SEMESTER 2 FINAL ASSESSMENT 2020/2021

Cryptography

This paper contains THREE questions

Answer **ALL** Questions

5 page paper

Question 1

(a) Calculate the index of coincidence for the message M1 below.

M1= EB OT TON RO EB OT

[5 marks]

(b) Give an example of how you can use textual Steganography to hide the message (M2) below.

M2 = Go at two

[5 marks]

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

NOLRYPPZDAMLWERLJEGRCNOLRYPZZIQMOQKBPLNHAGOWLSRJPOLREGE

[10 marks]

(d) Compute the value of “x” for each of the equations below, and explain your workings in each case. Note that all operations are performed in $\mathbb{Z}_{23}$.

1) $\mathrm{x} = 22^8$ 2) $x = \sqrt{2}$ 3) $x = \frac{5}{17}$

[13 marks]

Question 2

Let E be the elliptic curve $y^2 = x^3 + x + 3$ 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, and explain whether or not this is a cyclic group.

[10 marks]

(b) Find an integer $i \geq 0$ such that :

$i(16,16) = (12, 14)$ in E

[8 marks]

(c) Alice has recieved the encypted message {C1, C2} from Bob, where:
C1= (16,16)
C2= 13
Decrypt Alice's message, assuming the Elgamal encyption algorithm with the above group (E) has been used to encrypt it. You are aslo given the following information:
Alice's secret key: a=6.

[10 marks]

(d) What is the minimum number of points that can be found on an an elliptic curve E curve over a finite field Z_{17}

[5 marks]

Questions continues on following page

Question 3

(a) Use cryptanalysis methods to deduce the plaintext from the message below.

ANMTYVAAHIYIOELDUFLE

[10 marks]

(b) 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.

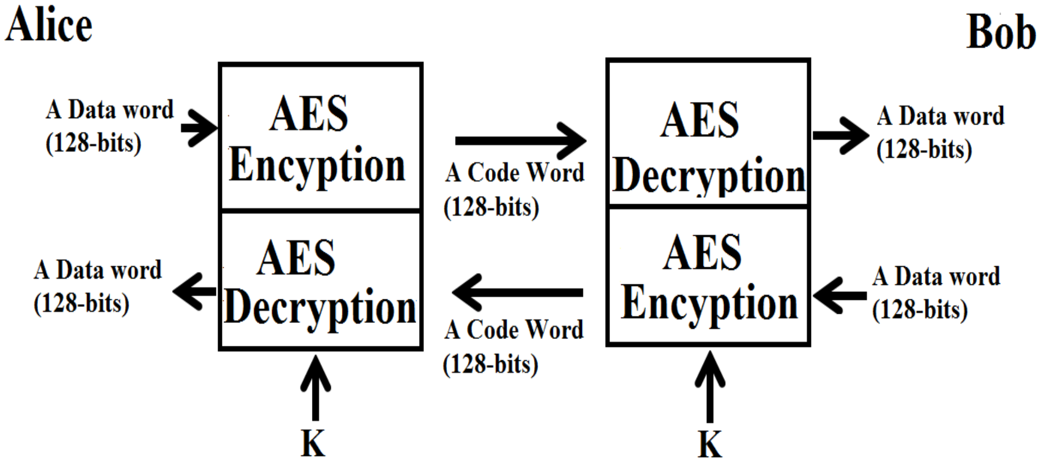

Figure 1

[5 marks]

Question continues on following page

(c) Read each of the following statements carefully, and explain whether or not it is correct.

1) The Kirchhoff principle was adhered to during the AES standard development process.
2) The development of the first quantum computer will render the current AES standard no longer secure.
3) The cipher block chaining (CBC) mode is always more immune to chosen plaintext attacks compared with the counter mode (CTR).
4) Elgamal encryption scheme can be considered a trap door function.
5) The adoption of computation perfect secrecy greatly reduces the vulnerability of cryptographic algorithms to timing attacks.
6) The order of an elliptic curve E defined over Z_P cannot exceed p.
7) The implementation of the BB84 quantum cryptography scheme will make it impossible for an adversary to eavesdrop on the communication channel without being detected.
8) The development of quantum computers will undermine the security of hash functions.
9) Given a room that has 60 people, the probability that at least two of them have been born on the same day and same month does not exceed than 80%.

[18 marks]

END OF PAPER