UNIVERSITY OF SOUTHAMPTON

SEMESTER 2 EXAMINATIONS 2016/17

Cryptography

Duration 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 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) What is the difference between cryptanalysis techniques and decryption methods? Give an example of a cryptanalysis technique for substitution ciphers

[5 marks]

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

M1 = Keep Calm and Carry on

[5 marks]

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

M2= ss os be bs os

[5 marks]

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

1)$2^{1/18}$ 2) $\sqrt{11}$ 3) 3743^{666}

[18 marks]

Question 2

Let E be the elliptic curve $y^2 = x^3 + 3x + 20$ 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.

[5 marks]

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

P=(3, 2) and Q= (5,2).

[10 marks]

(c) What is the order of the element P (3, 2) in the above group? Explain your answer.

[8 marks]

(d) Explain by means of a numerical example how Alice and Bob can use the above group to agree on a shared secret over an insecure communication channel.
(Tip: Diffie-Hellman Key Exchange protocol may be useful in this context).

[10 marks]

TURN OVER

Question 3

(a) Will it be possible to rely on error correction techniques to authenticate the origin of a received message? Explain your answer.

[5 marks]

(b) Explain with the help of a functional diagram, the operational principles of Merkle-Damgard Scheme used to construct Hash functions.

[5 marks]

(c) Given a Hash Function (F) with a digest size of 1024 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.

[10 marks]

(d) E is secure encryption algorithm defined as follows

$E: \;\; K \times X \;\rightarrow\; X \qquad where \qquad K = X = \{0,1\}^{256}$

E_{CBC} is an implementation of the E algorithm in the cipher block chaining mode.

E_{CBC} is used to encrypt information which are transmitted over an insecure link whereas adversaries can access encrypted messages. Assume that the advantage of the adversary over E is zero in the case of one time key use. Also, assume that the longest message transmitted over the link is 256 bits.

Calculate the maximum number of messages which can be transmitted over this link using the same encryption key such that the advantage of an adversary capable of carrying out a chosen plain test attack (CPA) does not exceed 2^{-45}.

[13 marks]

Question 4

(a) Use cryptanalysis method to crack the cipher below.

(Tip: A substitution technique was used in the encryption)

Wmuotmx rh t ylfmgib gstg rh ktig lv gsw Fmrgwx Prmuxln. Rg hstiwh otmx zlixwih drgs Hylgotmx gl gsw mligs tmx Dtowh gl gsw dwhg. Gsw Rirhs Hwt orwh mligsdwhg lv Wmuotmx tmx gsw Ywogry Hwt orwh gl gsw hlfgsdwhg. Wmuotmx rh hwktitgwx viln ylmgrmwmgto Wfilkw zb gsw Mligs Hwt gl gsw wthg tmx gsw Wmuorhs Ystmmwo gl gsw hlfgs. Gsw ylfmgib ylewih vrew-wrusgsh lv gsw rhotmx lv Uiwtg Zirgtrm rm rgh ywmgiw tmx hlfgs; tmx rmyofxwh lewi ntmb ntmb hntoowi rhotmxh hfys th gsw Rhowh lv Hyroob, tmx gsw Rhow lv Drusg.

[10 marks]

b) Given an RSA Scheme with a public key of (N, e)=(391, 43). deduce the secret key and use it to decrypt the message (1174).

[13 marks]

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

IVEVYGARMLMYIVEKFDIVEFRL

[10 marks]

End of Paper