The following protocol is meant to establish a strong shared secret between two wireless devices $A$ and $B$ through a Diffie–Hellman exchange over radio. To guard against man-in-the-middle attacks, in message 3 device $A$ sends device $B$ a 16-bit secret random value $R$ over a different channel, for example by showing the value on $A$’s screen and having the human user retype it into $B$’s keypad.

Notation: $x|y$ indicates the concatenation of bit strings $x$ and $y$, while $m_K(x)$ indicates the MAC (message authentication code) of message $x$ using key $K$.

\[
\begin{array}{lll}
(1) & A \rightarrow B & : \ g^a \\
(2) & A \leftarrow B & : \ g^b \\
(3) & A \rightarrow B & : \ R \\
(4) & A \rightarrow B & : \ m_{K_A}(A|g^a|g^b|R) \\
(5) & A \leftarrow B & : \ m_{K_B}(B|g^a|g^b|R) \\
(6) & A \rightarrow B & : \ K_A \\
(7) & A \leftarrow B & : \ K_B \\
(8) & \text{(on their own)} & : \text{(verification)} \\
(9) & A \leftrightarrow B & : \text{(confirmation)}
\end{array}
\]

(a) Explain what the resulting shared secret will be and what additional verification and confirmation steps each side must take after exchanging the first 7 messages shown above. [3 marks]

In the following questions, “explain in detail” means with reference to the exact messages exchanged and expected by $A$, $B$ and a man-in-the-middle $M$; and, where appropriate, with suitable protocol diagrams involving all three.

(b) Explain in detail how a man-in-the-middle $M$ could successfully attack this protocol if $R$ were not used or if $M$ could eavesdrop on message 3. [4 marks]

(c) Explain in detail how the introduction of $R$ stops the man-in-the-middle. [5 marks]

(d) Explain in detail how the man-in-the-middle could still successfully attack this protocol if the confirmation of step 9 were omitted. [8 marks]