Two hours

A table of exponentiations mod 35 is provided at the back of this question paper.

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cryptography

Date: Wednesday 26th January 2011
Time: 09:45 - 11:45

Please answer question ONE and TWO other questions

Question 1 is worth 10 marks. Questions 2-4 are worth 20 marks each.

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

[PTO]
1. **COMPULSORY**

   a) Why do the 26! different possible keys in a monoalphabetic substitution cipher not provide any real security against cryptanalysis? (1 mark)

   b) Briefly explain the terms **confusion** and **diffusion** in the context of substitution-permutation ciphers. (1 mark)

   c) Briefly explain the term **avalanche effect** and say why it is a desirable property of a cipher. (1 mark)

   d) What is a **group**? What can you do in a **ring** that you cannot do in a group? What can you do in a **field** that you cannot do in a ring? (1 mark)

   e) Briefly explain the term **triple DES**. Why are multiple DES encryptions genuinely stronger than a single DES encryption? (1 mark)

   f) Briefly explain the terms **one-way function** and **trapdoor one-way function**. (1 mark)

   g) State Fermat’s Theorem. State Euler’s Theorem. (You do not have to prove these theorems.) (1 mark)

   h) Why is it that in certain public key cryptographic tasks, discrete log problems in prime fields can be substituted by elliptic curve techniques? (1 mark)

   i) Briefly explain the difference between a **hash** and a **MAC**. (1 mark)

   j) In quantum cryptography, describe the two ways of encoding 0 and the two ways of encoding 1. What is the relationship between them? (1 mark)
2. a) In the context of block ciphers, what is an S-box? (3 marks)

b) What are the most important properties of an S-Box? (4 marks)

c) Explain how S-boxes are applied in DES. (3 marks)

d) Explain how S-boxes are applied in AES. (3 marks)

e) What is the main difference between the use of S-boxes in DES and AES. (3 marks)

f) Below is a prospective S-box on 4-bit bitpatterns to be used in some prospective block cipher. The leftmost 2-bits index the row and the rightmost 2-bits index the column. State as many things that are wrong with this design as you can. (4 marks)

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>6</td>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>12</td>
<td>4</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>14</td>
<td>13</td>
<td>15</td>
</tr>
</tbody>
</table>
3. a) Describe the Extended Euclid Algorithm for finding not only the GCD of two numbers \(x\) and \(y\), but also the coefficients \(a\) and \(b\) such that \(\text{GCD}(x, y) = ax + by\). (4 marks)

b) Describe how the Extended Euclid Algorithm can be used to find the multiplicative inverse of a number \(x\) modulo a number \(y\), provided that \(\text{GCD}(x, y) = 1\). (3 marks)

c) Describe the RSA public key cryptography scheme. (6 marks)

d) Construct an example of the RSA scheme as follows. The two primes to be used for the modulus \(N\) are 5 and 7. What is \(\phi(N)\)? What is the smallest encryption key that will work? What is the corresponding decryption key? Encrypt the message 12 using your smallest encryption key. Confirm that you can decrypt the ciphertext using your decryption key. (7 marks)

4. a) Outline four ways in which a hash function \(H\) can be combined with symmetric cryptography \(E_K(\cdot)\) and an optional additional piece of secret information \(S\), to authenticate a message \(M\). Say which of these is/are the most efficient. (6 marks)

b) What does a digital signature provide that a hash or MAC does not? (3 marks)

c) Choose your most useful scheme from part a) and outline how to strengthen it by exploiting a digital signature. (3 marks)

d) Explain the terms \textit{preimage resistance}, \textit{second preimage resistance}, \textit{collision resistance} for hash functions. Why does DES prove inadequate as a secure hash function? (4 marks)

e) Describe the Diffie-Hellman key agreement protocol. (4 marks)

\textbf{END OF EXAMINATION}
TableForm[Table[PowerMod[a, n, 35], {a, 1, 35}, {n, 1, 35}]]

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
1 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
```