1. To prove that {F’k} is not a PRF, we show that it does not satisfy requirements in order to be a PRF family.

For a PPT adversary A, the probability that A outputs 1 with or acle access to Fk must be negligibly close to that when A outputs 1 with oracle access to random function f.

i.e., Pr [A outputs 1 with oracle access to Fk] – Pr [A outputs 1 with oracle access to f] <= negl(n)

F ′k(x) = Fk(x) if x is even

Fk(x + 1) if x is odd

For a pair of {x0, x1} where x0 is even and x1 = x0 – 1. Here outputs of F’k(x0) and F’k(x1) are the same. So, we choose a distinguisher D such that it distinguishes between outputs of F’k(x0) and F’k(x1) to an output generated by random function f.

Distinguisher D:

D is given an input 1n and given oracle access O(.). Here O(.) evaluates either F’k(.) where k 🡨 {0,1} n or f(.) 🡨 Funcn where (f: {0,1} n 🡪{0,1} n is a random function).

* D generates two inputs x0 and x1. (x0 is even and x1 = x0 - 1)
* D queries y0 = O(x0) and y1 = O(x1) and checks if y0 = y1
* D outputs 1 if equal, else it outputs 0

Hence, D outputs 1 if and only if O(x0) = O(x1) \*.

* If O(.) evaluates F’k(.), then \* holds true. So, D outputs 1 with Pr = 1.
* If O(.) evaluates random function f(.), then O(x0) and O(x1) are independent of each other. The probability that it is equal is 2-n. So, D outputs 1 with Pr = 2-n.

Hence, Pr [A outputs 1 with oracle access to F’k] – Pr [A outputs 1 with oracle access to f]

= 1 - 2-n. i.e., non-negligible.

Hence, {F’k} is not a PRF family.

1. To prove that the given fixed length encryption scheme does not satisfy EAV-security, we have to create an adversary A that can distinguish between outputs of Enck(mb), where b equal to 0 and 1 for m0 and m1 respectively.

For ECB mode, we know that repeated plaintext blocks will result in repeated ciphertext blocks.

Adversary A:

* A generates two 2n bit long plaintext messages m0 and m1 such that they are n bit long each and m0[L] = m0[R] and m1[L] != m1[R]. (like m0 = [0n][0n] and m1 = [0n][1n])
* A receives ciphertext c such that c: = Enck(mb), where b 🡨 {0,1}. Ciphertext c is an encryption of m0 with probability ½ and m1 with probability ½ .
* A parses c as c[1] || c[2].
* A outputs b\* 🡨 {0,1} where,
  + b\* = 0 if and only if c[1] == c[2], else
  + b\* = 1 if and only if c[1] != c[2]
* If b\* = b, where b was used in Enck(mb), then adversary A wins the game.

Adversary A wins the game since ECB mode used for this encryption scheme is insecure with a high probability (non-negligibly greater than ½).