No calculator permitted in this examination

UNIVERSITY OF BIRMINGHAM

School of Computer Science

Final Year – Degree of MEng
Computer Science/Software Engineering

Degree of MSc
Advanced Computer Science
Computer Security
Intelligent Systems Engineering

Undergraduate Occasional
Computer Science/Software Engineering
Engineering
Mathematics

06 20008

Cryptography

Summer Examinations 2009

Time Allowed: 1 ½ hours

[This paper contains Three parts
Answer TWO Questions from EACH Part]

Turn over

Part I

1. Briefly explain the following concepts: [3+3+3+3+3]

   (a) Plaintext

   (b) Block Cipher

   (c) Cryptographic Hash Function

   (d) Key Exchange Protocols

   (e) Digital Signature

2. Discuss differences between asymmetric and symmetric ciphers and their respective advantages and disadvantages. Give an example for each type of cipher. [12 + 3]

3. Explain the working of the Pretty Good Privacy (PGP) protocol, its advantages and drawbacks, as well as its socio-ethical motivation. [15]

Part II

4. Carry out the following operations with permutations: 2+1+2

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

   (b) $(2\,3\,5)(1\,4\,6)^{-1}$

   (c) Apply $(1\,2\,7\,5\,3)(4\,6\,8\,9)$ to the list of letters `L L B H E E C Y T`

   Show that the following holds: 10

   (d) Let $(S, \star)$ be a finite set S that is closed under the binary operation $\star$. Let $f \in S$ be a left unit element, such that for every $s \in S$ holds $f \star s = s$, and let $e \in S$ be a right unit element, such that for every $s \in S$ holds $s \star e = s$. Then $f = e$.

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

   $$0xAB \otimes 0xF1$$

   Give the single steps of your computation. 15

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

6. Carry out the following modulo calculations in $\mathbb{Z}_{17}$: 1+2+2

   (a) $13 - 15$

   (b) 2^6

   (c) 2^{-1}

   Show that the following holds: 10

   (d) Assume $ab \equiv ac (\mathrm{mod}\, m))$ and $gcd(a, m) = 1$ then $b \equiv c (\mathrm{mod}\, m)$. (I.e., we can cancel a in $ab \equiv ac (\mathrm{mod}\, m)$.)

Part III

7. Consider a block cipher algorithm $\mathcal{A}$ that enciphers message blocks of size 4 with keys of length 6. Let $\mathcal{A}$ have the following components:

   - An expansion permutation E with schema 4 3 1 2 4 3.
   - An S-Box S of the form:

S	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1100	0001	1010	1111	1001	0010	0110	1000	0000	1101	0011	0100	1110	0111	0101	1011
01	1010	1111	0100	0010	0111	1100	1001	0101	0110	0001	1101	1110	0000	1011	0011	1000
10	1001	1110	1111	0101	0010	1000	1100	0011	0111	0000	0100	1010	0001	1101	1011	0110
11	0100	0011	0010	1100	1001	0101	1111	1010	1011	1110	0001	0111	0110	0000	1000	1101

   - A P-Box P that has the permutation schema 2 4 3 1.

   Moreover, keys for $\mathcal{A}$ are computed from an initial 6 bit key K as follows:

   Let $K_0 = K = L_0 \| R_0$. Then $K_i = L_i \| R_i, i = 1, 2, \ldots$ where L_i and R_i are both of 3-bit length and computed by

$$\begin{aligned} L_i &= L_{i-1} \lll 1 \\ R_i &= R_{i-1} \lll 2 \end{aligned}$$

   For a given input message $M := M_0 \| M_1 \| \ldots \| M_n$, where each M_i is a block of 4 bits, each block M_i is enciphered by the following steps:

   1. $Q := E(M_i)$ (Apply expansion permutation E to M_i.)
   2. $Q := R \oplus K_i$ (Xor the i^{th} key to the result of step 1.)
   3. $Q := S(R)$ (Apply S-Box S to the result of step 2.)
   4. $Q := P(R)$ (Apply P-Box P to the result of step 3.)
   5. $C_i := Q$

   The resulting ciphertext is then $C := C_0 \| C_1 \| \ldots \| C_n$.

   Given the plaintext message $M = 10110111$ and key $K = 010011$.

   (a) Compute the sub-keys K_0, K_1.

   (b) Encrypt M with cipher $\mathcal{A}$. Note carefully all the intermediate results of the single steps of the algorithm.

4+16

8. Consider a game of Cluedo for three players with 12 cards. (Cluedo is a murder mystery game in which players must determine who committed the crime, where they did it, and what weapon was used.) In preparation of the game the cards are shuffled and distributed such that each player gets three cards and three cards are put face down on the table (i.e., no player is allowed to see them).

   In each turn a player makes an accusation by suggesting a combination of three cards (a suspect, a murder weapon, and a location). One of the other two players can disprove the suggestion if they have one of the cards in question. The player then shows this card to the accusing player without revealing it to the third player.

   For example, Alice suggests "Mrs White, with the Lead Pipe, in the Kitchen". If Bob has the card representing the "Lead Pipe" he shows it to Alice without revealing it to Carol.

   To play the game electronically design protocols and commitment schemes for the preparation phase and for a player's turn. Assume that the players would not trust each other. Give sufficient explanations why your protocol works. [20]

9. Consider the following stream cipher generating keystreams of numbers up to $0, \ldots, 2^3 - 1$. Let S and K be arrays of size 8 and 4, respectively. The function "swap" exchanges the contents of two cells of an array.

```
S[0..7] := [0,1,2,3,4,5,6,7]
K[0..3] := [1,3,4,7]

KeyInitialisation(S,K)

i := 0
j := 0
while GeneratingOutput:
        i := (i + 1) mod 8
        j := (j + S[i]) mod 8
        swap(S[i],S[j])
        output S[(S[i] + S[j]) mod 8]
end
```

   (a) Design a **KeyInitialisation** function that performs an intial permutation of S with respect to K using the swap function. Make sure that your algorithm swaps each cell of S at least once and uses each key element of K at least twice. [8]

   (b) Use your **KeyInitialisation** function to compute the content of S before the GeneratingOutput phase. Then compute the first 2 elements of the output stream and give the content of S afterwards. [12]