The University of Newcastle
School of Electrical Engineering and Computer Science

COMP3260/COMP6360 Data Security
Week 11 Workshop – 22 & 23 May 2019

Sample Exam Questions

NOTE: This are just sample exam questions, to give you an idea about type of questions and what kind of solutions you need to provide; there will be only 8 questions in the final exam and some/all of them will be DIFFERENT. It is not enough to study these solutions; you need to study all the lecture notes and questions from tutorials, assignments and tests.

1. Give definitions of perfect secrecy, unconditional security and computational security.

2. For each of the following ciphers, state if they achieve perfect secrecy, unconditional security, computational security, or none of the above. Justify your answer.

    a. One time pad
    b. Homophonic cipher where each homophone appears in the ciphertext at most once
    c. Higher order homophonic cipher
    d. Caesar cipher
    e. DES
    f. AES
    g. RSA

3. Suppose that M is a 4-digit integer enciphered digit by digit, using a circular Caesar-type substitution cipher with key K, $0 \le K \le 9$, and that all possible 4-digit integers are equally likely. For example, if the plaintext M=1234 is enciphered with key K=7, then the ciphertext is C = 8901 and if the plaintext M'=0098 is enciphered with the same key, the corresponding ciphertext is C'=7765. How much ciphertext is needed to break this cipher? Explain your answer.

4. The Playfair cipher uses a 5×5 matrix of 25 letters as a key (letter J is not used), and enciphers a block of two letters at the time. Find the unicity distance for the Playfair cipher.

5. What is Kerckhoff's principle?

6. What is the difference between a stream and a block cipher?

7. S-boxes are commonly used in symmetric encryption systems to provide substitution and non-linearity. Explain in detail how S-boxes are designed in the following cryptosystems.

    a. ***AES***

    b. ***DES***

8. For each of the following elements of DES, indicate the comparable element in AES or explain why it is not needed in AES.

    a. XOR with subkey
    b. XOR of the output of F-function with the left half of data block
    c. F-function
    d. Permutation P
    e. Swapping of halves of the data block

9. With the aid of diagram describe the following two modes of operation of DES: Cipher Feedback Mode and Output Feedback Mode.

10. What is Double DES and how is it vulnerable to Meet-in-the-Middle Attack?

11. Consider the RSA scheme.

a. If the public key is *(e, n) = (3, 33),* encipher the plaintext *M = 7*. Break the cipher by finding p, q and d. Decipher the ciphertext *C = 2*. (You don't need a calculator – use fast exponentiation!)

b. Prove that M^{ed} mod $n = M$ for all values of M, including those where gcd $(M, n) \neq 1$.

12. Explain how a public-key cryptosystem can provide both privacy and authenticity.

13. Outline Diffie-Hellman key exchange scheme and show how it can be used for 3 or more parties.

14. What is a one-way hash function? What is a difference between a one-way hash function and a message authentication code (MAC)?

15. With the aid of diagrams describe in detail HMAC.

16. What are the main issues that digital signatures address?

17. What are the differences between a direct digital signature system and an arbitrated digital signature system?