Giao tiếp bảo mật tuyệt đối là bất khả thi trên lí thuyết. Bất kì thông điệp nào cũng luôn có khả năng rơi nhầm vào tay người khác. Thực tiễn, chỉ có thể làm giảm khả năng để điều này xảy ra ở một mức độ nhỏ có thể chấp nhận được. Ngày nay, mã hóa là phương pháp chính nhằm giữ bí mật thông tin liên lạc. Một thông điệp được truyền đi (văn bản thô) chỉ có thể hiểu được nếu đã được giải mã. Rõ ràng, thông điệp chỉ được coi là bí mật khi mức độ để giải mã mật mã là rất phức tạp. Một thông điệp có thể được mã hóa bằng nhiều cách.

Một phương thức mã hóa một thông điệp được gọi là một mật mã. Một ví dụ bình thường (và không an toàn cho lắm) về mật mã là đảo ngược các kí tự trong thông điệp. Nếu biết cách thông điệp đã được mã hóa, người nhận tin có thể giải mã nó bằng cách đảo ngược các kí tự trong bản mã để được bản thô.

Một ví dụ khác là mật mã thay thế, hoạt động theo nguyên lí thay thế từng kí tự của thông điệp dưới dạng bản thô thành một số kí tự khác. Cách này có thể được giải mã thông qua việc thay thế đảo ngược bởi người nhận khi người này biết phương thức thay thế nào đã được tạo ra. Trong ví dụ này, bản mã kết hợp với một khóa bí mật (một lược đồ thay thế). Cùng một mật mã sử dụng trên cùng một bản thô nhưng với các khóa khác nhau sẽ cho ra các bản mã khác nhau.

Mật mã thay thế đơn kí tự có thể dễ dàng bị bẻ khóa bởi các nhà phân tích mật mã (những người chuyên phá mã) thông qua các kĩ thuật như sự xuất hiện lặp đều đặn của các chữ cái “e”, “t” và “a” trong tiếng Anh. Bằng cách đếm tần số xuất hiện của mỗi chữ cái trong bản mã, một nhà phân tích mật mã có thể đoán được những chữ cái nào trong bản mã được ánh xạ đến những chữ cái này. Một khi quy luật này đã được thiết lập, các manh mối khác, chẳng hạn như các chữ cái nào thường đi trước và sau những chữ cái này, có thể được sử dụng để tiếp tục thực hiện quá trình giải mã

Một vài mật mã mạnh hơn, được gọi là mật mã khối, sẽ mã hóa một khối văn bản cùng một lúc chứ không chỉ mã hóa một kí tự đơn lẻ. Theo đó, một khối văn bản (giả sử, 128 bit) được thay thế bằng một khối khác có cùng hoặc khác kích thước. Số lượng chuyển dạng tăng lên nhanh chóng cùng với kích cỡ một khối, dẫn đến việc phân tích mật mã trở nên khó khăn hơn rất nhiều.

Dù con người có thể nghĩ ra rất nhiều phương pháp mã hóa khác nhau, nhưng nhu cầu chuẩn hóa khiến việc mã hóa cần phải tuân theo một hoặc một vài phương pháp phổ biến. Có vẻ phương diện này phá tan mục đích tối cao của việc mã hóa truyền thông. Dù sao đi nữa, Với mật mã “dựa trên khóa”, bản mã không chỉ phụ thuộc vào quy trình mã hóa mà còn phụ thuộc vào khóa bí mật được sử dụng trong quá trình mã hóa.

Một ví dụ về mật mã khối dựa trên khóa là DES (tiêu chuẩn mã hóa dữ liệu) được chính phủ Huê Kềy áp dụng vào năm 1977 và ngành tài chính áp dụng năm 1981. DES sử dụng khóa 56 bit. Ngày này DES không được coi là đủ an toàn chủ yếu vì kích thước khóa nhỏ của nó. Công nghệ máy tính đã trở nên đủ mạnh để các nhà phân tích mật mã có thể thử triệt để tất cả các tổ hợp khóa có thể có trên một bản mã DES trong một khoảng thời gian hợp lí ngay cả khi không có khóa bí mật trong tay

Nổi bật trong số các phương pháo mới xuất hiện là AES (hỗ trợ kích thước khóa 128, 192 và 256 bit), tam bội DES (khắc phục hạn chế về kích thước khóa bằng cách áp dụng DES 3 lần với 2 hoặc 3 khóa khác nhau), mật mã Rivest (RC2, RC4, RC5 và RC6) và các phương pháp khác như IDEA (Thuật toán mã hóa dữ liệu quốc tế) và CAST. Tất cả các mật mã được đề cập ở trên được gọi là “mật mã khóa đối xứng” bởi chúng dung cùng một khóa để mã hóa và giải mã.

