UNIVERSITY OF BRISTOL

JANUARY 2014 Examination Period

FACULTY OF ENGINEERING

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

COMS30002J
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. This question focuses on the Damgård ElGamal encryption scheme, which is a variation on the original ElGamal scheme. The scheme is defined as follows:

Key generation Kg generates a cyclic group G_q of prime order q with generator g. A private decryption key sk consists of two elements $x, \omega \in \mathbb{Z}_q$ both sampled independently and uniformly at random. The public key consists of the group description (G_q, q, g) together with the group elements $h \leftarrow g^{\omega}$ and $y \leftarrow g^{x}$.

Encryption Enc takes as input a public key pk and a message $\mathsf{m} \in \mathsf{G}_q$, uniformly at random selects r from $\mathbb{Z}_q$ and computes the ciphertext $c \leftarrow (g^r, h^r, m \cdot y^r)$.

Decryption Dec takes as input a private key sk and a ciphertext $c = (c_1, c_2, c_3)$. It checks whether $c_1^{\omega} = c_2$ and if and only if this is the case, it returns $m' \leftarrow c_3 c_1^{-x}$.

(a) Prove the correctness of the scheme.

[4 marks]

(b) The scheme is malleable. Explain what malleability means in general, demonstrate the malleability of this scheme, and comment on the implications in terms of security.

[4 marks]

(c) This scheme is derived from ElGamal. Explain how Damgård ElGamal differs from ElGamal.

[4 marks]

(d) ElGamal itself can be shown to be IND-CPA secure under the DDH assumption. Give the definition of IND-CPA security.

[3 marks]

(e) Prove that if ElGamal is IND-CPA secure, then so is Damgård ElGamal.

[5 marks]

Q2. This question focuses on building a message authentication code from an authenticated encryption scheme. To this end, let $(\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ be an authenticated encryption scheme and consider the MAC scheme $(\mathsf{Kg}, \mathsf{Tag}, \mathsf{Vrfy})$ where key generation Kg for the MAC scheme is exactly the same as that of the authenticated encryption scheme, and

Tagging Tag takes as input a key k and a message m. It computes $\tau \leftarrow \mathsf{Enc}(\mathsf{k}, \mathsf{m})$.

Verification Vrfy takes as input a k, a message m, and a tag τ. It computes $\mathsf{m}' \leftarrow \mathsf{Dec}(\mathsf{k}, \tau)$ and accepts iff $\mathsf{m}' = \mathsf{m}$.

(a) Prove the correctness of the MAC scheme, assuming correctness of the authenticated encryption scheme.

[2 marks]

(b) Comment on the efficiency and tag size of the MAC scheme.

[2 marks]

(c) Katz and Lindell gave three principles of modern cryptology. Name these principles (no explanation needed) and identify each of these principles in the statement:

The MAC scheme is existentially unforgeable under chosen message attacks (EUF-CMA secure) if the underlying authenticated encryption scheme satifies integrity of ciphertext (INT-CTXT secure).

[4 marks]

(d) Give the definition of EUF-CMA security for a MAC scheme.

[3 marks]

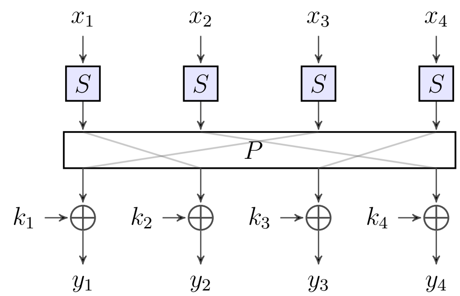
(e) Compare the definition of INT-CTXT security for a symmetric encryption scheme with that of EUF-CMA security for MACs: what are the differences and what are the similarities?

[5 marks]

(f) Consider the MAC scheme as described above, but where the verification routine is changed as follows: Vrfy' takes as input a k, a message m, and a tag τ. It computes $\mathsf{m}' \leftarrow \mathsf{Dec}(\mathsf{k}, \tau)$ and accepts iff $\mathsf{m}' \neq \perp$. How does this modification affect security? Argue your answer.

[3 marks]

Q3. This question focuses on substitution-permutation networks. These are commonly used to build blockciphers. A blockcipher typically consists of several rounds of an SP network, with S and P fixed and the various round keys generated from the master key using some key schedule. Below is an illustration of a single round of an SP-network.



(a) What is a blockcipher and what is meant by its block-length? *[2 marks]*

(b) Explain Kerckhoffs's principle in terms of a blockcipher built from an SP-network. What are the implications on the block-length and the key-length when a security level of 128-bit is desired (assuming a single round-key uniquely determines the overall blockcipher key)? *[3 marks]*

(c) One round (as depicted above) is insufficient as a blockcipher. Give an attack that is strong yet efficient, and describe what kind of attack it is. *[3 marks]*

(d) Why is omitting the S-boxes (from a multi-round SP-network) a bad idea? *[3 marks]*

Q4. This question focuses on a family of RSA-inspired signature schemes, defined as follows:

Key generation Kg selects 1023-bit prime numbers p' and q' such that $p \leftarrow 2p' + 1$ and $q \leftarrow 2q' + 1$ are both prime as well. Let $N \leftarrow pq$. Denote with Q_N the group of quadratic residues modulo N, that is $x \in Q_N$ iff $x \in \mathbb{Z}_N^*$ and there is some $y \in \mathbb{Z}_n$ such that $x \equiv y^2 \bmod N$. Key generation also selects a function f from the message space into Q_N (how this function is selected is immaterial to this question). The public key consists of N and the function f; the private key is (p', q').

Signing Sign takes as input a private key and a message m. It computes $y \in Q_N$ and e some 128-bit prime number such that $y^e = f(\mathsf{m}) \bmod N$. The signature is the pair (y, e).

Verification Vrfy takes as input a public key $\mathsf{pk} = (N, f)$, a message m, and a purported signature (y, e). It accepts iff $y^e = f(\mathsf{m}) \bmod N$.

(a) Show how to implement the signing algorithm, i.e. describe an efficient algorithm to compute the signature (y, e) using knowledge of the private key. You may assume an efficient routine $\mathrm{GenPrime}$ that on input ℓ outputs a random prime of length ℓ. *[4 marks]*

(b) Argue why your algorithm is efficient. *[3 marks]*

(c) Argue why your algorithm is correct, namely that the signatures that are generated will pass verification. *[3 marks]*

END OF PAPER