Universität des Saarlandes
Lehrstuhl für Softwaretechnik
Prof. Andreas Zeller, Stephan Neuhaus
Design of Secure Software Systems
Exercise 4 – Solution

Total number of points obtainable: 10, plus 0 bonus points.

1 Random Number Quality (2+3+3 points)

- The sequence $0, 1, 2, 3, ..., 2^{64} - 1, 0, 1, ...$ is ever-changing, but clearly not unpredictable (1 point). Whereas the sequence given by $Y_n = \text{MD5}(X_n) \bmod 2$, where $X_n = X_{n-1} + 1$, is unpredictable (if we don't know X_0), but not ever-changing because there are only two possible values (1 point).
- A sequence used to generate symmetric cryptographic keys needs to be both unpredictable *and* ever-changing (1 point). If it is not unpredictable, the attacker can determine the next key to be used by analysing the previous keys (1 point). If it is not ever-changing, the probability for an attacker to succeed by simply re-using an old key becomes non-negligible (1 point).
- Initialization vectors need to be ever-changing but not unpredictable (1 point). The purpose of IVs is to ensure that two identical plaintext messages do not encrypt to the same encrypted text (Recall: the *salt* had a similar purpose). IVs are also sent to the recipient in plain-text, so it would be a waste of effort to make them unpredictable (2 points).

2 Message Digest Ciphers (2 points)

It will be sufficient to show that P_1 and P_j evaluate to M_1 and M_j respectively. Note that this is *not* a proof by induction! (1 point)

$$\begin{aligned}
P_1 &= C_1 \oplus h(IV, K) \\
&= \big(M_1 \oplus h(IV, K)\big) \oplus h(IV, K) \qquad \text{expanding } C_1 \\
&= M_1 \oplus \big(h(IV, K) \oplus h(IV, K)\big) \qquad \text{using the associative property of } \oplus \\
&= M_1 \oplus 0_k \qquad \text{using the identity } A \oplus A = 0 \\
&= M_1 \qquad \text{using the identity } A \oplus 0 = A
\end{aligned}$$

Similarly for P_j (1 point):

$$\begin{aligned}
P_j &= C_j \oplus h(C_{j-1}, K) \\
&= \big(M_j \oplus h(C_{j-1}, K)\big) \oplus h(C_{j-1}, K) \\
&= M_j \oplus \big(h(C_{j-1}, K) \oplus h(C_{j-1}, K)\big) \\
&= M_j \oplus 0_k \\
&= M_j
\end{aligned}$$