Thông tin là sự thông báo, trao đổi, giải thích, được thể diện thông qua dạng âm thanh, chữ số,chứ viết nhằm mang lại sự hiểu biết cho đối tượng nhận thông tin.

Mã hóa là phương pháp biến thông tin sang định dạng không thể đọc nếu không có phương tiện giải mã

4 loại mã hóa:

+ cổ điển: chủ yếu dự trên hoán vị và mật mã thay thế

+ 1 chiều: mã hóa những tt ko cần dịch lại bản gốc (vd password đc hashfunfion mã hóa -> bảo mật)

+ đối xứng: dùng các khóa để giải mã và mã hóa, 2 khóa này liên hệ rõ ràng với nhau

+ bất đối xứng: 2 khóa khác nhau 1 cái public 1 cái private

Quy trình mã hóa bất đối xứng như sau:

Bên nhận sẽ tạo ra một cặp public + private key. Người này giữ lại private key cho riêng mình và cất cẩn thận, còn public key thì chuyển cho bên gửi (dưới hình thức email, copy qua USB, v.v) hoặc post đâu đó lên mạng.

Bên gửi sử dụng public key để mã hóa dữ liệu, sau đó gửi file đã mã hóa lại cho bên nhận.

Bên nhận lúc này sẽ xài private key đã lưu khi nãy để giải mã dữ liệu và sử dụng.

Giải mã là đưa thông tin về lại dạng ban đầu, ngược với mã hóa