UNIVERSITY OF SOUTHAMPTON ELEC6242W1

SEMESTER 2 EXAMINATIONS 2014/15

Cryptography

Duration 120 Minutes (2 Hours)

This paper contains 4 questions

Answer THREE questions

An outline marking scheme is shown in brackets to the right of each question

Only University approved calculators MAY be used.

A foreign language word to word® translation dictionary (paper version) is permitted provided it contains no notes, additions or annotations.

Number of Pages: 5

1. (a) Calculate the minimum number of bits needed to represent each of the following two messages:
M1= 01111
M2= AAAA

[6 marks]

(b) Explain in details the following terms:
1) Microdots
2) Index of Coincidence (IC)

[6 marks]

(c) Encrypt the following message(M3) using a columnar transposition cipher with a keyword “CAR”

M3= Keep your face to the sunshine and you cannot see a shadow

[9 marks]

(d) Decrypt the following message and explain the technique which was used to encrypt it.

Gtw hwyiwg lv tskkrmwhh nsb zw gl mlg wckwyg gll nfyt viln orvw. Vli rv blf hgsig lvv drgt old wckwygsgrlmh blf ylfox wmx fk kowshsmgob hfikirhwx, syylixrmu gl s hyrwmgrvry hgfxb rmgl tfnsm tskkrmwhh. Zirgrht hyrwmgrhgh vlfmx gtsg dwoozwrmu xlwh mlg iwvowyg tld dwoo gtrmuh siw ulrmu, zfg dtwgtwi gtrmuh siw ulrmu zwggwi gtsm wckwygwx. Xi Ilzz Ifgowxuw lv Fmrewihrgb Yloowuw Olmxlm hsrx trh gwsn dwiw hfikirhwx gl vrmx qfhg tld rnkligsmg wckwygsgrlm rh. Tw hsrx: ‘Rg rh lvgwm hsrx gtsg blf droo zw tskkrwi rv blfi wckwygsgrlmh siw oldwi. ‘Dw vrmx gtsg gtwiw rh hlnw gifgt gl gtrh - oldwi wckwygsgrlmh nspw rg nliw orpwob gtsg sm lfgylnw droo wcywwx gtlhw wckwygsgrlmh smx tsew s klhrgrew rnksyg lm tskkrmwhh.

[12 marks]

2. (a) Compute the following in Z_{313}

$1) 2192^{23}$ 2) $\sum_{i=1}^{5} 1251^{i}$ 3) $62 * 27$

[9 marks]

(b) Explain how a public key encryption algorithm is used to solve the key distribution problem of private key encryption systems.

[3 marks]

(c) You hear on the news that an efficient algorithm is invented which can factorise any integer number in less than 24 hours. Explain how this might affect the security of RSA encryption schemes.

[9 marks]

(d) A secret has been encrypted using RSA with a modulus of 449329 and an exponent of 89597. The encrypted message is 362797. What is the secret?

[12 marks]

TURN OVER

3. (a) Outline the principles of the quantum key distribution Scheme BB84.

[6 marks]

(b) Is it possible to eavesdrop on messages encrypted using quantum cryptography without being detected? Explain your answer.

[9 marks]

(c) Explain how to generate a public key for a McEliece cryptosystem.

[6 marks]

(d) Encrypt the plaintext (M= 0100) using a McEliece cryptosystem based on the single error correction code with the generator matrix G given below. You will need to use the invertible binary matrix S to generate your encryption key.

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}, \; S = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

[9 marks]

(e) Why is a McEliece cryptosystem considered to be a candidate for post quantum-computing cryptography?

[3 marks]

4. (a) Explain the meaning of Shannon Perfect Secrecy.

[6 marks]

(b) Consider a block cipher working on a block of 6 bits. How many possible mappings exist between the inputs and the outputs? If the secret key indicates which mapping to use, how many bits do you need to represent this key?

[3 marks]

(c) Illustrate by means of appropriate diagrams the AES encryption algorithm. Explain how you would use this algorithm to implement a semantically secure encryption scheme under chosen plaintext attack assuming the same key is used for multiple messages.

[12 marks]

(d) What does forgery mean?

[6 marks]

(e) Does the use of message authentication codes protect a communication link against Replay attacks? Explain your answer.

[6 marks]

END OF PAPER