UNIVERSITY OF BRISTOL

JANUARY 2016 Examination Period

FACULTY OF ENGINEERING

Examination for the Degree of
Bachelor and Master of Engineering and Bachelor and Master of Science

COMS-30002(J)
CRYPTOGRAPHY A

TIME ALLOWED:
2 Hours

This paper contains *four* questions.
All answers will be used for assessment.
The maximum for this paper is *60 marks*.

Other Instructions:

1. Calculators must have the Faculty of Engineering Seal of Approval.

TURN OVER ONLY WHEN TOLD TO START WRITING

Q1. For each of the following statements decide whether it is true or false, and write down the correct answer in the exam book. Provide a short justification for each answer.

(a) Perfect secrecy of the One-Time Pad implies that the key can be reused securely.

[3 marks]

(b) CTR mode using AES-128 is IND-CCA secure.

[3 marks]

(c) A single round of the Feistel construction does not suffice for a secure blockcipher.

[3 marks]

(d) For a *deterministic* public key encryption scheme, OW-CCA security does not imply OW-CPA security.

[3 marks]

(e) Cryptology is not used in practice.

[3 marks]

Q2. This question focuses on a variant of the RSA cryptosystem.

Key generation Kg selects three random yet distinct 767-bit prime numbers p', q', and r' such that $p \leftarrow 2p' + 1, q \leftarrow 2q' + 1$, and $r \leftarrow 2r' + 1$ are all prime as well. Let $N \leftarrow p \cdot q \cdot r$. Set $e \leftarrow 3$ and set d to the smallest positive integer such that the least common multiple $\text{lcm}(p-1, q-1, r-1)$ divides $d \cdot e - 1$. Publish (N, e) as the public key pk and keep (N, d) as the private key sk.

Encryption Enc takes as input the public key $\mathsf{pk} = (N, e)$ and a message $\mathsf{m} \in \mathbb{Z}_N$. It computes and returns ciphertext $\mathsf{c} \leftarrow \mathsf{m}^e \bmod N$.

Decryption Dec takes as input a private key $\mathsf{sk} = (N, d)$ and a ciphertext $\mathsf{c} \in \mathbb{Z}_N$. It computes and returns $\mathsf{m}' \leftarrow \mathsf{c}^d \bmod N$.

(a) Prove correctness of the scheme.

[5 marks]

(b) Discuss the strengths and weaknesses of the encryption scheme. Mention at least three distinct ones (strengths and weaknesses combined). Illustrate with attacks where appropriate (no reductions are required).

[5 marks]

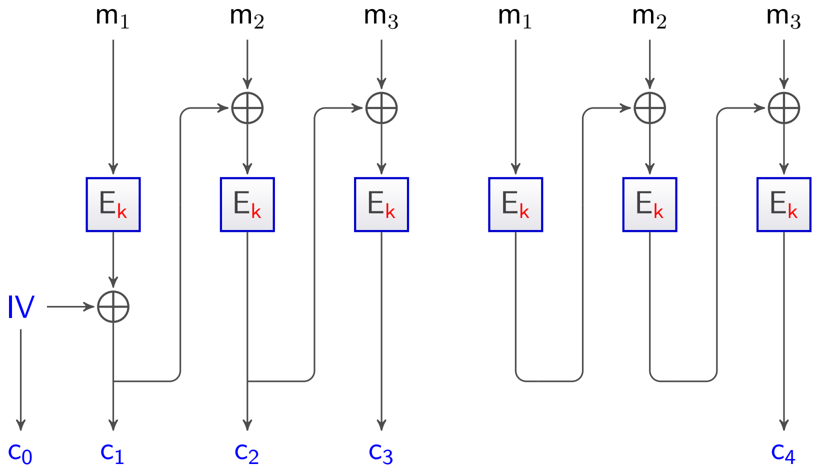
(c) Describe how you would build an EUF-CMA signature scheme related to this encryption scheme by specifying the relevant algorithms for key generation, signing, and verification.

[3 marks]

(d) Under what assumption(s) would your signature scheme be EUF-CMA secure (no reduction required)?

[2 marks]

Q3. This question asks you to evaluate the security of an authenticated encryption scheme. The scheme is based on combining CBC-style encryption and authentication, both based on DES. Let E denote the encryption algorithm of the DES blockcipher. For key generation, generate a single DES key k that will be used throughout. To encrypt a three block message $(\mathsf{m}_1, \mathsf{m}_2, \mathsf{m}_3)$, generate a random initial vector IV and output the ciphertext $(\mathsf{c}_0, \ldots, \mathsf{c}_4)$ with the computation according to the diagram below. Here the final block of ciphertext c_4 is used as an authentication tag. The scheme generalizes to messages of an arbitrary number of blocks in the natural way.



(a) Describe what decryption would look like for this scheme. Base your decryption algorithm on ciphertexts corresponding to 3-block messages (as above).

[3 marks]

(b) Point out as many dubious design decisions of the scheme as you can. For each shortcoming, you should identify as clearly as possible which part of the scheme you are referring to, explain how and why security (or efficiency) suffers by presenting attacks (or referring to taught material), and suggest a remedy. You can obtain up to four points per shortcoming.

[12 marks]

Q4. This question addresses an ElGamal-like cryptosystem. Assume G_q is a given group of (known) prime order q with public generator g. Consider the following algorithms defining key generation and encryption of the EGL cryptosystem.

Key generation Kg randomly generates a second generator f and selects two exponents x_1 and x_2 uniformly at random from $\mathbb{Z}_q$. Compute $y \leftarrow f^{x_1} g^{x_2}$. The public key comprises $\mathsf{pk} = (f, y)$ and the private key $\mathsf{sk} = (x_1, x_2)$.

Encryption Enc takes as input a public key $\mathsf{pk} = (f, y)$ and a message $m \in \mathsf{G}_q$. It randomly selects $r \in \mathbb{Z}_q$ and computes $c_1 \leftarrow f^r, c_2 \leftarrow g^r$ and $c_3 \leftarrow m \cdot y^r$. The ciphertext is (c_1, c_2, c_3).

(a) Describe a suitable decryption algorithm for the EGL cryptosystem.

[3 marks]

(b) Show that the EGL cryptosystem is homomorphic.

[2 marks]

(c) Under an appropriate assumption, either show that the EGL cryptosystem is OW-CPA or IND-CPA secure (your choice; both are possible). Clearly describe both the security notion and the assumption and explain how you set up your reduction, before fleshing out the details.

[10 marks]

END OF PAPER