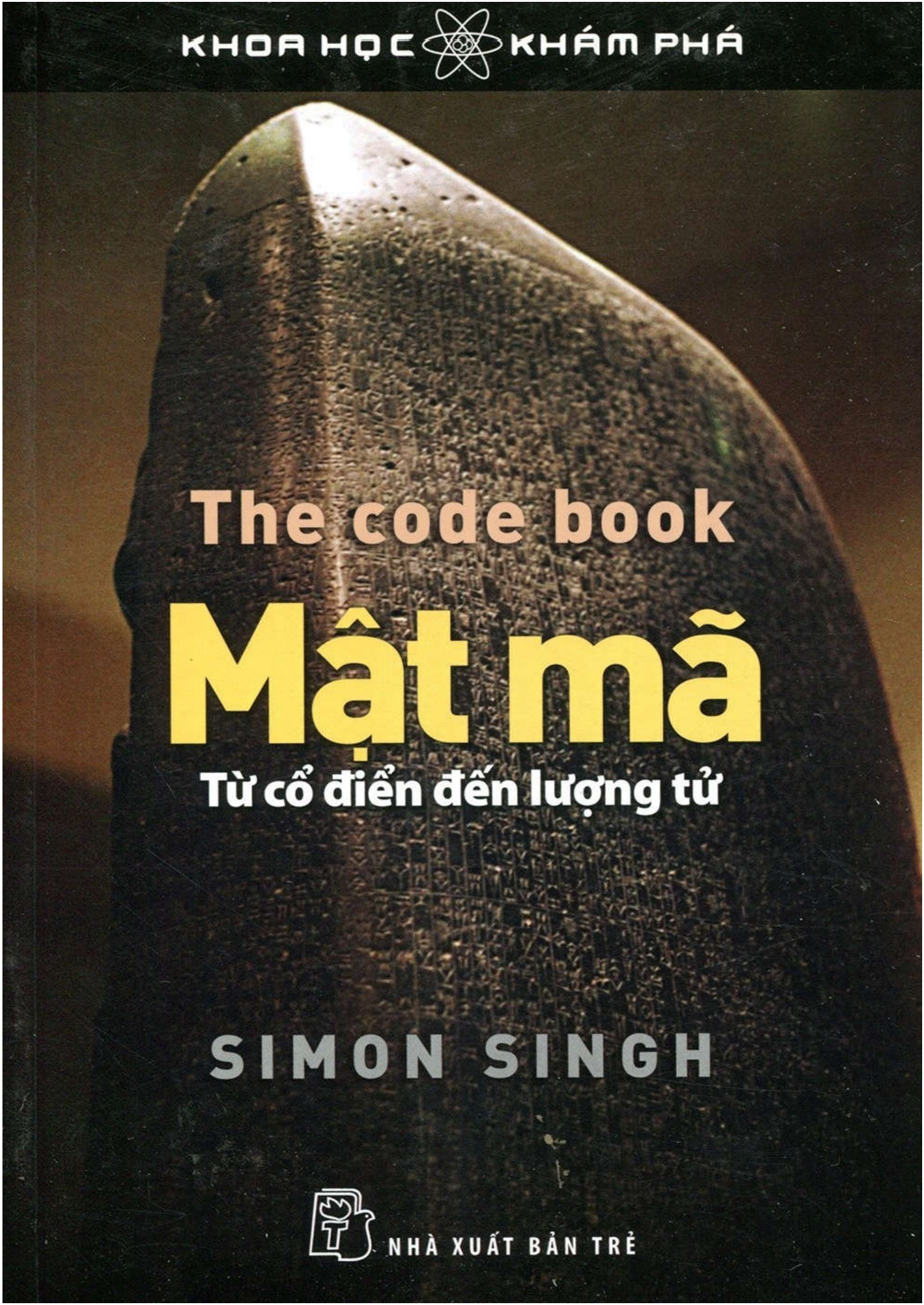
KHOA HỌC KHÁM PHÁ



The code book

Mật mã

Từ cổ điển đến lượng tử

SIMON SINGH

NHÀ XUẤT BẢN TRẺ

Mật Mã

THE CODE BOOK. Tác giả Simon Singh

BIỂU GHI BIÊN MỤC TRƯỚC XUẤT BẢN DO THƯ VIỆN KHTH TP.HCM THỰC HIỆN General Sciences Library Cataloging-in-Publication Data

Singh, Simon

Mật mã - Từ cổ điển đến lượng tử / Simon Singh; ng. d. Phạm Văn Thiều, Phạm Thu Hằng. Tái bản lần thứ 4 - T.P. Hồ Chí Minh : Trẻ, 2014.

