Calculators may be used in this examination provided they are not capable of being used to store alphabetical information other than hexadecimal numbers

UNIVERSITY OF
BIRMINGHAM

School of Computer Science

Cryptography

Main Summer Examinations 2019

Time allowed: 1:30

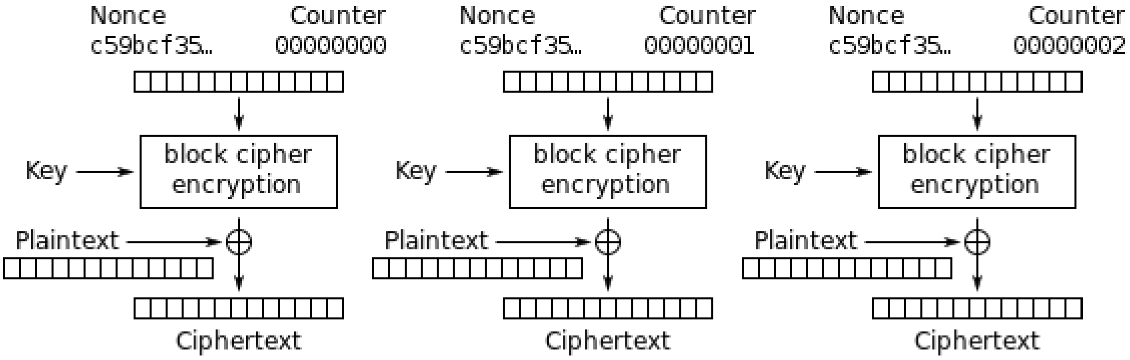
[Answer all questions]

Note

Answer ALL questions. Each question will be marked out of 20. The paper will be marked out of 60, which will be rescaled to a mark out of 100.

Question 1

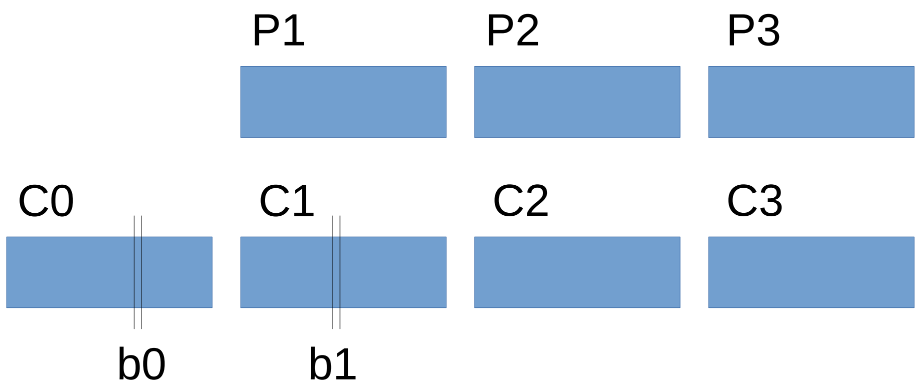
The diagram below shows the block cipher mode of operation known as counter (CTR) mode.



Counter (CTR) mode encryption

Question 1 continues over the page

The next diagram shows a plaintext consisting of three blocks, called P1, P2, P3. Each block consists of 128 bits. It is encrypted using AES in counter (CTR) mode. The resulting ciphertext has four blocks. C0 is the counter-mode nonce (64 bits) followed by the initial counter value (64 bits, all of them zero). C1, C2, C3 correspond to P1, P2, P3 respectively.



