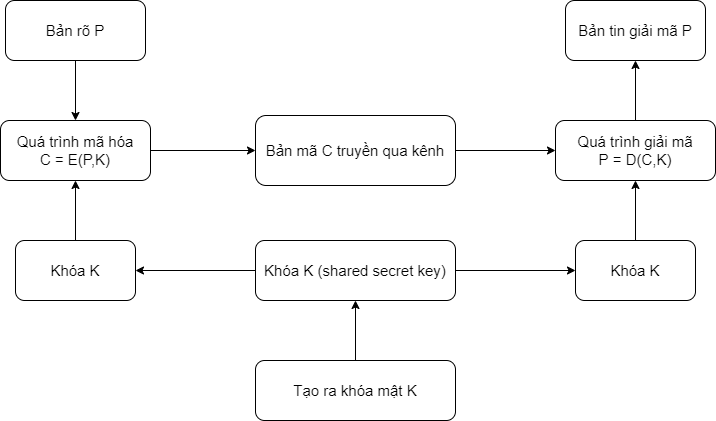
1. **Mật mã đối xứng là gì? Nó có những đặc điểm gì? Vẽ sơ đồ và giải thích hoạt động của mật mã đối xứng tổng quát.**

* **Khái niệm:** thuật toán mã hóa và giải mã sử dụng chung một khóa (shared secret key), thuật toán giải mã là phép toán ngược của thuật toán mã hóa và việc bảo vệ bản tin sinh ra việc phụ thuộc vào bảo vệ khóa.
* **Đặc điểm thứ nhất:** một đặc tính quan trọng của mã hóa đối xứng là khóa phải được giữ bí mật giữa người gởi và người nhận, hay nói cách khác khóa phải được chuyển một cách an toàn từ người gởi đến người nhận. Có thể đặt ra câu hỏi là nếu đã có một kênh an toàn để chuyển khóa như vậy thì tại sao không dùng kênh đó để chuyển bản tin, tại sao cần đến chuyện mã hóa? Câu trả lời là nội dung bản tin thì có thể rất dài, còn khóa thì thường là ngắn. Ngoài ra một khóa còn có thể áp dụng để truyền tin nhiều lần. Do đó nếu chỉ chuyển khóa trên kênh an toàn thì đỡ tốn kém chi phí.
* **Đặc điểm thứ hai:** đặc tính quan trọng thứ hai của một hệ mã hóa đối xứng là tính an toàn của hệ mã. Như đã thấy ở phần mã hóa Ceasar, từ một bản mã có thể dễ dàng suy ra được bản rõ ban đầu mà không cần biết khóa bí mật. Hành động đi tìm bản rõ từ bản mã mà không cần khóa như vậy được gọi là hành động phá mã (cryptanalysis). Do đó một hệ mã hóa đối xứng được gọi là an toàn khi và chỉ khi nó không thể bị phá mã (điều kiện lý tưởng) hoặc thời gian phá mã là bất khả thi.
* **Đặc điểm thứ ba:** mật mã đối xứng thích hợp mã hóa dữ liệu lớn với yêu cầu tính bảo mật không cao vì tính bảo mật được đảm bảo bằng việc bảo vệ khóa bởi mật mã bất đối xứng.
* **Sơ đồ:** về mặt khái niệm, phương pháp mã hóa đối xứng tổng quát được biểu diễn bằng mô hình sau.

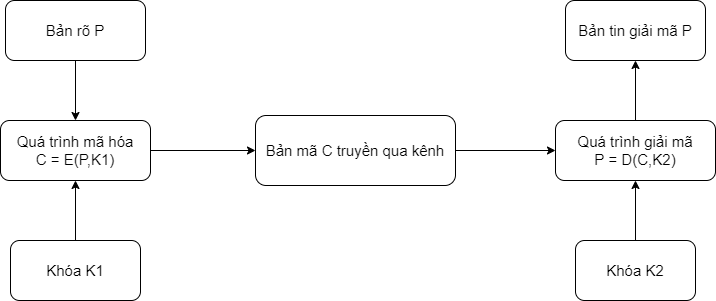


Mô hình trên gồm 5 yếu tố:

