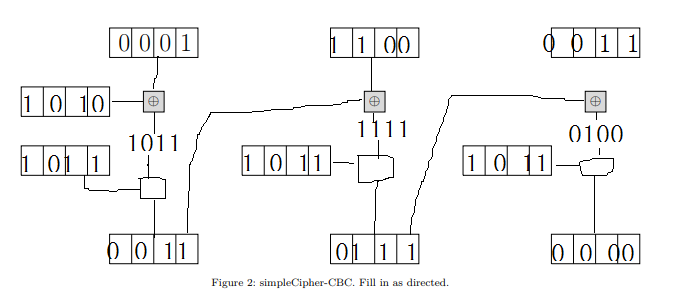
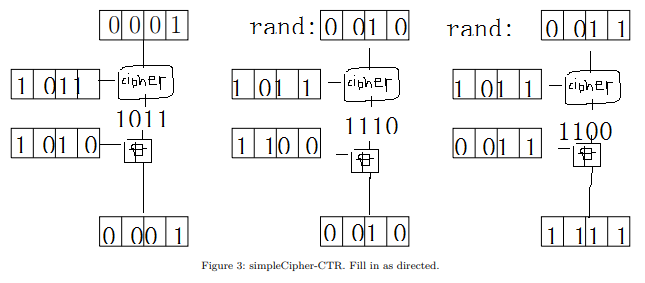
1 Task 1 Cipher Block Chaining Mode



2 Task 2 Counter Mode

1. Encrypting



1. Nonce reuse 1

Since the nonce is same, then the product of [cipher(key, nonce) = F] is same. In this case it would be 1011.

Then, c1 = p1(xor) F, c2 = p2(xor)F.

So c1 (xor)c2 = p1(xor)p2

Thus RHS = LHS.

1. Nonce reuse 2

That means, if the attacker knows key, reused nonce, and cipher algorithm/knows the product of cipher algorithm, he will be able to obtain plain text.

1. Nonce reuse 3

No. because there’s a possibility that there will be repeating value between different steps and blocks, that will lead to the cipher being breached.