# 2002 Paper 3 Question 2

## Introduction to Security

(*a*) (*i*) Explain the collision resistance requirement for the hash function used in a digital signature scheme. [4 marks]

(*ii*) Show how the DES block cipher can be used to build a 64-bit hash function. Is the result collision resistant? [4 marks]

(*b*) A sequence of plaintext blocks $P_1, \ldots, P_8$ is encrypted using DES into a sequence of ciphertext blocks. Where an IV is used, it is numbered $C_0$. Owing to a transmission error, one bit in ciphertext block $C_3$ changes its value, and as a consequence, the receiver obtains after decryption a corrupted plaintext block sequence $P'_1, \ldots, P'_8$. For the following modes of operation, how many bits do you expect to be wrong in each block $P'_i$?

(*i*) Cipher block chaining. [2 marks]

(*ii*) 64-bit output feedback. [2 marks]

(*c*) (*i*) Explain the *Feistel principle* used by block ciphers such as DES and its purpose. [4 marks]

(*ii*) Using a given pseudo-random function $F : \{0,1\}^{100} \rightarrow \{0,1\}^{100}$, construct a pseudo-random permutation $P : \{0,1\}^{300} \rightarrow \{0,1\}^{300}$ by extending the Feistel principle appropriately. [4 marks]