5 Cryptography (mgk25)

(*a*) How many different functions ($\rightarrow$) or permutations ($\leftrightarrow$) exist of each of the following types?

(*i*) $\{0,1\}^{256} \rightarrow \{0,1\}^{128}$

(*ii*) $\{0,1\}^{128} \leftrightarrow \{0,1\}^{128}$

(*iii*) $\mathbb{F}_{2^{64}} \rightarrow \mathbb{Z}_{10}^4$

(*iv*) $\mathbb{Z}_{pq} \leftrightarrow \mathbb{Z}_p \times \mathbb{Z}_q$

(*v*) $\mathbb{Z}_{13}^* \rightarrow \mathbb{Z}_{15}^*$

(*vi*) $\mathbb{E}(\mathbb{Z}_p, a, b) \rightarrow \{0,1\}$ [6 marks]

(*b*) X.509 certificates and Kerberos tickets are both trusted-third-party mechanisms for key distribution.

(*i*) Name six data fields found in a typical X.509 certificate. [3 marks]

(*ii*) Describe three key differences between X.509 certificates and Kerberos tickets. [3 marks]

(*iii*) What is the purpose of a ticket-granting ticket in Kerberos? [2 marks]

(*c*) Even though elliptic-curve group elements correspond to points in a two-dimensional space, they are often represented by three-dimensional coordinates in cryptographic implementations. Why is this done? [2 marks]

(*d*) Let (Gen, H_s) be a collision-resistant hash function. Is (Gen, H'_s) with $H'_s(x) = H_s(H_s(x))$ necessarily also collision resistant? Justify your answer. [4 marks]