Bài tập

Bài 1: Sơ đồ mã hoá OTP có thể dễ dàng tổng quát trên bộ chữ bất kỳ thay vì chỉ có hai ký tự $0, 1$.

1. Mô tả bộ mã hoá trên bảng chữ `a, b, ..., z` biểu diễn bởi số $0, 1, \ldots, 25$. Hàm mã hoá và giải mã ở đây là gì?

2. Giải mã bản mã

   ```
   bsaspp kkuosp
   ```

   biết rằng nó được mã hoá bằng khoá

   ```
   rsidpy dkawoa
   ```

3. Người đàn ông trẻ đã bị giết như thế nào?

Bài 2: Giả sử một hệ mã OTP dùng khoá ngắn 128 bit. Khoá này thường xuyên được sử dụng để mã hoá lượng lớn dữ liệu. Hãy mô tả một cách tấn công hiệu quả sơ đồ này.