11 Security II (MGK)

(*a*) Why does the formal security definition for collision-resistant hash functions require a key s and a security parameter n, even though most commonly used standard secure hash functions lack such input parameters? [4 marks]

(*b*) If $h_s : \{0,1\}^* \rightarrow \{0,1\}^{\ell(n)}$ is a collision-resistant hash function, do the following constructions H_s also provide collision-resistant hash functions? Explain your answers. [2 marks each]

(*i*) $H_s(x) = h_s(x) \parallel x$ (i.e. append x)

(*ii*) $H_s(x) = h_s(x) \parallel \mathrm{LSB}(x)$ (i.e. append least significant bit of x)

(*iii*) $H_s(x) = h_s(x \mid 1)$ (bitwise-or, i.e. set least significant bit of x to 1)

(*c*) Use Euler's theorem to calculate $5^{-1} \bmod 8$. [4 marks]

(*d*) The standard Digital Signature Algorithm (DSA) uses a cyclic subgroup $\mathbb{G} \subset \mathbb{Z}_p^*$ of the integers modulo a prime p, with prime order q, where q divides $p - 1$.

(*i*) Give two advantages of using a multiplicative subgroup of prime order, as opposed to just using $\mathbb{Z}_p^*$, in cryptographic schemes based on the Discrete Logarithm problem. [2 marks]

(*ii*) Why is it possible to choose q substantially smaller than p, and what is an advantage of doing so? [4 marks]