UNIVERSITY OF BRISTOL

January 2020 Examination Period

FACULTY OF ENGINEERING

Third Year Examination for the Degrees of
Bachelor of Science and Master of Engineering

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 50 marks.

PLEASE WRITE YOUR 7 DIGIT STUDENT NUMBER (NOT CANDIDATE NUMBER) ON THE ANSWER BOOKLET. YOUR STUDENT NUMBER CAN BE FOUND ON YOUR UCARD

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. Zero or more of these answers are correct. Select all the answers that you believe apply, or write ”none” if you believe none apply. You do not need to justify your answer.

Each question carries 3 marks. You lose one mark for each incorrect classification, down to a minimum of 0 marks per question. (For example, if the correct answer is ”A and B”, then answering ”B”, or ”none” leads to 2 points, whereas answering ”B and C” only leads to 1 point.) No marks will be awarded for questions to which you give no answer, so do make sure to write ”none” in case you believe none of the proposed answers apply.

(a) Which of these statements apply to the one-time pad?

A. The one-time pad provides perfect secrecy.

B. The one-time pad is not secure if keys are reused.

C. The one-time pad is always secure, however it is used.

D. The one-time pad is secure even when there are more messages than possible keys.

[3 marks]

(b) Which of these statements apply to Encrypt-then-MAC?

A. Encrypt-then-MAC is a blockcipher construction.

B. One needs to be careful to include both the nonce and ciphertext in the MAC computation.

C. If Encrypt is IND-secure and MAC is EUF-CMA-secure, then Encrypt-then-MAC is AE secure.

D. If Encrypt is IND-secure and MAC is EUF-CMA-secure, then Encrypt-then-MAC is IND-CCA secure.

[3 marks]

(c) Which of the following statements most accurately reflect the threat quantum computers pose to modern cryptography?

A. Grover’s algorithm allows a quantum computer to factor or compute discrete logarithms in time polynomial in the bitsize of the input.

B. Grover’s quantum search algorithm speeds exhaustive search attacks on symmetric cryptography from $\mathcal{O}(N)$ to $\mathcal{O}(\sqrt{N})$.

C. Grover’s and Shor’s algorithms are known to be the only possible threats that would arise from a scalable quantum computer.

D. Shor’s period-finding algorithm allows a quantum computer to factor or compute discrete logarithms in time polynomial in the bitsize of the input.

[3 marks]

(d) For which of the following choices for $f(x) \in \mathbb{Z}/3\mathbb{Z}[x]$ is $(\mathbb{Z}/3\mathbb{Z})[x]/(f(x))$ a field?

A. $f(x) = x^2 + 1$.

B. $f(x) = x^4 + 2 * x^2 + 1$.

C. $f(x) = x^2 - 1$.

D. $f(x) = x^3 + x + 1$.

[3 marks]

(e) If you are trying to solve a discrete logarithm problem in a large prime-order subgroup of a finite field $\mathbb{F}_p$, which of the following algorithms are likely to be most efficient (disregarding memory concerns)?

A. Index calculus

B. Pollard-rho

C. Baby-step-giant-step

D. Pohlig-Hellman

[3 marks]

Q2. In this question, we will consider a candidate authenticated encryption scheme, shown below, where E_K is a blockcipher that we assume is IND-secure. We only define this scheme for messages whose length is exactly three times the block length ℓ of the underlying blockcipher.

```
$\mathsf{Enc}_K^N(M = M[1] \| M[2] \| M[3])$
$C[0] \leftarrow N$
for $i \in [1, \ldots, 3]$
    $X[i] \leftarrow \mathsf{E}_K(C[i-1])$
    $C[i] \leftarrow M[i] \oplus X[i]$
$K' \leftarrow \mathsf{E}_K(N)$
$T \leftarrow C[n] \oplus K'$
return $(C[1] \| C[2] \| C[3], T)$
```

(a) Which mode of operation is the blockcipher being used in?

[2 marks]

(b) Describe, draw or define the decryption oracle, taking care to process as little unverified data as possible.

[3 marks]

(c) We would like to prove that our candidate scheme is a secure authenticated encryption scheme. This first requires us to prove that the scheme is a secure (nonce-based) encryption scheme. Define an adversary's advantage in breaking a scheme's indistinguishability. This must include a description (in words, diagram or code) of an experiment.

[3 marks]

(d) Our candidate scheme does not provide (nonce-based) indistinguishability. Name (or describe) a weaker indistinguishability notion that is likely to hold on our candidate scheme. Give a rough argument explaining why you believe this weaker notion applies to our scheme.

[3 marks]

(e) Does the scheme provide ciphertext integrity? If yes, explain why informally and explain the high-level reduction logic (without writing out the reduction or analyzing it). If no, demonstrate an attack and identify what kind of attack it is.

[4 marks]

Q3. (a) If p is a prime and $a \in \mathbb{Z}_{>0}$, state the conditions on $f(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ in order for $(\mathbb{Z}/p\mathbb{Z})[x]/(f(x))$ to be a field of size p^a.

[1 mark]

(b) Given a polynomial $g(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ and $m \in \mathbb{Z}_{\geq 2}$, define $g(x) \bmod m$ to be

$$g(x) \bmod m := \sum_{i=0}^{n} (a_i \bmod m) x^i \in (\mathbb{Z}/m\mathbb{Z})[x].$$

Give a polynomial $g(x) \in \mathbb{Z}[x]$ such that $(\mathbb{Z}/2\mathbb{Z})[x]/(g(x) \bmod 2)$ is a finite field of size 4, but $(\mathbb{Z}/3\mathbb{Z})[x]/(g(x) \bmod 3)$ is not a field. Justify your answer.

[4 marks]

Q4. In this question, we will play the part of an adversary and use index calculus to break the discrete logarithm problem to compute Alice's private key and forge her digital signature. It is recommended that you use a calculator to help you. Suppose that Alice is using a service which requires ElGamal signatures. This service uses the finite field $\mathbb{F}_{107}$ and the generator $g = 17$ for the unit group of the finite field $\mathbb{F}_{107}^*$. (The generator 17 has order 106 so does indeed generate the whole group).

(a) Using the following equations:

$$\begin{aligned} 17^2 &\equiv 3 \cdot 5^2 \pmod{107} \\ 17^9 &\equiv 2^2 \cdot 5 \pmod{107} \\ 17^{11} &\equiv 2 \pmod{107}, \end{aligned}$$

compute $\log_{17}(2)$, $\log_{17}(3)$, and $\log_{17}(5)$ mod 106.

[4 marks]

(b) Alice chooses a secret $a \in \mathbb{Z} \pmod{106}$ and publishes her public key $17^a = 94 \pmod{107}$. Find Alice's secret using index calculus with factor base $\{2, 3, 5\}$.

[3 marks]

(c) Give the steps of signing and verifying a message using ElGamal.

[4 marks]

(d) Using the nonce $k = 1$ and a message m with hash $H(m) = 0$, compute an ElGamal signature as if you were Alice. (If you did not manage part (b), suppose for this question that Alice's secret was $a = 102$. This is not the correct answer to (b).)

[2 marks]

(e) Suppose now that you observe Alice and Bob using the same parameters to compute a shared secret via a Diffie-Hellman key exchange. Bob's public key is $17^b = 54 \pmod{107}$. Compute their shared secret. (Hint: observe that $54 = 2^{-1} \pmod{107}$.)

[2 marks]

END OF PAPER