552 tr. ; 20 cm.

Nguyên bản: The Code Book

1. Mật mã. I. Phạm Văn Thiều d. II. Phạm Thu Hằng d. III. Ts. IV. Ts: The Code Book.

Table of Contents

Sự thôi thúc khám phá những bí mật đã ăn sâu vào bản chất của con người; ngay cả bộ não ít tò mò nhất cũng bị kích thích trước hứa hẹn sẽ được chia sẻ những thông tin bị che giấu từ người khác. Một số người đủ may mắn tìm được một công việc mà bản thân nó đã là nhằm khám phá những điều bí ẩn, còn hầu hết chúng ta buộc phải làm thăng hoa những thôi thúc đó bằng việc ngồi giải những trò chơi ô chữ do con người nghĩ ra để giải trí mà thôi. Những câu chuyện trinh thám hay trò chơi ô chữ nhằm làm thỏa mãn cho đại đa số, còn việc giải những bản mật mã thì có lẽ chỉ dành cho một số ít người theo đuổi.

John Chadwick

Giải mã Linear B

M Ở Đ Ầ U

Trong hàng ngàn năm, vua chúa cũng như các tướng lĩnh đều dựa vào mạng lưới thông tin liên lạc hiệu quả để cai trị đất nước và chỉ huy quân đội của mình. Đồng thời, tất cả họ đều ý thức được những hậu quả của việc để lọt thông tin của mình vào tay đối phương, để lộ những bí mật quý giá cho các nước thù địch cũng như hậu quả của sự phản bội cung cấp thông tin sống còn cho các lực lượng đối kháng. Chính nỗi lo sợ bị kẻ thù xem trộm đã thúc đẩy sự ra đời và phát triển của mật mã: đó là những kỹ thuật nhằm che giấu, ngụy trang thông tin, khiến cho chỉ những người cần được nhận mới có thể đọc được.

Mong muốn giữ bí mật đã khiến các quốc gia thiết lập những cơ quan mật mã, có nhiệm vụ đảm bảo an toàn cho thông tin liên lạc bằng việc phát minh và sử dụng những mật mã tốt nhất có thể được. Trong khi đó, những người phá mã của đối phương cũng lại cố gắng để giải mã và đánh cắp những bí mật. Người giải mã là những nhà "giả kim thuật" về ngôn ngữ, một nhóm người bí ẩn chuyên tìm cách phỏng đoán những từ ngữ có nghĩa từ những ký hiệu vô nghĩa. Lịch sử của mật mã là câu chuyện về cuộc chiến kéo dài hàng thế kỷ giữa người lập mã và người giải mã, một cuộc chạy đua vũ khí trí tuệ đã có tác động rất to lớn đến tiến trình của lịch sử.

Khi viết cuốn *Mật mã* này, tôi có hai mục đích chính. Một là nhằm phác họa sự tiến hóa của mật mã. Từ tiến hóa dùng ở đây là hoàn toàn thích hợp vì sự phát triển của mật mã cũng có thể coi là một cuộc đấu tranh tiến hóa. Một mật mã luôn bị người phá mã tấn công. Khi người phá mã đã tìm ra một vũ khí mới để phát hiện điểm yếu của một mật mã thì mật mã đó không còn hữu dụng nữa. Khi đó, hoặc nó sẽ bị xóa sổ hoặc nó sẽ được cải tiến thành một loại mật mã mới, mạnh hơn. Đến lượt mình, mật mã mới này chỉ phát triển mạnh mẽ cho tới khi người phá mã lại xác định được điểm yếu của nó, và cứ tiếp tục mãi như vậy. Điều này cũng tương tự như tình huống đối mặt với một giống vi khuẩn gây bệnh chẳng hạn. Vi khuẩn sống, phát triển mạnh và tồn tại cho đến khi bác sĩ tìm ra chất kháng sinh làm lộ ra những điểm yếu của vi khuẩn và tiêu diệt nó. Vi khuẩn buộc phải tiến hóa và lừa lại kháng

sinh, và nếu thành công thì chúng sẽ lại phát triển mạnh mẽ và tái xác lập trở lại. Vi khuẩn liên tục bị buộc phải tiến hóa để sống sót trước sự tấn công dữ dội của các loại kháng sinh mới.

