2007 Paper 4 Question 8

Introduction to Security

(*a*) Your colleague wants to use a secure one-way hash function h in order to store h(password) as password-verification information in a user database for which confidentiality might become compromised. For h, she suggests using an existing CBC-MAC routine based on AES with all bits of the initial vector and the 128-bit AES key set to zero. Is this construct a suitable one-way hash function for this application? Explain why. [8 marks]

(*b*) Explain how, and under which circumstances, overlong UTF-8 sequences could be used to bypass restrictions regarding which files an HTTP server serves. [8 marks]

(*c*) Name *four* techniques that can be used to make buffer-overflow attacks more difficult. [4 marks]