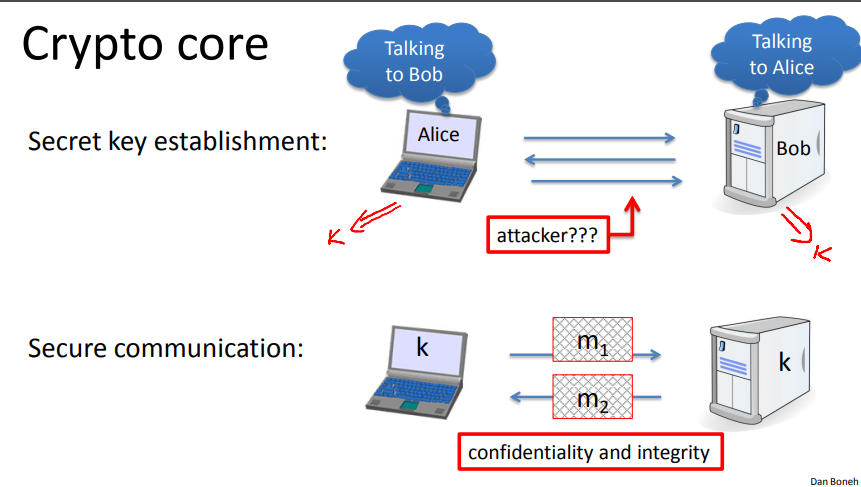
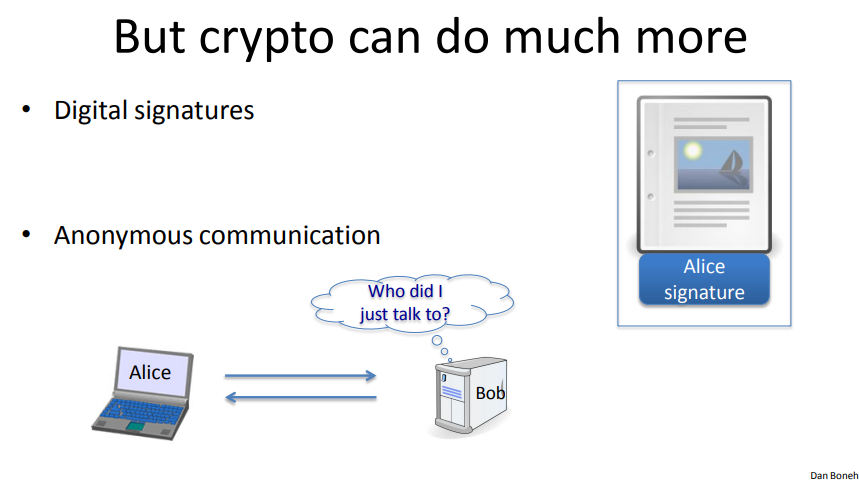
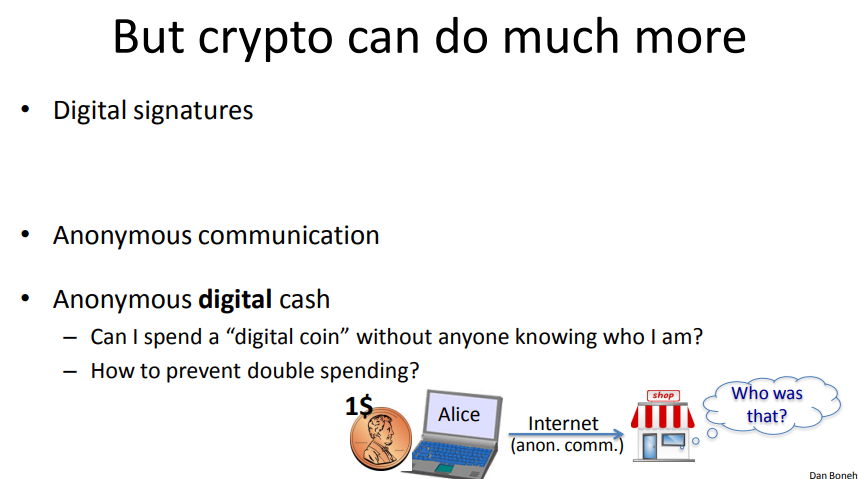
**What is cryptography?**