Cuộc chiến liên miên giữa người lập mã và người phá mã đã thúc đẩy hàng loạt những đột phá khoa học đáng kể. Người lập mật mã đã liên tục cố gắng xây dựng những loại mã mạnh hơn bao giờ hết để bảo vệ thông tin, trong khi những người phá mã cũng lại kiên trì tìm ra những phương pháp mạnh hơn nữa để phá vỡ chúng. Trong những cố gắng nhằm phá vỡ và bảo vệ thông tin bí mật, cả hai phía đã phải huy động nhiều lĩnh vực chuyên môn và công nghệ khác nhau, từ toán học cho tới ngôn ngữ học, từ lý thuyết thông tin cho đến lý thuyết lượng tử. Đổi lại, những người lập mã và phá mã cũng đã làm giàu thêm cho những lĩnh vực này và thành quả của họ đã đẩy nhanh tốc độ phát triển công nghệ, mà đáng kể nhất là trong lĩnh vực máy tính hiện đại.

Lịch sử được phân đoạn theo các loại mật mã. Chúng đã quyết định kết cục của các cuộc chiến và dẫn đến cái chết của nhiều vị vua chúa và nữ hoàng. Chính vì vậy mà tôi có thể sử dụng những câu chuyện về các âm mưu chính trị và những truyền thuyết về cuộc sống và cái chết để minh họa cho những bước ngoặt quan trọng trong quá trình tiến hóa của mật mã. Lịch sử mật mã phong phú một cách kỳ lạ khiến tôi buộc phải bỏ bớt đi rất nhiều câu chuyện hấp dẫn. Nếu bạn muốn tìm hiểu thêm những câu chuyện hoặc những người phá mã mà bạn ưa thích, tôi xin giới thiệu với các bạn một danh sách ở phần đọc thêm, nhằm giúp cho những ai muốn tìm hiểu vấn đề này một cách chi tiết hơn.

Sau khi đã bàn luận về sự tiến hóa của mật mã và những tác động của nó đến lịch sử, mục đích thứ hai của cuốn sách là nhằm chứng minh chủ đề này ngày nay còn trở nên hợp thời hơn bao giờ hết. Vì thông tin trở thành một loại hàng hóa có giá trị ngày một gia tăng và vì cuộc cách mạng về truyền thông làm thay đổi cả xã hội nên quá trình mã hóa thông tin sẽ đóng một vị trí ngày càng quan trọng trong đời sống hằng ngày của chúng ta. Ngày nay, các cuộc gọi điện thoại của chúng ta đều qua vệ tinh và các thư điện tử *(e-mail)* đi qua nhiều máy tính khác nhau, đồng thời cả hai loại giao tiếp này đều có thể bị nghe hoặc xem trộm khá dễ dàng, do vậy có nguy cơ làm tổn

hại đến những bí mật riêng tư của chúng ta. Cũng tương tự như vậy, vì ngày càng có nhiều hoạt động kinh doanh được thực hiện qua Internet, nên sự bảo mật phải được thực hiện để bảo vệ cho các công ty và khách hàng của họ. Mã hóa là cách duy nhất để bảo vệ những bí mật riêng tư của chúng ta và bảo đảm cho sự thành công của thị trường kỹ thuật số. Nghệ thuật truyền thông bí mật, hay nói cách khác là khoa học mật mã, sẽ cung cấp cả khóa lẫn chìa khóa của Thời đại Thông tin.

Tuy nhiên, nhu cầu ngày một tăng của xã hội đối với khoa học mật mã lại mâu thuẫn với yêu cầu tuân thủ luật pháp và bí mật quốc gia. Trong nhiều thập kỷ, cảnh sát và các cơ quan tình báo đã sử dụng biện pháp nghe trộm để thu thập chứng cứ chống lại bọn khủng bố và các tập đoàn tội phạm có tổ chức, song sự phát triển của những mã cực mạnh ngày nay đang đe dọa sẽ làm mất đi giá trị của việc nghe trộm đó. Khi chúng ta đang bước vào thế kỷ 21, những người theo chủ nghĩa tự do cá nhân đang gây sức ép cho việc sử dụng rộng rãi mã hóa để bảo vệ bí mật cá nhân. Đấu tranh cùng với họ là các doanh nhân, những người đòi hỏi phải mã hóa mạnh để bảo vệ bí mật giao dịch trong một thế giới phát triển chóng mặt của thương mại điện tử. Trong khi đó, các lực lượng luật pháp và trật tự lại vận động chính phủ hạn chế việc sử dụng mã hóa. Câu hỏi đặt ra là, chúng ta đánh giá cao việc nào hơn - bí mật riêng tư của chúng ta hay một lực lượng cảnh sát có hiệu quả? Hay cần phải có một sự thỏa hiệp?

