8 Cybersecurity (fms27)

(*a*) Compare and contrast, under at least four relevant aspects, the mechanical implementation of a master-keyed lock system against one using electronic key fobs. Then give one scenario where you would recommend the mechanical implementation and one where you would recommend the electronic one, justifying why. [6 marks]

(*b*) A building with 24 door locks, D0–D23, uses a mechanical (pin-tumbler) master key system. Locks have 5 pin stacks, there are 8 possible cut depths per stack from 0 (shallowest) to 7 (deepest) and each stack contains at most one master pin. Pretend, unrealistically, that all cut depths are usable. Each door has its own differ key that opens just that door. Doors D10–D19 may also be opened by master key 36735. All doors, D0–D23, may also be opened by grand master key 12735.

(*i*) In the lock for door D12, what is the minimum and maximum possible number of pin stacks containing a master pin? Explain your reasoning. [2 marks]

(*ii*) Door D13 is opened by differ key 32737. List *all* the other keys that also open that door. Mention and explain your assumptions. [4 marks]

(*iii*) The occupant of the D16 office, who legitimately owns the D16 differ key 32535 but not the master nor the grand master key, wants to open door D07 using the Matt Blaze privilege escalation attack, visiting door D07 only once in order not to arouse suspicion. She processes the pins left to right, processes the pin depths from shallowest to deepest and uses an optimal strategy. Assume there are no master pins in the D16 lock other than those necessary for it to be opened by the indicated differ key, master key and grand master key. List, in order, every key that the attacker must create and try, mentioning which lock she tries it on and whether it opens, and giving a clear running explanation of what she does. How many keys exactly (not an upper bound) does she need to test on D16, and how many on D07, before successfully opening D07? [8 marks]