

# 1 Tutorial 5

1. Prof. Beanstalk makes the following claim: (2 marks)

*Stack smashing attacks are made possible by the fact that stacks grow downwards (towards smaller addresses) on most popular modern architectures. Therefore, future architectures should ensure that the stack grows upwards; this would provide a good defense against buffer overruns.*

Do you agree or disagree? Why?

2. Alice and Bob share a secret key  $k$ . Alice encrypts a long message  $m$  in CBC mode and sends the resulting ciphertext,  $c$ , to Bob. Say the cipher block size is 64 bits (as in DES). Suppose that because of a transmission error, Bob receives a message  $c'$  which is identical to  $c$  except that an extra bit is inserted at some point. That is,  $c'$  is one bit longer than  $c$ , but otherwise identical to it. What is the maximum number of erroneous bits that will be present in the plaintext after Bob decrypts  $c'$ ? (1.5 marks)
3. You stumble upon an old ciphertext in a book close to where the book discusses cryptographic methods. You suspect that the ciphertext has been encrypted with a Vigenère cipher so you look for repeated strings in the ciphertext. The string `wxfirbglgwaw` is found to occur thrice in the ciphertext. The first occurrence starts at character position 38, the second at 59 and the third at 80 (assuming that the count starts from 1). You make an inspired guess that the ciphertext sequence `wxfirbglgwaw` is the encryption of the word *cryptography*. If this guess is correct, what is the key? (1.5 marks)
4. If one time pads are provably secure, why are they so rarely used? (1 mark)
5. Compute  $\{10110100\} \times \{01010011\}$  in the finite field  $\text{GF}(2^8)$ , assuming that the irreducible polynomial for the finite field is  $x^8 + x^4 + x^3 + x + 1$ . (1 mark)
6. Find an integer that leaves a remainder of 9 when it's divided by either 10 or 11, but that is divisible by 13. (1 mark)
7. Find a primitive root of 6 or show that 6 has no primitive root. (1 mark)
8. Use modular exponentiation to compute  $7236^{65537} \pmod{7}$ . Do not use Fermat's theorem in your computation, i.e., do not use the fact that for  $x \perp 7, x^6 \equiv 1 \pmod{7}$ . (1 mark)