9 Security II (MGK)

You are working on an encryption device with your new colleague, Mallory Baish, who proposes that you use a pseudo-random generator

\[ r_i = h_1(s_i), \quad s_{i+1} = h_2(s_i) \]

where \( s_0 \in G \) is the random initial state and the other \( s_i \in G \) are subsequent internal states, all invisible to adversaries. The \( h_1, h_2 : G \to G \) are two secure one-way functions.

Adversaries may see any of the past outputs \( r_0, \ldots, r_{n-1} \). If they can predict from those, with non-negligible probability, the next value \( r_n \), then the security of your device will be compromised.

(a) Give a rough estimate for the probability that an adversary can predict \( r_n \), as a function of \( n \) and \(|G|\). Explain your answer. \([6\text{ marks}]\)

(b) Mallory also suggests a specific implementation:

\[ h_1(x) = f(u^x \mod p) \quad p = \text{a 2056-bit prime number} \]
\[ h_2(x) = f(v^x \mod p) \quad u, v = \text{two numbers from } Z_p^* \]
\[ f(x) = x \mod 2^{2048} \quad G = Z_{2^{2048}} \]

(i) The constants \( p, u \) and \( v \) will be known to the adversary. What conditions should they fulfill so that \( h_1 \) and \( h_2 \) can reasonably be described as one-way functions, and how would you normally generate suitable numbers \( u \) and \( v \)? [Hint: quadratic residues] \([4\text{ marks}]\)

(ii) If \( f \) were replaced with the identity function, how could an adversary distinguish the \( r_i \) emerging from this pseudo-random generator from a sequence of elements of \( Z_p^* \) picked uniformly at random? \([4\text{ marks}]\)

(iii) After you choose a value for \( p \), Mallory urges you to use two particular values for \( u \) and \( v \) generated in your absence. You briefly see “\( v = u^e \mod p \)” scribbled on a whiteboard. You become suspicious that Mallory is trying to plant a secret backdoor into your pseudo-random generator.

Explain how Mallory could exploit such a backdoor. \([6\text{ marks}]\)