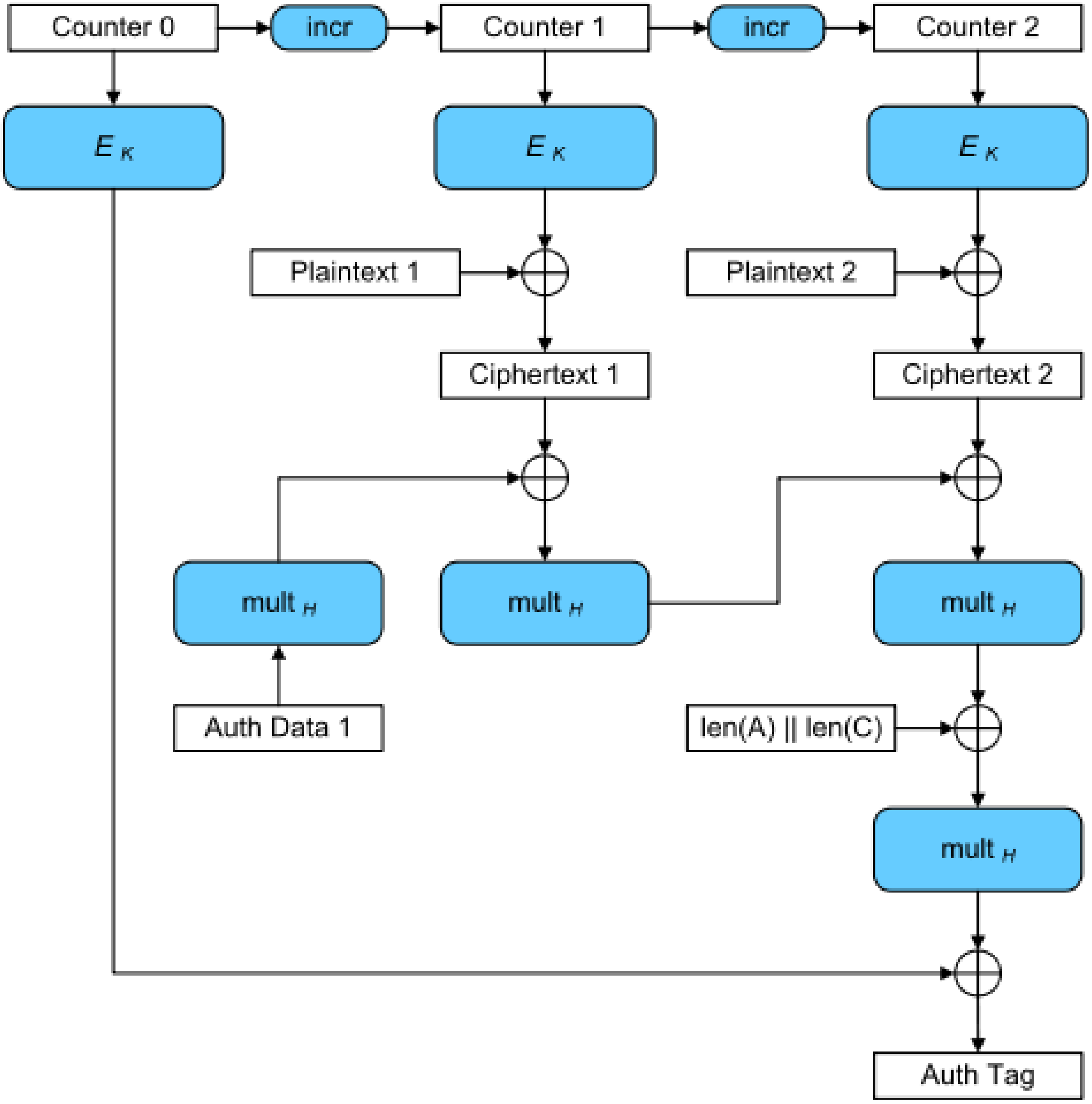
b0 is a certain bit in block C0 (let's say the 80th bit), and b1 is a certain bit in C1 (say the 60th bit). (Actually the values "80th" and "60th" are not important.)

(a) The four blocks of ciphertext are now transmitted to a receiver. However, a transmission error causes **bit b0** to be flipped. The receiver attempts to decrypt the blocks that have been received (with b0 flipped). Does the decryption process result in an error, or does the receiver obtain some putative plaintext blocks P1′, P2′, P3′? Which of these blocks are equal to the corresponding original plaintext blocks P1, P2, P3? Explain your answer. **[5 marks]**

(b) Starting again with the original four blocks C0, C1, C2, C3 of ciphertext, these blocks are once again transmitted to a receiver. However, this time a transmission error causes **bit b1** to be flipped. The receiver attempts to decrypt the blocks that have been received (with b1 flipped). Does the decryption process result in an error, or does the receiver obtain some putative plaintext blocks P1′, P2′, P3′? Which of these blocks are equal to the corresponding original plaintext blocks P1, P2, P3? Explain your answer. **[5 marks]**

Question 1 continues over the page

The diagram below (which was explained in lectures) shows the operation of Galois Counter Mode (GCM). Suppose Alice uses AES in GCM mode to encrypt two blocks of plaintext. In the diagram, they are called 'Plaintext 1' and 'Plaintext 2'. AES in GCM mode allows for the possibility of authenticated associated data, called 'Auth Data 1' in the diagram, but in this question we will assume there is no authenticated associated data. In the diagram, all the blocks are 128 bits in length. The block called 'Counter 0' consists of a nonce (64 bits), followed by the initial counter value (64 bits, all of them zero). 'Counter 1' consists of the same nonce (64 bits), followed by the integer 1 (63 bits of zero followed by a one), etc.



