A22648

Calculators may be used in this examination provided they are not capable of being used to store alphabetical information other than hexadecimal numbers.

UNIVERSITY OF BIRMINGHAM

School of Computer Science

MSc Computer Science
MSc Advanced Computer Science
MSc Computer Security
First Year – UG Affiliate Science without Borders Computer Science
Fourth Year – MSci Computer Science
Fourth Year – MEng Computer Science/Software Engineering
Fourth Year – MSci Mathematics and Computer Science
Fourth Year – MEng Electronic and Software Engineering

06 20008

Cryptography

Summer Examinations 2015

Time allowed: 1 hour 30 minutes

[Answer ALL Questions]

1. (a) What are the required properties of a Cryptographic Hash Function? **[6%]**

   (b) Briefly describe a way how a hash function can be constructed from a block cipher. **[6%]**

   (c) Consider the following function h: The input of h is a bit vector of arbitrary length. The output of h is a pair (π, y), where π is a random permutation on 128 bits and y is the result of applying π to the least 128 bits of the input. Is this function a cryptographic hash function? Justify your answer. **[8%]**

2. (a) How do you encrypt long messages using a block cipher? **[6%]**

   (b) Describe the electronic codebook mode. **[6%]**

   (c) By constructing a suitable game show that the electronic codebook mode does not satisfy IND-CPA security. **[10%]**

3. (a) Explain how to use public key cryptography for key exchange algorithms. **[6%]**

   (b) Consider the following El Gamal parameters: $p = 23$, $q = 11$, $g = 3$ and 5 as private key. Calculate the public key, and the encryption of $M = 4$ with the random 8. **[8%]**

   (c) Show that the attacker has a non-negligible probability of winning the authenticated encryption game for El Gamal. **[10%]**

4. (a) Perform the following operations in $\mathbb{Z}_{11}$:

      (i) 8^{33} **[3%]**

      (ii) Calculate the multiplicative inverse of 7 by using the extended Euclidean algorithm. **[6%]**

   (b) Calculate $(x^3 + 1) * (x^2 + x + 1)$ in $\mathbb{F}_2[x]/(x^4 + x + 1)$. **[7%]**

   (c) Discuss some of the legal and ethical issues surrounding AACS and DRM in general. You should give at least three legal or ethical issues. **[8%]**

5. Consider a website which provides downloads of out-of-copyright sheet music. Each piece of sheet music is provided as a pdf-file together with a hash of the pdf-file over an unencrypted http-connection.

   (a) Why is this not enough to prevent attackers modifying the pdf-file in transit by inserting malware? **[5%]**

   (b) provide a fix which prevents those attacks, explaining any assumptions that are required for your solution to work over an unencrypted http-connection. **[5%]**