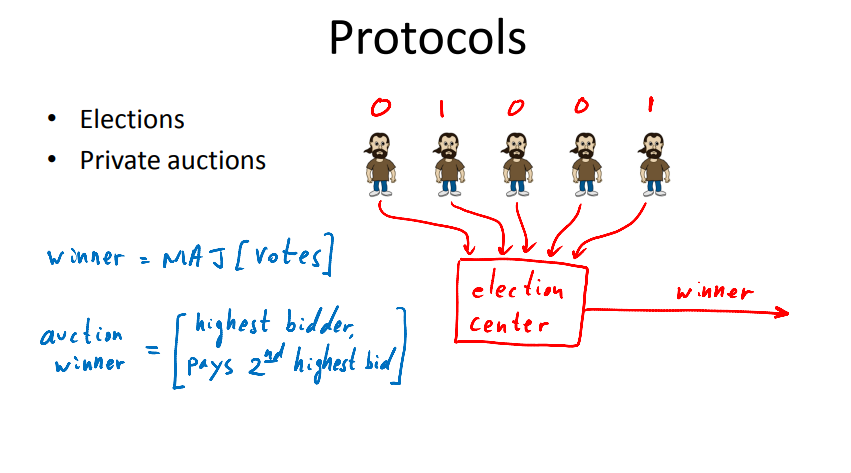
Mật mã học bao gồm hai phần chính: tạo lập khóa an toàn và truyền thông an toàn khi đã có khóa chung. Quá trình tạo khóa chung đảm bảo rằng cả Alice và Bob đều biết họ đang giao tiếp với đúng người, trong khi kẻ nghe lén không thể biết khóa chung. Sau khi có khóa, họ có thể trao đổi thông điệp an toàn bằng cách mã hóa, bảo đảm bí mật và tính toàn vẹn của thông điệp, ngăn cản kẻ tấn công phát hiện hoặc thay đổi thông tin. Mật mã học còn mang lại nhiều lợi ích hơn thế.



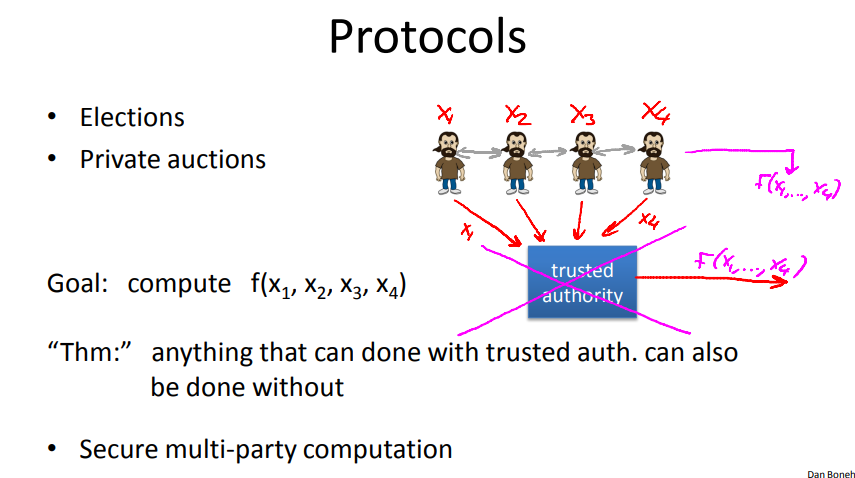
Ứng dụng của mật mã học: chữ ký kỹ thuật số và liên lạc nặc danh. Chữ ký kỹ thuật số đảm bảo rằng mỗi tài liệu có một chữ ký duy nhất dựa trên nội dung của nó, ngăn chặn việc sao chép chữ ký từ tài liệu này sang tài liệu khác. Mặt khác, liên lạc nặc danh cho phép Alice giao tiếp với Bob mà không tiết lộ danh tính, nhờ sử dụng mạng proxy (mixnet), trong đó các tin nhắn được mã hóa và giải mã qua nhiều bước để che giấu nguồn gốc và đích đến. Thú vị là liên lạc này là hai chiều, Bob vẫn có thể phản hồi Alice mà không biết cô là ai.



