1. To formally prove that the adversary A wins the experiment with probability non-negli\gibly greater than ½, we need to show that the advantage of A in distinguishing between the encryption of m0 and m1 is non-negligible.

So, | Pr[A outputs 1 when c is an encryption of m0] - Pr[A outputs 1 c is an encryption of m1] |

Case 1: A outputs 1 when c is an encryption of m0

In this case, since m0[L] == m0[R], the ECB mode encryption will result in two identical ciphertext blocks. Therefore, the output of A will be 0 with probability 1, i.e., Pr[A wins with m0] = 1.

Case 2: A outputs 1 when c is an encryption of m1

In this case, since m1[L] != m1[R], the ECB mode encryption will result in two different ciphertext blocks. Therefore, the output of A will be 1 with probability 1, i.e., Pr[A wins with m1] = 2-n.

| Pr[A outputs 1 when c is an encryption of m0] - Pr[A outputs 1 when c is an encryption of m1] | = 1 – 2-n

i.e., non-negligible greater than ½.

We can conclude that A wins the experiment with probability non-negligibly greater than ½.

1. To prove that the given fixed length encryption scheme does not satisfy EAV-security, we have to create an adversary A that that wins with high (i.e., non-negligibly greater than 1/2) probability.

Adversary A:

* A creates two strings m0 and m1 each of length 3n. Each message block of length n in m0 such that m0[0] = m0[1] = m0[2] and in m1 such that m1[0] != m1[1] != m1[2].
* A receives a ciphertext c from a challenger where c is either an encryption of m0 with probability ½ or an encryption of m1 with probability ½.
* A parses c as c = IV ||c[1] || c[2] || c[3], where |IV| = |c[1]| = |c[2]| = |c[3]| = n.
* A determines if IV is even or odd.
* If IV is even, A checks to see if c[1] == c[2] and outputs 0 if true; else outputs 1.
* If IV is odd, A checks to see if c[2] == c[3] and outputs 0 if true; else outputs 1.