COMP61411

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: Friday 29th January 2016

Time: 14:00 - 16:00

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) Distinguish between active and passive attacks. Give two examples of a passive attack and two examples of an active attack. (1 mark)

b) When a plaintext is allowed to be an arbitrary bitpattern, explain why there is no practical difference between unconditional security and computational security of a cipher. (1 mark)

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

d) Write down the equations for a round of a Feistel cipher. (1 mark)

e) What property of a number n is required so that Z_n forms a field under the usual arithmetic operations? (1 mark)

f) Define Euler's Totient function for a number n. (1 mark)

g) What unique property is possessed by digital signatures, that is not possessed by any other class of cryptographic primitive? (1 mark)

h) **HMAC** requires 3 additional hash calculations compared with using the constituent hash algorithm alone. Brefly indicate what they are. (1 mark)

i) In Weisner's quantum money, why does a forgery produce a 25% error rate when its quantum serial number is checked? (1 mark)

j) In 1994, Shor discovered a quantum algorithm for factoring integers that works in polynomial time. Why is this not an immediate threat to RSA? (1 mark)

2. a) In breaking Enigma, so-called cillies were often tried first. Describe three typical cillies used in Enigma cryptanalysis. (3 marks)

b) In breaking Enigma, cribs were crucial. What is a crib, and why is a crib so important for Enigma cryptanalysis? (4 marks)

c) Why is triple DES preferred over double DES? Describe the vulnerability of double DES. (4 marks)

d) Below is the AES S-box. Apply it to the hex string 520DDA8B. (3 marks)

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

e) Describe the key expansion process in AES. (6 marks)

[PTO]

3. a) Write down the *Miller Rabin Algorithm* for probabilistically testing a number for primality. (4 marks)

   b) Why does the algorithm not provide certainty regarding the primality of a number, and what remedy for this is there? (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 $\phi(N)$? Choose 11 as the encryption key. What is the corresponding decryption key? Encrypt the message 17 using your smallest encryption key. Confirm that you can decrypt the ciphertext using your decryption key. (7 marks)

4. a) What is the main vulnerability of the RSA public key encryption algorithm? Give a small illustration. (4 marks)

   b) Describe *Optimal Asymmetric Encryption Padding* (OAEP). (6 marks)

   c) What defence does OAEP provide against malevolent manipulation of the final cyphertext produced? (4 marks)

   d) Explain the terms *preimage resistance*, *second preimage resistance*, *collision resistance* for hash functions. Why is DES encryption inadequate as a secure hash function? (3 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