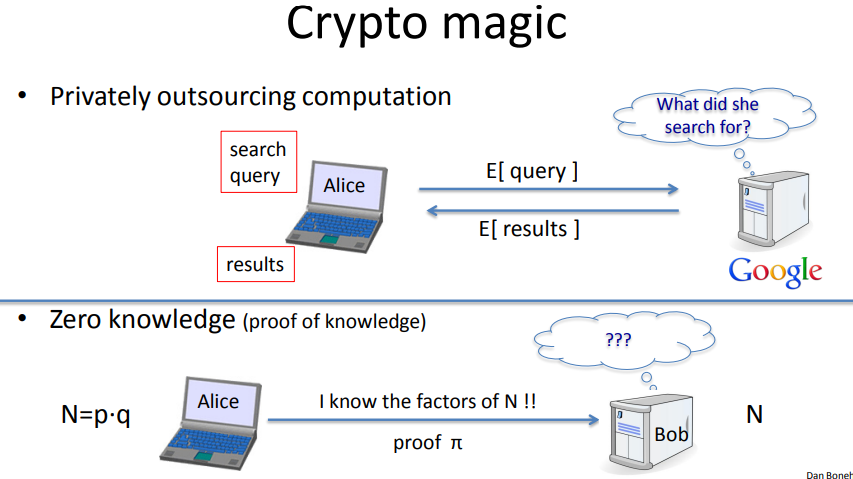
Slide này mô tả về tiền ảo nặc danh, tương tự như tiền mặt trong thế giới thực, nơi người dùng có thể chi tiêu mà không bị nhận diện. Thách thức trong thế giới ảo là Alice có thể sao chép và tiêu cùng một đồng tiền nhiều lần. Để giải quyết điều này, hệ thống tiền ảo nặc danh cần đảm bảo ẩn danh khi Alice chỉ tiêu tiền một lần. Tuy nhiên, nếu cô ấy cố gắng tiêu cùng một đồng tiền nhiều lần, danh tính của cô sẽ bị lộ. Điều này ngăn chặn gian lận và bảo đảm tính bảo mật. Hệ thống này sẽ được giải thích chi tiết hơn trong phần sau của khóa học.



Slide giới thiệu hai ứng dụng của mật mã học: bầu cử an toàn và đấu giá riêng tư. Trong hệ thống bầu cử, cử tri muốn tính toán kết quả đa số mà không tiết lộ lá phiếu cá nhân. Một trung tâm bầu cử sẽ giúp tính toán kết quả, đảm bảo phiếu bầu của mỗi cử tri vẫn bí mật. Tương tự, trong đấu giá Vickrey, người tham gia đấu giá muốn tìm ra người trả giá cao nhất và giá thầu cao thứ hai, nhưng thông tin chi tiết về các giá thầu còn lại phải được giữ kín. Cả hai ví dụ đều minh họa cho vấn đề "An Toàn Tính Toán Đa Thành Viên," nơi các bên có thể tính toán kết quả chung mà không tiết lộ dữ liệu riêng tư.



Slide giải thích khái niệm "An Toàn Tính Toán Đa Thành Viên," trong đó nhiều bên có đầu vào bí mật (như phiếu bầu hoặc giá thầu) và muốn tính toán một hàm mà chỉ kết quả của hàm được công khai, trong khi các đầu vào cá nhân vẫn được giữ bí mật. Thay vì dựa vào một đơn vị tin cậy để thu thập và xử lý dữ liệu, các bên có thể giao tiếp với nhau qua một giao thức bảo mật, cho phép tính toán kết quả mà không tiết lộ đầu vào. Điều này loại bỏ sự cần thiết của đơn vị tin cậy và đảm bảo tính bảo mật của các thông tin cá nhân. Mật mã học đã chứng minh rằng việc này hoàn toàn khả thi, và slide nhấn mạnh sự "kỳ diệu" của các ứng dụng mật mã học.

