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

Answers to COMS-30002(J): Cryptography A

Intended Learning Outcomes:

- Explain and apply the principles of modern cryptology in the context of secure communication;
- Explain and demonstrate the functionality and desired security of standard cryptographic schemes used for confidentiality and authenticity;
- Link the design and operation of standard, state-of-the-art symmetric and asymmetric cryptographic schemes to their mathematical underpinnings;
- Use basic cryptanalytic techniques to evaluate the security level of simple cryptographic schemes.

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.

Solution:

Marking note: Answer C could be valid or invalid depending on the definition of AE-security used, as recognized by some students. Marks were never deducted for ticking, or not ticking, it.

[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.

(cont.)

[3 marks]

(cont.)

(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?

Solution: The blockcipher is being used in CFB mode.

Marking note: The original sample answer erroneously read “CBC”. Partial marks were given to students who recognized that the mode was not quite CBC but could not name it. Partial marks were given to students who identified the Encrypt-then-MAC “feel” of the mode.

[2 marks]

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

Solution:

```
$\mathsf{Dec}_K^N(C = C[1] \| M[2] \| M[4], T)$
$K' \leftarrow \mathsf{E}_K(N)$
$T' \leftarrow C[3] \oplus K'$
if $T \neq T'$
    return $\perp$
$C[0] \leftarrow N$
for $i \in 1, \ldots, 3$
    $X[i] \leftarrow \mathsf{E}_K(C[i-1])$
    $M[i] \leftarrow C[i] \oplus X[i]$
return $(M[1] \| M[2] \| M[3])$
```

Marking note: 1 mark for verifying the tag before decryption, 1 mark for recomputing the tag properly, 1 mark for decrypting properly.

[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.

Solution: The advantage of an adversary $\mathbb{A}$ in distinguishing a scheme Enc from random is defined as

$$\mathsf{Adv}^{\mathsf{(n)ind}}_{\mathrm{Enc}}(\mathbb{A}) = \mathsf{Pr}\left[\mathsf{Exp}^{\mathsf{(n)ind\text{-}real}}_{\mathrm{Enc}}(\mathbb{A}) : \hat{b} = 1\right] - \mathsf{Pr}\left[\mathsf{Exp}^{\mathsf{(n)ind\text{-}ideal}}_{\mathrm{Enc}}(\mathbb{A}) : \hat{b} = 1\right]$$

where the real and ideal experiments are defined as follows.

```
$\mathsf{Exp}^{\mathsf{(n)ind\text{-}real}}_{\mathrm{Enc}}(\mathbb{A})$
    $K \leftarrow_{\$} \mathsf{Kg}$
    $\hat{b} \leftarrow_{\$} \mathbb{A}^{\mathcal{E}(\cdot,\cdot)}$

    $\mathcal{E}(N, M)$
        no repeat nonces
        $C \leftarrow \mathsf{Enc}^{N}_{K}(M)$
        return $C$
```

```
$\mathsf{Exp}^{\mathsf{(n)ind\text{-}ideal}}_{\mathrm{Enc}}(\mathbb{A})$
    $\hat{b} \leftarrow_{\$} \mathbb{A}^{\mathcal{E}(\cdot,\cdot)}$

    $\mathcal{E}(N, M)$
        no repeat nonces
        $C \leftarrow_{\$} \mathcal{C}(|M|)$
        return $C$
```

Marking note: IND-CPA and IND-CCA were both accepted as valid answers. 1 mark for real/ideal idea, 1 mark for good oracles with appropriate restrictions, 1 mark for good advantage expression. Some students used Left-or-Right definitions, which were accepted for full marks (as equivalent).

[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.

Solution: From the point of view of confidentiality, our scheme is simply the blockcipher being used in CFB mode, which is not nonce-based indistinguishable from random.

However, CFB mode is indeed indistinguishable from random if nonces are chosen at random (this is the (IV)IND security notion), rather than controlled by the adversary. Our scheme is likely to inherit this property since the tag computation can easily be simulated with oracle access to the blockcipher and information that is known to the (IV)IND adversary.

Qu. continues ...

