A22648 No calculator permitted in this examination

UNIVERSITY OF BIRMINGHAM

School of Computer Science

First Year – Degree of BSc with Honours
Artificial Intelligence and Computer Science
Computer Science

Final Year – Degree of MEng with Honours
Computer Science/Software Engineering

Final Year – Joint Degree of MEng with Honours
Computer Science and Civil Engineering

Degree of MSc
Advanced Computer Science
Natural Computation
Internet Software Systems
Computer Science

Undergraduate Occasional
Business

06 20008

Cryptography

Summer Examinations 2007

Time allowed: 1 ½ hours

[Answer TWO Questions from EACH PART]

A22648

[redacted]8 No Calculator

Part I

1. Briefly explain the following concepts: $\boxed{4+4+4+4+4}$

   (a) Ciphertext

   (b) Symmetric Cipher

   (c) Mode of Operation

   (d) Message Authentication Code

   (e) Zero Knowledge Proof

2. Describe the basic workings of a Feistel Cipher. $\boxed{20}$

3. Discuss the differences and similarities between Block Ciphers and Stream Ciphers. Give an example for each. $\boxed{15+5}$

Part II

4. Carry out the following muliplications on permutations: $\boxed{8+7}$

   (a) $(1\ 2\ 4)(3\ 6\ 5) * (2\ 3\ 6)$

   Compute the inverse of the following permutation:

   (b) $(1\ 3\ 2\ 5\ 6)$

5. Compute the following bit operation modulo $x^8 + x^4 + x^3 + x + 1$ in the finite field $\mathbb{F}_{2^8}$:

$$0xAB \otimes 0xF1$$

   Give the single steps of your computation. It is sufficient to give the result as a polynomial in $\mathbb{F}_{2^8}$. $\boxed{15}$

   [Hint: Translate the hexadecimal numbers into polynomials first.]

6. Consider $\mathbb{Z}_{55}$ together with multiplication $\cdot$ and the subgroup in $(\mathbb{Z}_{55}, \cdot)$ generated by 26

$$\langle 26 \rangle = \{26, 16, 31, 36, 1\}.$$

   Compute the following discrete exponentations in $(\mathbb{Z}_{55}, \cdot)$. $\boxed{5+5+5}$

   (a) 26^7

   (b) 26^{14}

   (c) 26^{-1}

Part III

7. Let L be a 10 bit Linear Feedback Shift Register with connection polynomial $c(x) = x^9 + x^8 + x^4 + x + 1$ and seed $s = [1, 0, 1, 1, 1, 0, 0, 1, 1, 0]$ (i.e. the last bit of s, 0, becomes the first keystream bit). Compute 8 bits of the keystream. Give both key bits and feedback bits. $\boxed{15}$

8. Perform hashing with the second round of the MD4 hash function adapted as follows:

$$\begin{aligned}
&(H_1, H_2, H_3, H_4) := (A, B, C, D) \\
&t := A + G(B, C, D) + M_i + (M_{i+2} \lll 2) \\
&(A, B, C, D) := (D, t, B, C) \\
&(A, B, C, D) := (H_1 + A, H_2 + B, H_3 + C, H_4 + D)
\end{aligned}$$

   where $G(X, Y, Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$.

   Assume that we compute a 16 bit hash, i.e., A, B, C, D are 4 bit words, G takes three 4 bit arguments and the message blocks are 16 bits partitioned into 4 bit chunks. Initially let $(A, B, C, D) = (0x1, 0x4, 0xA, 0xB)$ and $i = 0$; i is increased by 1 for every 16 bits of the message hashed.

   Compute the 16 bit hashes for the following 32 bit message given as hexadecimal number: $M := 0x13579BDF$.

   Initialise the algorithm with

$$\begin{aligned}
M_0|M_1|M_2|M_3|M_4|M_5|M_6|M_7 \;&:=\; 0x1 \mid 0x3 \mid 0x5 \mid 0x7 \mid 0x9 \mid 0xB \mid 0xD \mid 0xF \mid \\
&=\; 0001|0011|0101|0111|1001|1011|1101|1111|
\end{aligned}$$

   give the intermediate steps and the final result again as a hexadecimal number. $\boxed{15}$

9. Peform RSA secret key generation, encryption, and decryption for the following parameters: Prime numbers $p = 5$ and $q = 11$, Alice's chosen integer $e = 23$, and message $M = 26$. $\boxed{15}$