محمد عبدالهی 9530153

اگر به جای مد cbc از مد ebc در صورتی که تکه هایی از متن تکراری باشند کاربر مخرب توانایی تشخیص آنها را دارد و همچنین به ازای یک کلید ثابت همیشه به یک متن رمز شده نگاشته می شود و امکان پیدا شدن کلید وجود دارد.

در این حالت 2^{256} کلید داریم. پس برای ایجاد کلید ها $(2^{256} * 20ms) / 32$ و برای رمزگشایی:

$$(2^{256} * 20ms) / 32 + (2^{256} * 96ms) / 32 * 7$$