UNIVERSITY OF SOUTHAMPTON

SEMESTER 2 EXAMINATIONS 2017/18

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) Explain how encryption can be enhanced using compression techniques, indicating the best approach of combining the two techniques.

[5 marks]

(b) Encode the message M1 using a Rail Fence Cipher

M1= “Without perseverance talent is a barren bed”

[5 marks]

(c) Explain the functionality of the plug-board used in the Enigma machines, and then discuss how the number of pulgboard settings can be calculated, assuming it has 10 sockets and 4 cables.

[10 marks]

(d) Use cryptanalysis methods to crack the cipher below, explaining all working.

Lnsd gcavm aezfe itpts ts uhwle eniq

[13 marks]

Question 2

(a) Consider the following *Hash* function:
H: $\mathbf{\{0,1\}^{64} \rightarrow \{0,1\}^{8}}$

$X \in \mathbf{\{0,1\}^{64}}$, such $X= (x_0,x_1,\ldots,x_7)$, each x_i is a byte

$H(X)= (x_0+x_1+\ldots+x_7)$

Provide a possible pre-image of the hashed value of
H(X)= 00000000

[5 marks]

(b) Explain, using a numerical example, whether or not the above Hash function is collision resistant?

[5 marks]

(c) Explain, with the aid of an illustrative diagram, the working principles of a Hash function based on the Merkle-Damgard Scheme.

[5 marks]

(d) Alice and Bob wish to communicate over an insecure link and have agreed to use the AES encryption algorithm with a key length of 128 bits. However, they need to agree on a cryptographic mode of operation.
E_{CBC} , E_{CTR} are two possible implementations of the AES algorithm in the cipher block chaining and counter modes, respectively, in both cases assuming the standard AES block of 128 bits. Which of the above two modes do you recommend in order to reduce the number of times the key needs to be changed? Explain and justify your answer.
For your chosen mode, calculate, with full explanation, the maximum number of bits that can be transmitted over this link using the same encryption key such that the advantage of an adversary capable of carrying out a chosen plaintext attack does not exceed 2^{-40}. It is assumed that the advantage of the adversary over AES is 2^{-45} in the case of one time key use.

[18 marks]

TURN OVER

Question 3

Let E be the elliptic curve $y^2 = x^3 + 7x + 15$ 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 all pairs of points (P,Q) such that
P+Q= O

[10 marks]

(c) Alice and Bob are using the above elliptic curve to to agree on a shared secret using the Diffie–Hellman scheme with the following parameters: the generator element (1, 6), Alice's public key: (9,12). Bob's public key: (7, 2). What is their secret ? Explain your answer.

[10 marks]

(d) What is the maximum number of points that can be found in an elliptic curve group defined over the field $\mathbb{F}_{13} = \mathbb{Z}_{13}$? Explain your answer.

[8 marks]

Question 4

(a) Eve managed to intercept two of Alice‘s messages (m1=10197, m2=10317) with their respective RSA digital signatures RSA digital signatures (s1=24021, s2= 18336).
Assuming the following RSA parameters are public knowledge ((RSA modulus N=227429 and the exponent of e=113)
Would it be possible for Eve to forge Alice’s signature? Explain your answer with a numerical example.

[13 marks]

b) Explain the principles of the BB84 key distribution protocol.

[5 marks]

(c) Use cryptanalysis methods to crack the cipher below, explaining your working.

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

S HGFZB OSLLTNV UMD ZTNMHSFIH HLIXSZ SYIMHH GUX DMIPZ HUMDH GUXB OSB USEX KXXN S ETYGTO MW GUXTI MDN HFYYXHH. FQ IXHXSIYUXIH KXPTXEX GUXB DXIX SPIXSZB TN ZXYPTNX KXWMIX GUX QTPPXI SHGXIMTZ UTG KXYSFHX GUXB USZ MYYFLTXZ XEXIB USKTGSG MN XSIGU. WIMO GUXTI IMMGH TN HMFGU SOXITYS, GUX ZTNMHSFIH OTVISGXZ "TN S WIXNAB MW OMEXOXNG GM YMEXI GUX LPSNXG"

[10 marks]

(d) Using “big O” notation and assuming limited computing resources, estimate the following:

1. The time needed to factorize an integer number N=157929489 using the number field sieve algorithum.

2. The time needed to find a 256-bit AES encryption key k using Grover’ s algorithm running on a quantum computer.

[5 marks]

End of Paper