2009 Paper 5 Question 9

Introduction to Security

(*a*) Make the following statements correct by changing one word or number. (Negating the sentence is not sufficient.)

(*i*) The Advanced Encryption Standard defines a 16-round Feistel cipher. [1 mark]

(*ii*) Files encrypted with Cipher Block Chaining start with a zero initial vector. [1 mark]

(*iii*) Each user on a Unix system is identified by a unique prime number. [1 mark]

(*iv*) The "read" bits associated with a Unix directory affect whether the files in its subdirectory "`foo`" can be accessed. [1 mark]

(*v*) The "real user ID" associated with a Unix process determines its access rights. [1 mark]

(*b*) Name *five* examples of actions for which a Unix application will need to be invoked with *root* privileges. [5 marks]

(*c*) Explain the attack on Double DES that motivates the use of Triple DES. [6 marks]

(*d*) Under which conditions is the Vignère cipher unconditionally secure? [4 marks]