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 2020

Time allowed: 1:30

[Answer all questions]

Turn Over

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 key schedule for AES-128 works as follows. Split the encryption key K into four words W_0, W_1, W_2 and W_3 of 32 bits each. Then compute W_j (for $4 \leq j \leq 43$) as follows:

for $i := 1$ **to** 10 **do**
$T := W_{4i-1} \lll 8$
$T :=$ SubBytes(T)
$T := T \oplus RC_i$
$W_{4i} := W_{4i-4} \oplus T$
$W_{4i+1} := W_{4i-3} \oplus W_{4i}$
$W_{4i+2} := W_{4i-2} \oplus W_{4i+1}$
$W_{4i+3} := W_{4i-1} \oplus W_{4i+2}$
end

Recall that, although there are 10 rounds in AES-128, we derive a total of 11 subkeys because an initial subkey is consumed before the rounds begin. The subkeys K_i (where $0 \leq i \leq 10$) are obtained as follows:

$$K_i = W_{4i}, W_{4i+1}, W_{4i+2}, W_{4i+3}.$$

To answer the questions below, you will need the following facts: SubBytes(0xFFFFFFFF)= 0x16161616; RC_1=0x01000000; 0x16$\oplus$0x01=0x17; 0x16$\oplus$0xFF=0xE9; 0x17$\oplus$0xFF=0xE8.

(a) Suppose the encryption key is all-ones (i.e., 128 bits of 1, or 0xFFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF in hexadecimal). What is the value of the initial subkey K_0? **[5 marks]**

(b) Compute the values of W_4 and W_5. Hence, write down the first half of the first round subkey K_1. **[5 marks]**

Parts (c) and (d) do not require any calculations to be done.

(c) Alice sends her stockbroker a daily instruction, which is either "*buy!*" or "*sell!*". For example, on the five days last week, the instructions were "*buy!*", "*buy!*", "*sell!*", "*buy!*", "*sell!*". She decides to encode "*buy!*" as the bitstring consisting of 128 zeros, and "*sell!*" as the bitstring consisting of 128 ones, and to encrypt this representation of the instruction using AES in ECB mode using a key she has previously agreed with her stockbroker. Explain why this arrangement is a poor way of ensuring confidentiality of Alice's instructions. **[5 marks]**

(d) Recommend to Alice a better way to achieve confidentiality of her instructions. **[5 marks]**

Question 2

(a) What is the *birthday paradox*? Explain why this is relevant for cryptographic hash functions. **[5 marks]**

(b) Why is DES considered insecure? **[5 marks]**

(c) Consider a network of N computers $C_1, \ldots, C_N$ that are accessible by their IP addresses. Describe how to set up pairwise confidential and authenticated communication channels in this network. You can use either symmetric key or asymmetric key cryptographic primitives, or both. (Pairwise means we want to secure the communication between each pair of computers in the network $\{C_1, \ldots, C_N\}$.) **[5 marks]**

(d) Define the existential unforgeability game for digital signature schemes. Name two schemes that are conjectured to be existentially unforgeable. **[5 marks]**

Question 3

Consider MElGamal, a variant of the ElGamal public key encryption (PKE) scheme, with encryption algorithm that only accepts plaintexts in $0, 1$. MElGamal is defined as follows:

- Key generation (λ)
  - Let q, p be primes wrt. security parameter λ such that $q|p-1$
  - Let $g \neq 1$ be such that $g^q = 1 \bmod p$
  - Let $\mathbf{G}$ be the subgroup of $\mathbf{Z}_p^\star$ generated by g
  - Let $x \xleftarrow{R} \mathbf{Z}_q$. Let $h = g^x \bmod p$
  - Public-key : $PK = (p, q, g, h)$. Private-key : $SK = x$
- Encryption ($PK, m \in \{0, 1\}$)
  - m must be a single bit (i.e. $m \in \{0, 1\}$).
  - Let $r \xleftarrow{R} \mathbf{Z}_q$
  - Output $c = (g^r \bmod p, h^r \cdot g^m \bmod p)$
- Decryption ($SK, C = (c_1, c_2)$)
  - ...

(a) Define the decryption algorithm of MElGamal. Show that MElGamal satisfies the completeness property for PKE schemes. **[5 marks]**

(b) Is MElGamal an IND-CPA secure scheme? Justify your answer. **[5 marks]**

(c) Let us define an operation $\otimes$ over MElGamal ciphertext as follows: $(c_1, c_2) \otimes (c_1', c_2') := (c_1 \cdot c_2 \bmod p, c_1' \cdot c_2' \bmod p)$. Show that for any $m, m' \in \{0, 1\}$ such that $m \neq m'$ holds that $\mathsf{Enc}(PK, m) \otimes \mathsf{Enc}(PK, m') = \mathsf{Enc}(PK, m \oplus m')$, where $\oplus$ is the XOR operation. **[5 marks]**

(d) Is MElGamal non-malleable? Justify your answer. **[5 marks]**

End of Paper

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.