Mặc dù mã hóa ngày nay có ảnh hưởng rất lớn đến các hoạt động dân sự, thì cũng cần lưu ý rằng mã hóa trong quân sự cũng vẫn là một lĩnh vực quan trọng. Người ta cho rằng Thế chiến thứ I là cuộc chiến tranh của các nhà hóa học, bởi vì khí mù tạt và clo lần đầu tiên được sử dụng, còn Thế chiến thứ II là chiến tranh của các nhà vật lý, vì bom nguyên tử đã được thả xuống. Tương tự, người ta cho rằng Thế chiến thứ III sẽ là cuộc chiến tranh của các nhà toán học bởi vì các nhà toán học sẽ điều khiển loại vũ khí vĩ đại tiếp theo của chiến tranh - đó là thông tin. Các nhà toán học là những người chịu trách nhiệm phát triển các loại mã mà ngày nay đang được sử dụng để bảo vệ thông tin quân sự. Không có gì đáng ngạc nhiên khi chính các nhà toán học cũng lại là những người tiên phong trong cuộc chiến phá các loại mật mã đó.

Trong khi mô tả sự tiến hóa của mật mã và tác động của chúng đến lịch

sử, tôi cũng tự cho phép mình đi lạc đề một chút. Chương 5 mô tả việc giải mã những văn bản cổ khác nhau, trong đó có bản *Linear B* và chữ viết tượng hình cổ Ai Cập. Về mặt kỹ thuật, mã hóa liên quan đến những cách truyền thông tin được thiết kế một cách cẩn trọng nhằm giữ bí mật đối với kẻ thù, trong khi đó thì những văn bản của các nền văn minh cổ đại lại hoàn toàn không có ý định viết ra để cho không ai có thể đọc được: đó chỉ đơn giản là do chúng ta đã mất khả năng diễn giải chúng mà thôi. Tuy nhiên, những kỹ năng cần thiết để khám phá ý nghĩa của những văn bản khảo cổ học cũng có quan hệ rất gần gũi với nghệ thuật giải mã. Ngay từ khi đọc cuốn *Giải mã Linear B* của John Chadwick mô tả quá trình đọc một văn bản cổ được tìm thấy ở Địa Trung hải, tôi đã bị cuốn hút bởi thành quả trí tuệ đáng kinh ngạc của những người đã giải mã được các văn bản của tổ tiên chúng ta, nhờ đó chúng ta mới biết được nền văn minh, tôn giáo và cuộc sống hằng ngày của họ.

Đối với những người ưa chính xác, tôi xin được thứ lỗi vì tựa đề của cuốn sách. Mật mã ở đây không chỉ nói riêng về mã từ *(code)*. Thuật ngữ "mã từ" hàm ý một dạng truyền thông bí mật rất cụ thể, một dạng mã đã lụi tàn qua nhiều thế kỷ sử dụng. Ở mã từ, một từ hay một cụm từ được thay thế bởi một từ, một con số hay một ký hiệu. Chẳng hạn, các điệp viên đều có bí danh, tức là các từ được sử dụng thay cho tên thật nhằm che giấu nhân dạng của mình. Tương tự, cụm từ **Attack at dawn** (*Tấn công vào lúc bình minh*) có thể được thay thế bằng một từ mã là **Jupiter**, và từ này sẽ được gửi cho người chỉ huy trận đánh như một cách gây khó khăn cho đối phương. Nếu sở chỉ huy và viên tướng ngoài mặt trận đã thống nhất về mật mã trước đó, thì nghĩa của **Jupiter** là rất rõ ràng đối với người nhận, nhưng sẽ chẳng có nghĩa gì với đối phương khi chặn bắt được nó. Một cách tạo mã khác là mã thay thế chữ cái *(cipher),* đây là một kỹ thuật thực hiện ở mức độ cơ bản hơn, bằng cách thay thế các chữ cái chứ không phải là cả một từ hoặc cụm từ. Ví dụ, mỗi chữ cái trong một cụm từ có thể được thay thế bằng chữ cái tiếp theo trong bảng chữ cái, chẳng hạn như **A** được thay bằng **B, B** bằng **C**, v.v... Như vậy thì **Attack at dawn** sẽ trở thành **Buubdl bu ebxo**. Mã chữ cái đóng vai trò không thể thiếu trong khoa học mã hóa và vì vậy lẽ ra tên cuốn sách này phải là *Mã từ và mã chữ cái* mới phải. Tuy nhiên, tôi đã bỏ qua sự quá chi li đó cho ngắn