UNIVERSITY OF BRISTOL

JANUARY 2017 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 *60 marks*.

Other Instructions:

1. Calculators must have the Faculty of Engineering Seal of Approval.

TURN OVER ONLY WHEN TOLD TO START WRITING

Q1. (a) A friend of yours has stumbled over the concept of the one-time pad. Unfortunately, he did not attend Crypto A, so he needs your help to make sense of the following statements. Moreover, some of the statements are misleading or even incorrect. Comment on the validity of each of the statements below, drawing particular attention to mistakes or misleading claims.

[12 marks]

A. the one time pad is useless because it just xors plaintexts and ciphertexts.

B. the one time pad provides perfect secrecy, and hence the key can be reused securely.

C. the one time pad is not secure because the key needs to be as long as the message that you encrypt.

D. the one time pad is so secure that even an adversary with unlimited computing power cannot break it.

E. the one time pad provides perfect secrecy and hence integrity of ciphertexts.

(b) Your friend has moved on to more modern cryptology, but is still struggling. He has realized that key lengths are important when implementing cryptography in real life, but isn't entirely sure about the following four statements. Again, comment on each of the statements below, drawing particular attention to mistakes or misleading ones.

[6 marks]

A. The longer the key the more secure any system will be.

B. Furthermore, it is important to have a good random number generator for key generation.

C. However, in case of public key cryptography, it is o.k. to have short public keys.

D. Even if you loose your secret key, you can still decrypt messages.

Q2. WhatsApp is a messaging service that introduced end-to-end encryption in 2016. There is a WhatsApp Security Whitepaper that explains how media and other attachments are transmitted. There are various steps to ensure that both the sender and receiver share two keys, namely an AES256 key and a HMAC-SHA256 key. With these in place, the main cryptographic step reads:

> The sender encrypts the attachment with the AES256 key in CBC mode with a random IV, then appends a MAC of the ciphertext using HMAC-SHA256.

(a) Unpack the terminology from the quote above by explaining what the various abbreviations (AES256, CBC, IV, MAC, HMAC, SHA256) refer to and what their general purpose is. You do not (yet) have to explain how they work.

[12 marks]

(b) For *one* of the schemes or modes mentioned (AES256, CBC, HMAC, SHA256) explain at a high level how it works.

[3 marks]

(c) Assume a receiver already has all the relevant keys. How would they decrypt some received ciphertext? (Note: describe the steps in roughly the same amount of detail as in the quote above.)

[3 marks]

(d) What security goal(s) do you think WhatsApp is targeting? Describe the goal informally and link it to a formal security notion (you do not need to give the full definition or diagram of the security notion).

[4 marks]

Q3. This question addresses RSA-OAEP and a simplification thereof. Let's first consider the original.

(a) Explain the purpose of the original OAEP. In particular, which weaknesses of vanilla or textbook RSA are addressed by using RSA-OAEP instead?

[3 marks]

(b) RSA-OAEP can be proven IND-CCA secure under the RSA assumption in the random oracle model. Prove that any IND-CCA secure public key encryption scheme is also OW-CPA secure (you may ignore the random oracle).

[6 marks]

Now consider the following simplified version of RSA-OAEP instead. Let H be a public hash function from $\{0,1\}^{1535} \to \{0,1\}^{512}$ and, given an RSA modulus N and some $R \in \{0,1\}^{128}$, define $\mathsf{pad}_R : \{0,1\}^{512} \to \mathbb{Z}_N$ by $\mathsf{pad}_R(\mathsf{m}) = (0^{1407}||R||\mathsf{H}(0^{1407}||R) \oplus \mathsf{m})$ where this 2047-bit string is interpreted as an integer in $\{0, ...2^{2047} - 1\} \subset \mathbb{Z}_N$ (for instance, the bitstring $(0^{2045}||11)$ corresponds to 3).

Key generation Kg selects two random yet distinct 1024-bit prime numbers p and q, both congruent to 2 modulo 3. Let $N \leftarrow p \cdot q$ and $e \leftarrow 3$. Set d to the inverse of e modulo $\phi(N)$. Select a random $R \in \{0,1\}^{128}$ and publish (N, R, e) as the public key pk while keeping (N, R, d) as the private key sk.

Encryption Enc takes as input the public key $\mathsf{pk} = (N, R, e)$ and a message $\mathsf{m} \in \{0,1\}^{512}$. It computes and returns ciphertext $\mathsf{c} \leftarrow \mathsf{pad}_R(\mathsf{m})^e \bmod N$.

(c) Describe how decryption for the RSA version with padding as above works.

[2 marks]

(d) Explain why decryption, as described by you, works. Concentrate on the modular arithmetic involved.

[3 marks]

(e) Assume H is a secure hash function. Argue about the security of the scheme above. Highlighting multiple strengths and weaknesses may result in higher marks. Where possible, illustrate a weakness by giving an explicit attack.

[6 marks]

END OF PAPER