UNIVERSITY OF BRISTOL

JANUARY 2015 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 in the exam book the correct answer. Provide a short justification for each answer.

(a) The One-Time Pad is malleable.

[3 marks]

(b) CBC mode is OW-CCA secure.

[3 marks]

(c) Any probabilistic symmetric key encryption scheme is IND-CPA secure.

[3 marks]

(d) A deterministic symmetric key encryption scheme cannot be OW-CCA secure.

[3 marks]

(e) A homomorphic public key encryption scheme cannot be OW-CCA secure.

[3 marks]

Q2. This question focuses on the relationship between symmetric and public key primitives.

Let $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be a public key encryption scheme. Consider the symmetric key encryption scheme $(\mathsf{Kg}', \mathsf{Enc}', \mathsf{Dec}')$ that works as follows:

Key generation Kg' runs $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{Kg}$ and returns the pair $(\mathsf{pk}, \mathsf{sk})$ as the symmetric key k.

Encryption Enc' takes as input the symmetric key $\mathsf{k} = (\mathsf{pk}, \mathsf{sk})$ and a message m and returns $\mathsf{Enc}_{\mathsf{pk}}(\mathsf{m})$.

Decryption Dec' takes as input the symmetric key $\mathsf{k} = (\mathsf{pk}, \mathsf{sk})$ and a ciphertext c and returns $\mathsf{Dec}_{\mathsf{sk}}(c)$.

(a) Describe the IND-CCA security notion for symmetric encryption schemes.

[3 marks]

(b) Which oracle is missing from the IND-CCA security notion of public key schemes and why?

[2 marks]

(c) Prove that if the public key scheme $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ is IND-CCA secure, then so is the resulting symmetric scheme $(\mathsf{Kg}', \mathsf{Enc}', \mathsf{Dec}')$.

[5 marks]

(d) Show that if for some public key scheme $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$, the resulting symmetric scheme $(\mathsf{Kg}', \mathsf{Enc}', \mathsf{Dec}')$ is IND-CCA secure, this does not imply that the original public key scheme is IND-CCA secure.

[5 marks]

Q3. This question focuses on signature schemes and the related use of hash functions.

(a) Give the generic syntax of a signature scheme (in the standard model) by describing which algorithms are involved and what their general input/output behaviour is. Also include the appropriate correctness requirement.

[4 marks]

(b) Describe the security model which should be satisfied by an EUF-CMA secure scheme in the standard model by giving a diagram depicting the relevant security game together with an informal explanation (in words).

[3 marks]

(c) The hash-then-sign paradigm can be used to extend the domain of a signature scheme. Given a signature scheme with domain $\{0,1\}^n$ and an arbitrary hash function $H : \{0,1\}^{2n} \to \{0,1\}^n$, the corresponding hash-then-sign signature scheme can sign messages in $\{0,1\}^{2n}$. Describe how the hash-then-sign scheme works by specifying the relevant algorithms.

[3 marks]

(d) Consider the hash function $H : \{0,1\}^{2n} \to \{0,1\}^n$ defined by $H(x_0||x_1) = x_0 \oplus x_1$ (that is, the input to H is split in two equal parts that are subsequently xored together). Evaluate the security of the resulting hash-then-sign scheme.

[5 marks]

Q4. This question addresses a cryptosystem using ideas from both RSA and ElGamal.

Key generation Kg randomly generates distinct primes p', q' such that $p \leftarrow 2p' + 1$ and $q \leftarrow 2q' + 1$ are prime as well. Set $N \leftarrow pq$ and let Q_N denote the group of quadratic residues modulo N, thus $z \in Q_N$ iff $z \in \mathbb{Z}_N{}^*$ and there exists a $w \in \mathbb{Z}_N{}^*$ such that $z = w^2 \bmod N$. Pick a generator g of Q_N; both g and Q_N have order $p'q'$. Select private exponent $x \in \mathbb{Z}_q$ and compute $y \leftarrow g^x \bmod N$. The public key comprises $\mathsf{pk} = (g, y, N)$ and the private key $\mathsf{sk} = (x, p', q')$.

Encryption Enc takes as input a public key $\mathsf{pk} = (g, y, N)$ and a message $m \in Q_N$. It randomly selects $r \in \mathbb{Z}_{N^2}$ and computes $c_1 \leftarrow g^r \bmod N$ and $c_2 \leftarrow m \cdot y^r \bmod N$. The ciphertext is (c_1, c_2).

Decryption Dec takes as input a private key $\mathsf{sk} = (x, p', q')$ and a ciphertext (c_1, c_2). It computes and returns $m' \leftarrow c_2 \cdot c_1^{p'q'-x} \bmod N$.

(a) Prove correctness of the cryptosystem as described above.

[5 marks]

(b) Give a detailed explanation how to exploit the Chinese Remainder Theorem for efficient decryption. How could you store the private key redundantly to facilitate this speed up?

[5 marks]

(c) Using your knowledge of both the RSA and the ElGamal cryptosystems, argue about the (in)security of the RSA-ElGamal cryptosystem. Make at least one positive and one negative observation.

[5 marks]

END OF PAPER