Question 1 continues over the page

(c) After encrypting ‘Plaintext 1’ and ‘Plaintext 2’, Alice wants to send the ciphertext to Bob, so he can authenticate and decrypt it. Using the names of the blocks given in the diagram, specify which blocks Alice needs to send. **[5 marks]**

(d) Explain what computation Bob needs to perform in order to authenticate the message (this is what he does before he decrypts it). **[5 marks]**

Question 2

(a) Explain why AES is generally considered better than 3DES. Also explain why there may be some circumstances in which 3DES is preferred today. **[5 marks]**

(b) Consider SHA-256, which is the hash function in the SHA-2 family that outputs a hash value of 256 bits. Why do we say that this hash function has at most 128 bits of security? **[5 marks]**

(c) In the context of RSA encryption, what is OAEP? What properties does OAEP enjoy over the basic RSA encryption scheme? **[5 marks]**

(d) Suppose a company wishes to allow its customers to verify that the software they download from the company website has not been modified in transit. Which one of the following two methods should be preferred to achieve that goal: a digital signature (such as an RSA signature) or a message authentication code (MAC)? Justify your answer. **[5 marks]**

Question 3

Let us consider the family of Discrete Logarithm based computational problems with parameters (G, p, q) for large primes p, q, where G has q elements and is a subgroup of $\mathbf{Z}_p^\star$. Let g be a generator of G.

(a) Consider the following variation of the Computational Diffie-Hellman problem that is called Square Computational Diffie-Hellman (2CDH) problem:

> The 2CDH problem consists of computing $g^{x^2} \bmod p$ given (G, p, q) and (g, g^x), where $x \in Z_q$. We write 2CDH$(g, g^x) := g^{x^2}$

Solve the 2CDH problem on input $(3, 4)$ for group parameters $(G, p, q) := (\langle 3 \rangle, 11, 5)$, where $\langle 3 \rangle$ stands for the subgroup of $\mathbf{Z}_{11}^\star$ generated by 3. Justify your answer. **[5 marks]**

(b) Assume that you have a very powerful calculator that solves the Computational Diffie-Hellman problem on inputs (g, g^x, g^y) for $x, y \in \mathbf{Z}_q$ with respect to parameters (G, p, q), and let us denote by CDH(g, g^x, g^y) the corresponding solution. Explain how to solve 2CDH(g, g^x) from a calculator that solves CDH(g, g^x, g^y). Use your answer to solve CDH$(3, 4, 4)$ for parameters $(G, p, q) := (\langle 3 \rangle, 11, 5)$? **[5 marks]**

(c) Given the triple (g, g^x, g^y), explain how to compute CDH(g, g^{2x}, g^{2y}) from a calculator that computes 2CDH. *(Hint: consider computing each of the solutions 2CDH(g, g^x), 2CDH(g, g^y) and 2CDH$(g, g^{(x+y)})$)*

[5 marks]

(d) Consider a group (G, p, q) where the 2CDH problem is conjectured to be infeasible to solve. Choose from the following claims those you think are true and explain your answer.

(i) The CDH problem is also conjectured to be infeasible to solve.

(ii) The respective computational hardness of the CDH and 2CDH problems are independent.

[5 marks]

This page intentionally left blank.

Do not complete the attendance slip, fill in the front of the answer book or turn over the question paper until you are told to do so

Important Reminders

- Coats/outwear should be placed in the designated area.
- Unauthorised materials (e.g. notes or Tippex) must be placed in the designated area.
- Check that you do not have any unauthorised materials with you (e.g. in your pockets, pencil case).
- Mobile phones and smart watches **must** be switched off and placed in the designated area or under your desk. They must not be left on your person or in your pockets.
- You are not permitted to use a mobile phone as a clock. If you have difficulty seeing a clock, please alert an Invigilator.
- You are not permitted to have writing on your hand, arm or other body part.
- Check that you do not have writing on your hand, arm or other body part – if you do, you must inform an Invigilator immediately
- Alert an Invigilator immediately if you find any unauthorised item upon you during the examination.

Any students found with non-permitted items upon their person during the examination, or who fail to comply with Examination rules may be subject to Student Conduct procedures.