UNIVERSITY OF BRISTOL

JANUARY 2018 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 *three* questions.
All answers will be used for assessment.
The maximum for this paper is *50 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 questions below, four possible answers are presented. Select *all* the answers that you believe apply, or write "none" if you believe none apply. You do not need to justify your answer.

For each question, you can receive up to 3 points, with 3 points only for the perfect answer and one point deducted per incorrect classification, to a minimum of 0 points per question (e.g. if the correct answer is "A and B" then answering "B" leads to 2 points, whereas answering "B and C" only leads to 1 point).

[15 marks]

(a) Which of the following modes most closely mirrors the one-time pad?

A. CTR
B. CBC
C. CFB
D. OFB

(b) Which of the following statements is accurate?

A. AES is an SP Network
B. AES is a Feistel cipher
C. AES is an iterated cipher
D. AES uses key-whitening

(c) In the sentences below, "harder than" should be interpreted as "known to be equally hard as or strictly harder than".

A. Solving the DDH problem is harder than solving DLP
B. Solving the DDH problem is harder than solving the CDH problem
C. Solving the CDH problem is harder than solving DLP
D. Solving DLP is harder than solving the DDH problem.

(d) Which of the following schemes are homomorphic?

A. Vanilla ElGamal
B. Vanilla RSA Encryption
C. RSA-OAEP
D. Hybrid ElGamal

(e) The Chinese Remainder Theorem is commonly used to speed up

A. RSA encryption
B. RSA decryption
C. ElGamal encryption
D. ElGamal decryption

Q2. The one-time pad can be proven to be perfectly secret.

(a) Describe the three algorithms Kg, Enc, and Dec of the one-time pad.

[3 marks]

(b) Give the definition of perfect secrecy as a formal, probabilistic statement and describe in words what that statement intuitively captures.

[3 marks]

(c) There is an equivalent formalisation of perfect secrecy. Provide that statement and its intuitive meaning.

[2 marks]

(d) The one-time pad is seldom used directly and on its own in practice, say for secure e-mail. Why is this?

[5 marks]

(e) Imagine that one would create OTP-MAC in a similar way to CBC-MAC, by encrypting a message of arbitrary length and outputting the final 128 bits (padded with zeroes if needed) as the tag. Why is this OTP-MAC a bad idea?

[2 marks]

Q3. Schnorr signatures are a way of creating signature scheme based on the discrete logarithm problem in Schnorr subgroups of $\mathbb{Z}_p^*$. Key generation and signing work as follows.

Key generation Kg Selects random 2048-bit p and 256-bit q prime numbers such that q divides $p-1$. It selects a random element $g \in \mathbb{Z}_p^*$ of order q. Let $\mathsf{G}_q \subseteq \mathbb{Z}_p^*$ be the group of order q generated by g and let $\mathsf{H} : \mathsf{G}_q \times \{0,1\}^* \to \mathbb{Z}_q$ be a hash function.

Finally, it selects a random exponent $x \in \mathbb{Z}_q$ and sets $h \leftarrow g^x \bmod p$. Publish (p, q, g, h, H) as the verification key vk and keep (p, q, g, x, H) as the private signing key sk.

Signing Sign Takes as input the private signing key $\mathsf{sk} = (p, q, g, x, \mathsf{H})$ and a message $m \in \{0,1\}^*$. It selects a random element $w \in \mathbb{Z}_q$ and sets $a \leftarrow g^w \bmod p$ followed by $c \leftarrow \mathsf{H}(a, m)$. Set $r \leftarrow w - cx \bmod q$. Return (c, r) as the signature on m.

With a suitable verification algorithm, Schnorr signatures can be proven secure—for some relevant notion of security—in the random oracle model based on the discrete logarithm problem.

(a) State the discrete logarithm problem.

[2 marks]

(b) Describe and motivate a relevant security notion for signature schemes.

[6 marks]

(c) In the security reduction, what component of the signature scheme would be modelled by the random oracle?

[1 mark]

(d) Describe a suitable verification algorithm (hint: recompute a).

[3 marks]

For a chosen-prefix preimage attack against the hash function H, an adversary is given a target digest $z \in \mathbb{Z}_q$ and target prefix $a \in \mathsf{G}_q$, and has to find an m such that $z = \mathsf{H}(a, m)$.

(e) Prove that if H is collision resistant, then it is also resistant against chosen-prefix preimage attacks.

[4 marks]

(f) Show how susceptibility of H against chosen-prefix preimage attacks leads to a vulnerability against the signature scheme; name the attack against the signature scheme as precisely as possible.

[4 marks]

END OF PAPER