Marking note: The scheme is thoroughly insecure! The idea was to get students to think about the hierarchy of security notions, and to briefly come up with rationales for their thoughts. The sample answer is one of those I expected. 1 mark was given for identifying (and naming or definining) a security notion that is truly weaker than the one given by the student in 2c; 1 mark for a rough rationale for security; the final mark was given to any student who noted that the scheme simply cannot meet any notion that requires indistinguishability (even under passive attack) since the tag reveals the first block of plaintext.

[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.

Solution: The scheme does not provide ciphertext integrity. Given a single nonce-ciphertext-tag triple (N, C, T) given by a known-message oracle, the adversary can easily forge a new valid triple as $(N, C \oplus Z, T \oplus Z)$ for any $Z \neq 0^\ell$.

Since it requires a nonce-ciphertext-tag triple but does not require the adversary to control the plaintext (or indeed the ciphertext), the attack is a known-message (or known-ciphertext) attack. Classifying it as a chosen-message attack would yield partial marks.

Marking note: 1 mark for "No"; 1 mark for identifying the flaw; 1 mark for demonstrably exploiting it; 1 mark for a name (CMA was, in the end, accepted for full marks).

[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.

Solution: $f(x)$ must be a polynomial of degree a, and must be irreducible.

[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.

Solution: To fulfill the first condition, we must have $g(x) \bmod 2 = x^2 + x + 1$. To avoid forming a field of characteristic 3, we must have that $g(x) \bmod 3$ is reducible in $\mathbb{Z}/3\mathbb{Z}[x]$.

We can, for example, pick $x^2 + x + 1$ itself as this factors mod 3 as $(x - 1)^2$.

[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:

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

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

Solution: The last equation immediately gives us

$$\log_{17}(2) \equiv 11 \pmod{106}$$

From the second equation, we get that $9 \equiv 2 \cdot \log_{17}(2) + \log_{17}(5) \pmod{106}$. We substitute and simplify, obtaining

$$\log_{17}(5) \equiv 93 \pmod{106}$$

Finally, from the first equation, we get $2 \equiv \log_{17}(3) + 2 \cdot \log_{17}(5) \pmod{106}$, and conclude after substitution and simplification that

$$\log_{17}(3) \equiv 28 \pmod{106}$$

[4 marks]

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

Solution: Observe that 94 does not factorise into only powers of elements in the factor base, so we try $17 \cdot 94$, which is $2^2 \cdot 5^2 \pmod{107}$. Therefore, we have $\log_{17}(94) \equiv 2 \cdot \log_{17}(2) + 2 \cdot \log_{17}(5) - 1 \pmod{106}$. Using the pre-computed values for $\log_{17}(2)$ and $\log_{17}(5)$, we conclude that

$$\log_{17}(94) \equiv 101 \pmod{106}$$

[3 marks]

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

(cont.)

Solution:

```
$\mathsf{Sign}_{\mathsf{sk}}(m)$
$s \leftarrow 0$
while $s = 0$
    $k \leftarrow_{\$} (\mathbb{Z}/p\mathbb{Z})^*$
    $r \leftarrow g^k \pmod{p}$
    $s \leftarrow (\mathsf{H}(m) - r \cdot \mathsf{sk}) \cdot k^{-1} \pmod{p-1}$
return $(r, s)$
```

```
$\mathsf{Verify}_{\mathsf{pk}}(m, (r, s))$
Check that $0 < r < p$
Check that $0 < s < p - 1$
return $g^{\mathsf{H}(m)} \equiv \mathsf{pk}^r \cdot r^s \pmod{p}$
```

[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).)

Solution: $r = g^k = 17^1 = 17$, and with $a = \mathsf{sk} = 101$ as computed in part (b) we get

$$\begin{aligned} s &= (0 - 17 \cdot 101) \cdot 1 \pmod{106} \\ &= 17 \cdot 5 \pmod{106} \\ &= 85 \pmod{106}. \end{aligned}$$

The result using $a = 102$ is $(17, 68)$.

[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 $54 = 2^{-1} \pmod{107}$.)

Solution: Their shared secret is

$$\begin{aligned} (17^b)^a \pmod{107} &\equiv 54^{101} \pmod{107} \\ &\equiv 2^{-101} \pmod{107} \\ &\equiv 2^5 \pmod{107} \\ &\equiv 32 \pmod{107}. \end{aligned}$$

The result using $a = 102$ is 16.

[2 marks]

END OF PAPER