6 Cryptography (mgk25)

(*a*) Consider a message-authentication code Mac expected to provide *existential unforgeability under adaptive chosen-message attack*.

(*i*) What requirement does existential unforgeability impose on any padding function applied to the message by Mac and why? [4 marks]

(*ii*) What is an example of a padding function that satisfies that requirement? [2 marks]

(*b*) While reviewing the *MacGyver* burglar alarm system, you notice that a sensor S uses the following stream authentication protocol to report its status to the controller C once every second over a data wire:

$$
\begin{array}{lcll}
C & \rightarrow & S: & R \qquad\qquad \text{with } R \in_{\mathsf{R}} \{0,1\}^{128} \\
S & \rightarrow & C: & (M_1, T_1) \qquad \text{with } T_1 = \mathsf{trunc}_{32}(\mathsf{Mac}_K(M_1, R)) \\
S & \rightarrow & C: & (M_2, T_2) \qquad \text{with } T_2 = \mathsf{trunc}_{32}(\mathsf{Mac}_K(M_2, T_1)) \\
 & \vdots & & \\
S & \rightarrow & C: & (M_i, T_i) \qquad \text{with } T_i = \mathsf{trunc}_{32}(\mathsf{Mac}_K(M_i, T_{i-1})) \\
 & \vdots & &
\end{array}
$$

The controller C picks a new 128-bit random value R when the system is powered up. Each message (M_i, T_i) is sent i seconds after that. The messages M_i are normally all identical, of the form $M = 0$ meaning "no burglary has happened in the last second". Mac is a 128-bit message-authentication code function, using a private key K shared between S and C. Because of the very limited data rate available on the alarm-wire interface, the output of Mac is truncated to the first 32 bits.

(*i*) How can an attacker, who has been observing this communication since power up, eventually predict future tags T_i for the constant message $M_i = M$? [4 marks]

(*ii*) How long will it take, on average, after powerup until the attacker can start sending simulated sensor messages? [4 marks]

(*iii*) What security implication does the predictability of message-authentication codes from a sensor have for a burglar alarm system? [2 marks]

(*iv*) How can you improve the protocol to practically eliminate the risk of that attack, without increasing the number of bits transmitted over the wire? [4 marks]