2005 Paper 3 Question 9 / Paper 10 Question 11

(Computer Science Tripos Part Ib, Part II (General), Diploma)

MGK may have available a more up to date version of this answer.

Introduction to Security (MGK) – Solution Notes

(*a*) (*i*) The email transmission introduces a variable delay. Players cannot be sure whether the opponent really submitted a value *before* receiving the other one. A could wait until R_B arrived and then win by sending back $R_A = (R_B + 1) \bmod 3$, or vice versa.

(*ii*) To make the game work at a distance over a store-and-forward computer network, players first have to commit to their respective choice, without leaking any information about what it is. Only then can the chosen numbers be revealed and exchanged. In one simple solution, A and B each choose randomly a 128-bit word, N_A and N_B respectively. Then, they first send to each other the values

$$A \rightarrow B: \quad V_A = h(N_A||R_A) \qquad \text{and} \qquad B \rightarrow A: \quad V_B = h(N_B||R_B),$$

where h is a secure hash function. Only after the players have received V_B and V_A, respectively, they exchange and then verify the preimages:

$$A \rightarrow B: \quad N_A||R_A \qquad \text{and} \qquad B \rightarrow A: \quad N_B||R_B$$

(*iii*) The secure hash function h must be preimage resistant, otherwise A could determine R_B from V_B. It must also be collision resistant, otherwise A could be able to generate values N_A, R_A, N'_A, R'_A with $R_A \neq R'_A$ but $V_A = h(N_A||R_A) = h(N'_A||R'_A)$. This might allow A to choose between releasing either (R_A, N_A) or (R'_A, N'_A), whichever avoids loosing the game, after having already seen R_B. SHA-256 is an example of a function h that is today believed to fulfill these requirements.

(*iv*) The opponent is not assumed to be able to compute or store the result of $h(N||R)$ for all 2^{128} possible values of $N \in \{0,1\}^{128}$ and all three values of $R \in \mathbb{Z}_3$. Otherwise, there would be a risk that h could be inverted here, either by brute-force search or by lookup in a pre-computed table.

(*b*) A security policy is meant to be the outcome of a systematic planning approach for analysing the security requirements of an organisation. This typically involves a security requirements analysis, in which available assets along with their value and vulnerabilities are identified, as well as threats to them and security-related legal requirements to the organisation. The resulting written high-level security policy should then give its readers a clear understanding of authorised, required and prohibited activities, states and information flows. It should help in working out a low-level security policy that defines the detailed controls and responsibilities to be implemented.

[The questions relate to (a) applications of secure hash functions (lecture on symmetric cryptography) and (b) security management (introductory lecture).]