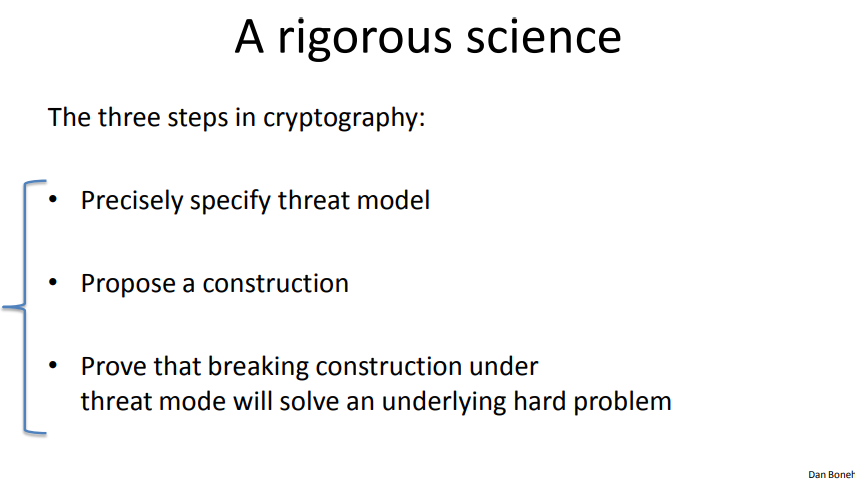


Slide giới thiệu hai ứng dụng kỳ diệu của mật mã học:

1. Tính Toán Gia Công Riêng Tư (Private Outsourced Computation): Alice có thể gửi một truy vấn mã hóa đến Google và Google có thể thực hiện tìm kiếm trên dữ liệu mã hóa mà không biết nội dung truy vấn. Google trả về kết quả được mã hóa và Alice giải mã để nhận kết quả. Điều kỳ diệu là Google không hề biết truy vấn thực sự là gì. Mặc dù lý thuyết này khả thi, việc áp dụng thực tế hiện nay vẫn còn rất chậm và chưa hiệu quả.

2. Chứng Minh Không Tiết Lộ Thông Tin (Zero-Knowledge Proof): Alice có thể chứng minh với Bob rằng cô biết thừa số của một số N (là tích của hai số nguyên tố lớn) mà không tiết lộ thông tin về các thừa số này. Bob có thể xác minh điều đó mà không biết thêm gì về các số nguyên tố. Điều này có thể áp dụng cho nhiều bài toán khác, chẳng hạn như chứng minh rằng Alice đã giải một trò Sudoku mà không tiết lộ lời giải.

Cả hai ứng dụng này đều cho thấy sức mạnh của mật mã học trong việc bảo vệ quyền riêng tư và bảo mật thông tin.



Slide giải thích rằng mật mã học hiện đại là một lĩnh vực khoa học nghiêm ngặt, được xây dựng theo ba bước cơ bản khi giới thiệu một cơ chế mật mã mới:

1. Xác định mô hình mối đe dọa: Đầu tiên, cần xác định chính xác các hành động mà một kẻ tấn công có thể thực hiện để tấn công hệ thống và mục tiêu của họ. Ví dụ, với chữ ký ảo, cần xác định rõ ràng việc làm giả chữ ký là gì.

2. Đề xuất cấu trúc: Tiếp theo, đề xuất một cấu trúc mật mã để giải quyết vấn đề trong mô hình mối đe dọa.

3. Chứng minh an toàn: Cuối cùng, chứng minh rằng bất kỳ kẻ tấn công nào có thể tấn công cấu trúc đó sẽ phải giải quyết một vấn đề toán học khó khăn, từ đó chứng minh tính an toàn của cấu trúc.

Cách tiếp cận ba bước này sẽ được áp dụng cho mọi cơ chế mật mã trong khóa học. Kết thúc đoạn văn, tác giả nhắc đến việc sẽ nói về lịch sử của mật mã học trong phần tiếp theo.