UNIVERSITY OF SOUTHAMPTON ELEC6242W1

SEMESTER 2 EXAMINATIONS 2015/16

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

Let E be the elliptic curve $y^2 = x^3 + 7x + 4$ over the field $\mathbb{F}_{17} = \mathbb{Z}_{17}$

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

(a) Find the order of this group

[8 marks]

(b) Find all the points P on E such that $2P = (\infty, \infty)$

[6 marks]

(c) Find an integer $i \geq 0$ such that $i(0,2) = (3,1)$ in E.

[11 marks]

(d) Why is the *Discrete Logarithm* problem interesting to cryptographers? Give an example of its use in constructing a *shared secret*.

[8 marks]

Question 2

(a) What is the difference between cryptography and Steganography? Give an example of a Stenographic method.

[6 marks]

(b) Encrypt the following message (M1) using a rail fence cipher with three rails.

M1 = “Only in the darkness can you see the stars”

[8 marks]

(c) Compression methods are typically used to prevent the use of data redundancy in cryptanalysis. Calculate the theoretical maximum compression ratio which can be achieved for the following message (M2):

M2 = 1111100111

[8 marks]

(d) Decrypt the following message and explain the technique which was used to encrypt it. (Tip: Ignore the spaces between letters).

v v o n g p r u e e i h e e p

[11 marks]

TURN OVER

Question 3

(a) Compute the following in Z_{23}

$$1) 5^{1/13} \qquad 2) \frac{6}{14} \qquad 3) 162^{111}$$

[8 marks]

(b) Illustrate by means of a circuit diagram the AES encryption Algorithm (the key size is assumed 128 bit)

[6 marks]

(c) Is it possible for an adversary to gain knowledge of the secret key by analysing the power consumption of an AES hardware core? Explain your answer

[8 marks]

(d) Alice had always wanted to establish a secure communication link with Bob, so when she won the lottery, she decided to hire Steve, a security expert to do this. Steve designed an AES encryption system(see figure 1) with a key size of 128 bit, where the plain text is divided into 128-bits data words, which are encrypted and transmitted individually.
Alice and Bob managed to agree secretly on a shared key, and then they started exchanging secret information ever after. Do you think Steve's encryption system is semantically secure? Explain your answer.

[11 marks]

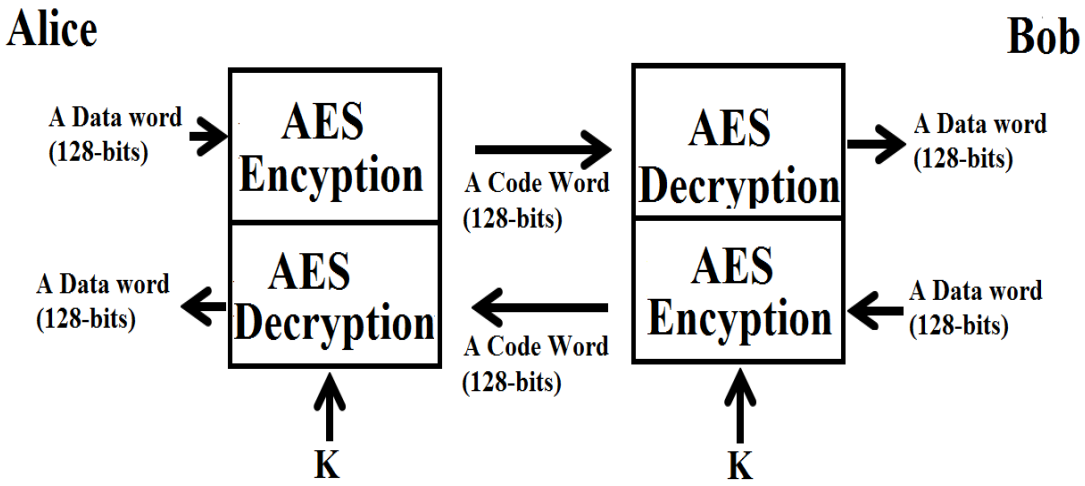

Figure 1: Steve's AES Encryption/Decryption Scheme

Question 4

Consider the following *Hash* function:

H: $\mathbf{\{0,1\}^{16} \rightarrow \{0,1\}^4}$

$X \in \mathbf{\{0,1\}^{16}}$, such $X= (x_0,x_1,x_2,x_3)$, each x_i is a half-byte

$H(X)= (x_0+x_1+x_2+x_3)$

(a) Name two possible pre-images of the hashed value of $H(X)= 0101$.

[6 marks]

(b) Explain whether or not the hash function described above is a suitable candidate for secure applications

[8 marks]

(c) Explain with the help of a functional diagram the message authentication scheme called ECBC-MAC.

[8 marks]

(d) Alice uses the RSA digital signature scheme to sign all her purchase order from Bob's company.
One day; Alice realised that Steve one of her most trusted employees had managed to forge her signature and make numerous purchase orders behind her back. His motives for such a morbid act remain unknown.
Alice also discovered that Bob already knows the scheme's parameters (RSA modulus N=693313 and the exponent of e=350209), and he also managed to steal at least the following two messages (m1=666, m2=69) and their respective RSA digital signatures (s1=315928, s2= 117027).
Explain by means of numerical examples how Steve could have forged Alice's signature.

[11 marks]

End of Paper