Các mật mã khóa đối xứng gần như là không thể phá vỡ được nhưng là một phần của thương mại điện tử??? :D :D :D Các vấn đề khác phải được định danh địa chỉ để liên lạc an toàn trên Thế Giới ngày nay, nơi rất nhiều tổ chức cần liên lạc thông qua phương tiện truyền thông không an toàn như Internet. Bất kì phương án nào được sử dụng đều phải đáp ứng một cách lí tưởng các yêu cầu sau:

Bảo mật: Hầu như không ai có thể giải mã thông điệp ngoại trừ đúng người nhận. Đây là khía cạnh rõ ràng nhất của vấn đề an toàn thông tin liên lạc và đã được giải quyết tốt nhờ các mật mã khóa đối xứng đã được đề cập.

Khả năng mở rộng: Phương pháp thực hiện nên thuận tiện để sử dụng khi số lượng người truyền thông và thông điệp là rất lớn. Giao tiếp bí mật sử dụng khóa đối xứng không thể mở rộng nếu chỉ sử dụng riêng lẻ. Nó sẽ vướng vào rất nhiều vấn đề khi có nhiều bên không quen biết cần được liên lạc với nhau một cách bí mật. Ví dụ như trong giao dịch thương mại điện tử.

Nút thắt lớn nhất của các hệ thống như vậy là việc phân phối và quản lí các khóa bí mật. Giả sử có n bên liên lạc đôi một với nhau và tất cả các kết nối đều cần giữ bảo mật, vậy mỗi bên phải theo dõi một khóa bí mật của n-1 bên còn lại để giữ liên lạc.

Một vấn đề thậm chí còn lớn hơn là việc phân phối các khóa an toàn ngay từ ban đầu sao cho khóa an toàn không rơi vào tay nhầm người. Có thể trao đổi khóa một cách an toàn qua các phương tiện không an toàn; trên hết, thực tế, không thể mong đợi việc tất cả các bên giao tiếp sẽ gặp mặt trực tiếp để trao đổi cho nhau các khóa an toàn. Hơn nữa, để phá vỡ một mật mã , một nhà phân tích mật mã cần rất nhiều các bản mã được tạo bởi một khóa duy nhất. Do đó, để giảm thiểu các rủi ro ảnh hưởng đến bảo mật, cần phải thay đổi định kì các khóa đối xứng được sử dụng. Yêu cầu này càng làm phức tạp hơn việc phân phối các khóa an toàn

Tính toàn vẹn: Người nhận có thể xác nhận được rằng thông điệp không bị can thiệp thay đổi trong quá trình vận chuyển. Điều này là rất quan trọng, bởi lẽ kẻ tấn công có thể chặn ngang thông điệp và chèn một thông điệp khác vào vị trí của thông điệp cũ. Một ví dụ đương thời về kiểu tấn công này là khi tin tặc chặn đường truyền từ một máy chủ thương mại điện tử tới máy khách và chèn trang web của chính kẻ tấn công vào vị trí của trang web của server đã gửi. Một người dung ít nghi ngờ gì sẽ có thể điền những thông tin nhạy cảm vào trang của kẻ tấn công và gửi chúng cho tin tặc.

Tính xác thực: Nên cho phép người nhận thông điệp xác minh danh tính của người tạo ra thông điệp để tránh giao dịch với kẻ mạo danh. Điều này rất cần thiết bởi vì một kẻ mạo danh trên mạng có thể đóng vai trò là một nhà cung cấp thương mại điện tử chính hãng và đánh cắp những thông tin nhạy cảm

Một vấn đề liên quan khác là không được phép bác bỏ. Một người gửi một thông điệp (một tài liệu kinh doanh hợp pháp qian trọng) không thể sau đó tuyên bố rằng mình chưa bao giờ gửi nó. Mục tiêu này đạt được một khi danh tính của người gửi tin nhắn có thể được tạo ra mà không thể xóa bỏ.