UNIVERSITY OF SOUTHAMPTON

SEMESTER 2 EXAMINATIONS 2018/19

Cryptography

Duration 120 mins (2 hours)

This paper contains FOUR 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 dictionary is permitted ONLY IF it is a paper version of a direct ‘Word to Word’ translation dictionary AND it contains no notes, additions or annotations.

5 page examination paper

Question 1

(a) Explain the principles of rotor cipher machines

[5 marks]

(b) Give an example of how you can use textual Steganography to hide the message (M1) below.

M1 = Attend at 2 pm

[5 marks]

(c) Calculate the index of coincidence for the message M2 below.

M2= GDGOOONAOTOW

[5 marks]

(d) Compute the following in $\mathbb{Z}_{19}$

$1)18^7$ 2) $\sqrt{5}$ 3) $\frac{9}{14}$

[18 marks]

Question 2

Let E be the elliptic curve $y^2 = x^3 + 11x + 20$ over the field $\mathbb{F}_{13} = \mathbb{Z}_{13}$

We regard E as an Abelian group in the usual way.

(a) Find the order of this group, and indicate whether or not this is a cyclic group.

[10 marks]

(b) Find the point R= P+Q in the above group, where

P=(10, 5) and Q= (6,4).

[5 marks]

(c) Find all pairs of points (P,Q) such that:
P+Q= O

[8 marks]

(d) Explain by means of a numerical example how Bob can use the Elgamal encyption algorithm and the above group to send an encypted message to Alice. You are given the following information:
G=(6,4), Q_{Alice}= (10, 5).

[10 marks]

TURN OVER

Question 3

(a) Briefly outline the meaning of Shannon perfect secrecy. Do shift ciphers satisfy this notion? Explain your answer.

[10 marks]

(b) Outline the process of generating the round keys of the AES algorithm and explain how this process can enhance the security of this algorithm.

[10 marks]

(c) Given a Hash Function (F) with a digest size of 512 bits, explain with a numerical example how you can search for collision using the Birthday Attack. Indicate approximately using the big O notation how long it should take to find a collision using this attack.

[5 marks]

(d) Consider a block cipher working on a block of 4 bits. How many possible mapping exists between the input and the output? If the secret key indicates which mapping to use, how many bits do we need to represent this key?

[8 marks]

Question 4

(a) Use cryptanalysis methods to find the decryption key for the ciphertext below. Assume that a substitution technique has been used in the encryption.

Dspyh th s nlfmgib gvsg th ksig lx gvy Fmtgyz Qtmwzlo smz gvy thpsmz lx Wiysg Uitgstm. Tg th ulizyiyz ub Ymwpsmz gl gvy yshg, gvy Tithv Hys gl gvy mligv smz dyhg, smz gvy Uithglp Nvsmmyp gl gvy hlfgv. Tg vsz s klkfpsgtlm leyi gviyy otptlm smz vsh s glgsp siys lx. Dspyh vsh plmw nlshgptmy smz th psiwypb olfmgstmlfh, dtgv tgh vtwvyi kysqh tm gvy mligv smz nymgisp siysh, tmnpfztmw Hmldzlm Gvy nlfmgib ptyh dtgvtm gvy mligv gyokyisgy almy smz vsh s nvsmwysupy, ositgtoy nptosgy.

[10 marks]

b) Given an RSA Scheme with a public key of (N, e) = (899, 37). Deduce the secret key and show how you can use it to decrypt the message (M3) below:

M3=36

[13 marks]

(c) The message below has been encrypted using a Vigenère cipher. Deduce the possible length of the encryption key.

JEGRYPPZDAMLWERLJEGRYPZZIQMOQKBXYPLNHAGOWLSRJEGR

[10 marks]

End of Paper