Module: Modern Cryptography
Exam: Summer 2024
Lecturer: Dr. Martin Harrigan

Instructions:

- Answer any four questions.
- You have 2.5 hours to complete the exam.
- The exam is worth 50% of your final grade.

Question 1 **(20 marks)**

(a) Consider a Feistel scheme with 8-bit blocks and two rounds. The round function for round i is $f_i(x, K) = x \oplus K_i$ where x is the input to the round, K_1 and K_2 are the first and the last four bits of the main key K respectively, and $\oplus$ is the XOR operation. If the plaintext is `01010101` and the key is `00001111`, what is the ciphertext?

(8 marks)

(b) Draw a diagram that illustrates the Cipher Block Chaining (CBC) mode of operation for decryption. Your diagram should show the flow of data from the plaintext blocks to the decryption processes, and to the ciphertext blocks.

(8 marks)

(c) Padding expands a message to fill a complete block by adding extra bytes to the end of the message. Assuming a 16-byte block, describe what gets added to a message by the popular padding scheme PKCS#7 when:

(i) there is one byte of data leftover;

(ii) there are two bytes of data leftover;

(iii) there are fifteen bytes of data leftover; and

(iv) there are no bytes of data leftover, i.e., the length of the message is a multiple of sixteen.

(4 marks)

Question 2 **(20 marks)**

(a) AES uses a substitution-permutation network with a number of rounds that depends on the size of the key. Draw a sketch of the network when the key is 256-bits. Your sketch should include the number of rounds, the `SubBytes`, `ShiftRows`, `MixColumns` and `AddRoundKey` functions as they occur in the first and last rounds, the `KeyExpansion` function, and the flow of data from a key and plaintext block to a ciphertext block.

(6 marks)

(b) The key schedule for AES, `KeyExpansion`, derives the round keys from the main key. Is it possible to recover the main key from a round key?

(4 marks)

(c) Fast implementations of AES use *table-based implementations* and/or *native instructions.* Briefly describe one of these optimisations.

(6 marks)

(d) What are the practical implications of choosing between AES key sizes in terms of encryption strength and computational efficiency. Specifically, address how the increase in key size from 128 bits to 256 bits impacts the resistance of AES to brute-force attacks.

(4 marks)

Question 3 **(20 marks)**

Python's `cryptography` package provides many cryptographic primitives such as block ciphers, stream ciphers, hashing functions, keyed-hashing functions, etc. All of the following code snippets, except the last one, using functionality from this package.

(a) In the following code snippet, what is the purpose of the `length`, `n`, `r` and `p` arguments? In what circumstances would they need to be changed?

```
import os
from cryptography.hazmat.primitives.kdf.scrypt import Scrypt

salt = os.urandom(16)
kdf = Scrypt(salt=salt, length=32, n=2**14, r=8, p=1)
```

(4 marks)

(b) The following code snippet signs a message (`message`) using a private-key (`private_key`). Why are there two references to a hash function (`hashes.SHA256()`)?

```
  from cryptography.hazmat.primitives import hashes
  from cryptography.hazmat.primitives.asymmetric import padding

  # [snip]

  signature = private_key.sign(
    message,
    padding.PSS(
      mgf=padding.MGF1(hashes.SHA256()),
      salt_length=padding.PSS.MAX_LENGTH
    ),
   hashes.SHA256()
  )
)
```

(4 marks)

(c) In the following code snippet, is the value generated by `os.urandom(16)` cryptographically random? Is it appropriate to use this value as a nonce for AES in CTR mode, or should we take the narrower definition of a nonce, and keep track of all values we used in the past?

```
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms,
    modes
import os

# [snip]

nonce_bytes = os.urandom(16)

aes_ctr_cipher = Cipher(algorithms.AES(key_bytes),
                        mode=modes.CTR(nonce_bytes))
```

(4 marks)

(d) When experimenting with the implementation of the AES block cipher provided by `cryptography/hazmat/primitives/ciphers/algorithms.py`, we used two datasets provided by the National Institute of Standards and Technology (NIST): Known Answer Tests (KATs) and Multiblock Message Tests (MMTs). What is the primary difference between KATs and MMTs? What type of implementation error could be identified by MMTs but not by KATs?

(4 marks)

(e) What cryptographic primitive is being implemented by the following code snippet?

```
def encrypt_decrypt(input, key):
  output = bytearray()
  for (b, c) in zip(input, key):
    output.append(b ^ c)
  return bytes(output)
```

(4 marks)

Question 4 (20 marks)

(a) What is meant by the terms *attack model*, *security goal* and *security notion*?

(6 marks)

(b) Suppose you are required to design a web portal to allow students to upload photographs of their medical certificates. State an appropriate security goal and list any three aspects of your attack model.

(5 marks)

(c) Explain Kerckhoffs's Principle.

(3 marks)

(d) In the context of black-box attack models, what can an attacker do in each of the following attack models:

(i) Ciphertext-only attack (COA)
(ii) Known-plaintext attack (KPA)
(iii) Chosen-plaintext attack (CPA)
(iv) Chosen-ciphertext attack (CCA)

(6 marks)

Question 5 **(20 marks)**

(a) In 2017, researchers from CWI Amsterdam and Google Research published two different PDF files that, when hashed using the SHA-1 algorithm, produce the same 160-bit hash. What property of hash functions did this attack break for SHA-1?

(2 marks)

(b) Name two popular hash functions that are considered secure as of today.

(3 marks)

(c) A Merkle tree is a tree where every leaf node contains the hash of a piece of data. What does every non-leaf node contain?

(3 marks)

(d) Draw and annotate the structure of a Merkle tree that fulfils the following criteria:

(i) The tree is binary, i.e., every non-leaf node has two children.
(ii) The tree has sixteen leaf nodes, i.e., it can store the hashes of at most sixteen pieces of data.
(iii) The root node and any one of the leaf nodes are highlighted.

(6 marks)

(e) Using your answer from (d), describe a Merkle proof that your tree with the highlighted root contains the highlighted leaf node. How many nodes will the Merkle proof require? Identify the nodes that will be part of the Merkle proof.

(6 marks)