COMP 61411

Two hours

Question ONE is COMPULSORY

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

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cryptography

Date: Thursday 26th January 2017

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) Say approximately, how many different new malware signatures are seen every day by typical cybersecurity software providers. (1 mark)

b) Consider a block cipher working on 64 bit blocks. How many possible block ciphers are there in the ideal case? How many are there if a key of 64 bits is used? (1 mark)

c) What is the key idea behind the Babbage/Kasiski method of breaking the Vignere cipher? (1 mark)

d) Which stage of an AES round is **not** a linear transformation? (1 mark)

e) Write down the three main ways of doing arithmetic using polynomials. (1 mark)

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

g) What property is possessed by counter mode, that is not possessed by any other standard block cipher mode? (1 mark)

h) What is the major vulnerability of the Diffie-Hellman protocol? (1 mark)

i) What unique quantum property is used in Eckert's QKD protocol? (1 mark)

j) What does the term **capacity** refer to in a sponge function? (1 mark)

2. 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) Given a block cipher, write down the main ways that it may be used to encrypt larger amounts of data. (You do not need to give a full description.) (6 marks)

   d) Describe the XTS-AES scheme. (7 marks)

3. a) Describe the structure of AES. (6 marks)

   b) Briefly describe the principles behind the construction of the AES S-box. (3 marks)

   c) Briefly describe the working of the Mix Columns stage of AES. (3 marks)

   d) What idea from Classical Encryption is the key expansion technique in AES based on? (2 marks)

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

4. a) What goal was the *Keywrap* algorithm intended to meet? (4 marks)

   b) Describe the *Keywrap* algorithm. (6 marks)

   c) Explain the RSA-PSS digital signature scheme. (5 marks)

   d) What useful property does the RSA-PSS digital signature scheme have? (2 marks)

   e) Describe the Diffie-Hellman key agreement protocol. (3 marks)

END OF EXAMINATION

```
TableForm[Table[PowerMod[a, n, 35], {a, 1, 35}, {n, 1, 35}]]
```

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	32	29	23	11	22	9	18	1	2	4	8	16	32	29	23	11	22	9	18	1	2	4	8	16	32	29	23	11	22	9	18
3	9	27	11	33	29	17	16	13	4	12	1	3	9	27	11	33	29	17	16	13	4	12	1	3	9	27	11	33	29	17	16	13	4	12
4	16	29	11	9	1	4	16	29	11	9	1	4	16	29	11	9	1	4	16	29	11	9	1	4	16	29	11	9	1	4	16	29	11	9
5	25	20	30	10	15	5	25	20	30	10	15	5	25	20	30	10	15	5	25	20	30	10	15	5	25	20	30	10	15	5	25	20	30	10
6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6
7	14	28	21	7	14	28	21	7	14	28	21	7	14	28	21	7	14	28	21	7	14	28	21	7	14	28	21	7	14	28	21	7	14	28
8	29	22	1	8	29	22	1	8	29	22	1	8	29	22	1	8	29	22	1	8	29	22	1	8	29	22	1	8	29	22	1	8	29	22
9	11	29	16	4	1	9	11	29	16	4	1	9	11	29	16	4	1	9	11	29	16	4	1	9	11	29	16	4	1	9	11	29	16	4
10	30	20	25	5	15	10	30	20	25	5	15	10	30	20	25	5	15	10	30	20	25	5	15	10	30	20	25	5	15	10	30	20	25	5
11	16	1	11	16	1	11	16	1	11	16	1	11	16	1	11	16	1	11	16	1	11	16	1	11	16	1	11	16	1	11	16	1	11	16
12	4	13	16	17	29	33	11	27	9	3	1	12	4	13	16	17	29	33	11	27	9	3	1	12	4	13	16	17	29	33	11	27	9	3
13	29	27	1	13	29	27	1	13	29	27	1	13	29	27	1	13	29	27	1	13	29	27	1	13	29	27	1	13	29	27	1	13	29	27
14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14	21	14
15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15
16	11	1	16	11	1	16	11	1	16	11	1	16	11	1	16	11	1	16	11	1	16	11	1	16	11	1	16	11	1	16	11	1	16	11
17	9	13	11	12	29	3	16	27	4	33	1	17	9	13	11	12	29	3	16	27	4	33	1	17	9	13	11	12	29	3	16	27	4	33
18	9	22	11	23	29	32	16	8	4	2	1	18	9	22	11	23	29	32	16	8	4	2	1	18	9	22	11	23	29	32	16	8	4	2
19	11	34	16	24	1	19	11	34	16	24	1	19	11	34	16	24	1	19	11	34	16	24	1	19	11	34	16	24	1	19	11	34	16	24
20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20	15	20
21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21	21
22	29	8	1	22	29	8	1	22	29	8	1	22	29	8	1	22	29	8	1	22	29	8	1	22	29	8	1	22	29	8	1	22	29	8
23	4	22	16	18	29	2	11	8	9	32	1	23	4	22	16	18	29	2	11	8	9	32	1	23	4	22	16	18	29	2	11	8	9	32
24	16	34	11	19	1	24	16	34	11	19	1	24	16	34	11	19	1	24	16	34	11	19	1	24	16	34	11	19	1	24	16	34	11	19
25	30	15	25	30	15	25	30	15	25	30	15	25	30	15	25	30	15	25	30	15	25	30	15	25	30	15	25	30	15	25	30	15	25	30
26	11	6	16	31	1	26	11	6	16	31	1	26	11	6	16	31	1	26	11	6	16	31	1	26	11	6	16	31	1	26	11	6	16	31
27	29	13	1	27	29	13	1	27	29	13	1	27	29	13	1	27	29	13	1	27	29	13	1	27	29	13	1	27	29	13	1	27	29	13
28	14	7	21	28	14	7	21	28	14	7	21	28	14	7	21	28	14	7	21	28	14	7	21	28	14	7	21	28	14	7	21	28	14	7
29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29	1	29
30	25	15	30	25	15	30	25	15	30	25	15	30	25	15	30	25	15	30	25	15	30	25	15	30	25	15	30	25	15	30	25	15	30	25
31	16	6	11	26	1	31	16	6	11	26	1	31	16	6	11	26	1	31	16	6	11	26	1	31	16	6	11	26	1	31	16	6	11	26
32	9	8	11	2	29	18	16	22	4	23	1	32	9	8	11	2	29	18	16	22	4	23	1	32	9	8	11	2	29	18	16	22	4	23
33	4	27	16	3	29	12	11	13	9	17	1	33	4	27	16	3	29	12	11	13	9	17	1	33	4	27	16	3	29	12	11	13	9	17
34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34	1	34
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0