1. CBC's encryption is performed serially, and the next plaintext group cannot be encrypted until the ciphertext group corresponding to the previous plaintext group is obtained.

Therefore, there are 2 plaintext blocks will be corrupted, namely number t/2 and number t/2+1.

1. Define A’s advantages: .

We know that the nonce will return to 0 when it reaches 100, and the procedure repeats.

So, A will find the similarities every hundred.

And the:.

Therefore, the encryption is not semantic secure under a CPA attack.

1. Game as:





Therefore, the MAC is not a secure MAC.