* Bản rõ P (plaintext)
* Thuật toán mã hóa E (encrypt algorithm)
* Khóa bí mật K (shared secret key)
* Bản mã C (ciphertext)
* Thuật toán giải mã D (decrypt algorithm)
* Trong đó:
  + C = E (P, K)
  + P = D (C, K)
* **Cách thức hoạt động:** Bản rõ X là thông tin cần mã để bảo mật, trước khi chuyển đến nơi nhận nó phải được mã hóa thông qua thuật toán E với sự tham gia của khóa mật K, sau khi biến đổi kết quả thu được bản mã C. Bản mã C truyền qua kênh thông tin đến nơi người cần nhận sẽ tiến hành giải mã, với việc sử dụng thuật toán giải mã D và khóa mật K sẽ giải mã thành công thành bản rõ P ban đầu. Nếu như khóa không đúng, tức nguyên do bởi dựa trên sự không suy đoán hoặc nghe lén không thành công của kẻ tấn công hoặc bản mã C trong quá trình trung chuyển bị biến đổi thì kết quả sau khi giải mã không thu được bản rõ P ban đầu.

1. **Định nghĩa hàm một chiều ở dạng tổng quát và các đặc điểm liên quan.**
2. **Trình bày cơ chế và mô hình hoạt động của hệ mật mã RSA.**
3. **Mật mã bất đối xứng là gì? Nó có những đặc điểm gì? Vẽ sơ đồ và giải thích hoạt động của mật mã bất đối xứng tổng quát.**

* **Khái niệm:** mã hóa bất đối xứng (Asymmetric cryptography) là mật mã sử dụng hai khóa khác nhau phục vụ cho hai quá trình mã hóa và giải mã. Sự tham gia của hai khóa được đặt tên là khóa công khai (public key) và khóa bí mật (private key).
* **Đặc điểm thứ nhất:** mục đích mã hóa dữ liệu sẽ sử dụng phương án khóa công khai để mã hóa và khóa bí mật để giải mã.
* **Đặc điểm thứ hai:** mục đích chứng thức và tính không thể chối bỏ sẽ sử dụng phương án khóa bí mật để mã hóa và khóa công khai để giải mã.
* **Đặc điểm thứ ba:** mật mã bất đối xứng thích hợp mã hóa dữ liệu nhỏ và yêu cầu độ bảo mật cao, được sử dụng để mã hóa khóa bí mật.
* **Sơ đồ:** về mặt khái niệm, phương pháp mã hóa bất đối xứng tổng quát được biểu diễn bằng mô hình sau.

****

Mô hình trên gồm 5 yếu tố:

* Bản rõ P (plaintext)
* Thuật toán mã hóa E (encrypt algorithm)
* Khóa K1 và K2.
* Bản mã C (ciphertext)
* Thuật toán giải mã D (decrypt algorithm)
* Trong đó:
  + C = E (P, K1)
  + P = D (C, K2)
* **Cách thức hoạt động:** Bản rõ X là thông tin cần mã để bảo mật, trước khi chuyển đến nơi nhận nó phải được mã hóa thông qua thuật toán E với sự tham gia của khóa công khai Ku (public key), sau khi biến đổi kết quả thu được bản mã C. Bản mã C truyền qua kênh thông tin đến nơi người cần nhận sẽ tiến hành giải mã, với việc sử dụng thuật toán giải mã D và khóa bí mật Kr (private key) sẽ giải mã thành công thành bản rõ P ban đầu. Nếu như khóa không đúng, tức nguyên do bởi dựa trên sự không suy đoán hoặc nghe lén không thành công của kẻ tấn công hoặc bản mã C trong quá trình trung chuyển bị biến đổi thì kết quả sau khi giải mã không thu được bản rõ P ban đầu.

1. **Hàm băm là gì? Tính chất của hàm băm.**

* **Khái niệm:** là hàm một chiều, không thể tính ra dữ liệu ban đầu m nếu đang giữ dữ liệu băm. Một hàm băm nhận dữ liệu đầu vào m với độ dài bất kỳ và cho ra kết quả một chuỗi có độ dài cố định ở đầu ra.
* **Tính chất:**

1. **Chữ ký số là gì? Vẽ và giải thích sơ đồ thực hiện kí và kiểm tra chữ kí sử dụng mật mã khóa công khai.**

* **Khái niệm:** là thông tin đi kèm theo dữ liệu nhằm mục đích xác nhận danh tính của người gửi hoặc người ký dữ liệu đó. Chữ ký số được sử dụng để khẳng định dữ liệu có bị thay đổi hay không.