**ÔN TẬP**

1. Theo luật của Kirchoff thì độ an toàn của hệ mã phụ thuộc vào yếu tố : Khóa
2. Ứng dụng của mật mã bao gồm: Bảo mật dữ liệu, xác thực toàn vẹn thông tin, chữ ký số và quản lý khóa
3. Các cách tăng sự an toàn của bản rõ trong hệ mã : Che giấu mối quan hệ giữa bản rõ và bản mã
4. Các yếu tố **không** ảnh hưởng đến sự an toàn của hệ mật mã : Độ dài bản mã
5. Lược đồ của một hệ mật mã có 5 tập khác nhau
6. SKC là hệ mã Phi đối xứng
7. Có 3 phương pháp chính cho mã hóa và giải mã : mã hóa khóa đối xứng, mã hóa khóa công khai , hàm băm
8. Theo Shannon, để che giấu sự dư thừa thông tin bản rõ thì bản mã có sự lộn xộn và rườm rà
9. Theo Shannon, hệ mã an toàn nếu Khóa có độ dài tối thiểu tương đương độ dài thông báo
10. Entropy là đo khối lượng thông tin của thông điệp
11. Nghịch đảo của số nguyên a trong tập Zn tồn tại theo điều kiện