2004 Paper 8 Question 6

Security

A car locking system consists of an engine management system E which shares a key K with a microcontroller M embedded in the key fob. When an attempt is made to open the door, a challenge N_C is sent by E to M; M computes a response N_R by encrypting N_C with K using a block cipher.

$$\begin{aligned} E \rightarrow M &: N_C \\ M \rightarrow E &: N_R = \{N_C\}_K \end{aligned}$$

M must respond to a challenge in 100 ms, which means that the total length of N_C and N_R can be no more than 64 bits. In addition, if a wrong response is received, E will wait 900 ms before sending another challenge, so that only one trial response can be attempted per second.

A hotel parking valet has access to guests' keys for a few hours or days at a time. He builds test equipment to try out many random challenges and thus constructs a table of (N_C, N_R) pairs. His goal is to follow a guest home, try to unlock the door until E sends a challenge N_C already in the table, whereupon he will return the corresponding N_R and steal the car.

(*a*) Which is the most secure design against this type of attack – $N_C = 24$ bits and $N_R = 40$ bits, $N_C = N_R = 32$ bits, or $N_C = 40$ bits and $N_R = 24$ bits? Justify your answer. [5 marks]

(*b*) Is it important whether the underlying block cipher is AES or DES? Justify your answer. [5 marks]

(*c*) Such a design has been fielded and a long-term contract awarded for the manufacture of key fobs. As a consequence, only the engine controller software can be modified. Is there a modification that makes the valet attack significantly harder? [5 marks]

(*d*) The company that owns the patent on this protocol now wishes to sell handheld password generators, containing the key-fob chips, to banks, with a view to authenticating their customers and thus stopping "phishing" attacks. If you were a bank security manager, would you be enthusiastic about such a proposed solution? [5 marks]