# CSCI971 Advance Computer Security: Homework #3

**Mei Wangzhihui**
**2019124044**

# Problem 1

**Solution**

We know:

$$m[j] \leftarrow D(k, c[j+1]) \oplus c[j]$$

As we miss $c[50]$ so $m[49] \leftarrow D(k, c[50]) \oplus c[49]$ and $m[50] \leftarrow D(k, c[51]) \oplus c[50]$ will be corrupted.

# Problem 2

**Solution**

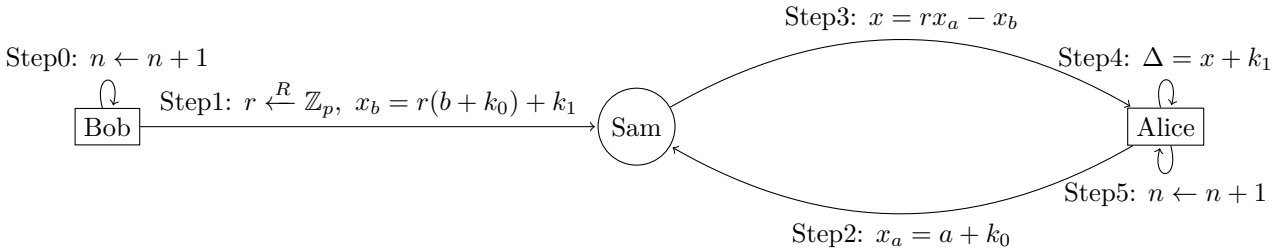


Figure 1: The fixed protocol procedure