3 Cryptography (mgk25)

LegacyGates Ltd has for decades sold garage-door openers that implement a simple challenge–response authentication protocol using their time-honoured 42-bit blockcipher E:

Door D:		Key fob F:
pick $C \in_R \{0,1\}^{42}$	$\xrightarrow{\quad C \quad}$	
		$R := E_K(C) \in \{0,1\}^{42}$
open if $R = E_K(C)$	$\xleftarrow{\quad R \quad}$	

$K \in \{0,1\}^{42}$ is a private key shared between door D and radio key fob F.

E and E^{-1} have become publicly known and burglars have started to eavesdrop some challenge–response pairs (C_1, R_1), (C_2, R_2), (C_3, R_3) and brute-force search for a K that satisfies $R_i = E_K(C_i)$. Renting servers that can try 2^{42} encryptions per day, or even store 2^{42} pairs of blocks in a lookup table, is now quite affordable.

Product teams have been asked to upgrade the protocol to 84-bit security. For "commercial reasons" the company wants to continue to use E, but with a pair of 42-bit keys (K_1, K_2). Five teams each came up with a different proposal. Your task is to evaluate if they succeeded.

For each of the following modifications of the protocol, estimate the number of test encryptions needed, and the amount of storage required, to find a pair (K_1, K_2) that will open the door, and give the corresponding search algorithm.

(*a*) $R := E_{E_{K_2}(K_1)}(C)$ [3 marks]

(*b*) $R := E_{K_1}(C) \oplus K_2$ [4 marks]

(*c*) $R := E_{K_2}(E_{K_1}(C))$ [4 marks]

(*d*) $R := E_{K_2}(E_{K_2}(E_{K_1}(C)))$ [4 marks]

(*e*) $R := E_{K_1}(E_{K_2}(E_{K_1}(C)))$ [4 marks]

Regarding proposal (*e*):

(*f*) What practical advantage would using $R := E_{K_1}(E_{K_2}^{-1}(E_{K_1}(C)))$ instead have? [1 mark]