NATIONAL UNIVERSITY OF SINGAPORE

CS4236 — CRYPTOGRAPHY THEORY AND PRACTICE

(Semester 1: AY 2016/17)

Time Allowed: 2 Hours

INSTRUCTIONS TO STUDENTS

1. Please write your Student Number only. Do not write your name.
2. This assessment paper contains **FIVE** questions and comprises **ELEVEN** printed pages.
3. Answer **ALL** questions.
4. Write your answer within the given box in each question.
5. You may use pencil.
6. This is an Open Book assessment.

Student Number: _____

Question	Full Marks	Marks	Remark
Q1	20		
Q2	22		
Q3	20		
Q4	16		
Q5	22		
Total	100		

In all questions, schemes with less than 56-bit security are considered to be insecure.

1. **[20 marks]** Bob implemented a $(2,3)$-secret sharing scheme with 4 as the moduli. Let w be the secret to be shared, and a be the coefficient randomly & uniformly chosen (from $\{0,1,2,3\}$). Hence, the polynomial is $f(x) = (ax + w) \mod 4$, and the participant P_i will get the share $f(i)$ for $i = 1, 2, 3$.

   Let s_i be the share received by P_i for $i = 1, 2, 3$. Let W, A, S_1, S_2 and S_3 the corresponding random variable for w, a, s_1, s_2 and s_3. Suppose the secret k follows the distribution:

$Prob(W=0)$	$Prob(W=1)$	$Prob(W=2)$	$Prob(W=3)$
$\frac{1}{8}$	$\frac{3}{8}$	$\frac{1}{8}$	$\frac{3}{8}$

   (a) (2 marks) Let $\tilde{a} = 3a \mod 4$, and $\tilde{A}$ the corresponding random variable. What is the distribution of $\tilde{A}$?

$Prob(\tilde{A}=0)$	$Prob(\tilde{A}=1)$	$Prob(\tilde{A}=2)$	$Prob(\tilde{A}=3)$

   (b) (5 marks) Determine the following conditional probabilities.

$Prob(W=0\|S_3=0)$	$Prob(W=1\|S_3=0)$	$Prob(W=2\|S_3=0)$	$Prob(W=3\|S_3=0)$

   What about when $S_3 = 1$?

$Prob(W=0\|S_3=1)$	$Prob(W=1\|S_3=1)$	$Prob(W=2\|S_3=1)$	$Prob(W=3\|S_3=1)$

   (c) (3 marks) What can be said regarding information on w that P_3 can obtain?

(d) (5 marks) Now, consider s_2. Determine the following conditional probabilities.

$Prob(W = 0 \mid S_2 = 1)$	$Prob(W = 1 \mid S_2 = 1)$	$Prob(W = 2 \mid S_2 = 1)$	$Prob(W = 3 \mid S_2 = 1)$

(e) (5 marks) Bob made a mistake in his implementation. What is the mistake and how to fix it? Describe the consequences of this mistake.

2. **[22 marks]**

Consider a hash function $H()$ with 160-bit digests. Let $\ell(x)$ be the 80 least significant bits of x, and $rev(x)$ be the reversal of x (hence, $rev(\text{“}11101\text{”})$ is “10111”).

(a) (5 marks) Let $H_1(x) = H(H(x)\|H(x))$. Show that if $H()$ is not collision-resistant, then $H_1()$ is also not collision-resistant.

(b) (6 marks) Let $E(k, x)$ be a block cipher that on input a 160-bit key k and a 160-bit plaintext, outputs a 160-bit ciphertext. Let $H_2(k\|x) = E(k, x)$. In other words, on input a 320-bit message, $H_2()$ outputs a 160-bit digest. Show that $H_2()$ is not one-way.

Not one-way = not pre-image resistant
Given E(k, x) => computationally feasible to find k||x s.t. H2(k||x) = E(k,x)
Proof by reduction
A can find k and x from E(k, x)

A' runs A as subroutine

H2(k'||x') =H2(k||x) for some k', x'
not second pre-image resistant => not one-way

(c) (5 marks) Let $H_3(x) = \ell(H(x))$. Show that $H_3()$ is not collision-resistant.

Clearly not coll-res

Suppose H is coll-res
H(x) ≠ H(x'), for x, x', x≠x'
But
l(H(x)) = l(H(x'))

(d) (6 marks) Let $H_4(x) = \ell(H(x)) \parallel \ell(H(rev(x)))$. Show that $H_4()$ is not collision-resistant.

3. **[20 marks]**

(a) (10 marks) Alice has access to an encryption device $\mathcal{O}$ that performs AES under CBC mode. On input m, $\mathcal{O}$ outputs the ciphertext c encrypted using a fixed 128-bit key k and a 128-bit IV. The device chooses the IV in the following way:

i. Randomly pick a 70-bit string r from a true random source.

ii. Take the leading 128 bits of SHA3(r) as the IV.

Alice doesn't know k. If the device is faulty, it will output a randomly chosen string of the same length as the ciphertext. Give a method for Alice to test whether the device $\mathcal{O}$ is faulty.

Does the (non-faulty) device achieve semantic security?

(b) (10 marks) Bob plans to build a rainbow table to invert hashes of passwords from a dictionary $\mathcal{D}$ where size of $\mathcal{D}$ is 2^{40}. Under Bob's plan, the length of each chain is 2^{10} (hence, there are 2^{10} passwords in a chain), and there are a total of 2^{30} chains. The digest at the end of each chain is unique (i.e. no repetition). Bob claims that his table can achieve 90% accuracy. Explain why Bob's claim is likely to be wrong.

Suppose the number of chains is to be fixed at 2^{30}, estimate the smallest possible chain length in order to achieve 90% accuracy?

To reduce the total size, instead of storing the full digest, Bob plans to store only a few bits extracted from each digest. Bob has the choices of either 25, 30, 35, 40, 45 or 50 bits. Which would be a good choice? Why?

4. **[16 marks]** Bob feels that RSA is cool and wants to use it under the symmetric key setting, where the key (for both encryption and decryption) is to be kept secret. He implemented 3 variants.

   (a) (5 marks) First variant. The secret encryption and decryption key consists of both the RSA public key n, e and the private key d. Given a plaintext x, the ciphertext is:

   $$Enc_{\langle n,e,d\rangle}(x) = x^e \bmod n.$$

   Give the decryption algorithm $Dec_{\langle n,e,d\rangle}()$. Note that the input consists of the ciphertext c and the key $k = \langle n, e, d\rangle$.

   Does this scheme achieve semantic security? Why?

   (b) (5 marks) Second variant. The secret encryption/decryption key is d, a 32-bit integer. Given a plaintext x, the encryption is done as follows:

   S1. Randomly picks two 1024-bit strong primes p and q.

   S2. Compute $n = pq$. Compute $e = d^{-1} \bmod \phi(n)$.

   S3. The ciphertext is $\langle n, x^e \bmod n\rangle$.

   Does this scheme achieve semantic security? Why?

(c) (6 marks) Third variant. The secret encryption/decryption key consists of two numbers $\langle p, d \rangle$, where p is a 1024-bit strong prime, and d is a 32-bit integer. Given the plaintext x, the ciphertext is computed as follows:

S1. Randomly picks a 1024-bit strong prime q.

S2. Compute $n = pq$. Compute $e = d^{-1} \bmod \phi(n)$.

S3. The ciphertext is $\langle n, x^e \bmod n \rangle$.

During decryption, with the key $\langle p, d \rangle$, the plaintext can be efficiently computed from the ciphertext $\langle n, x^e \bmod n \rangle$.

This variant is not secure. Why? (Hints: what would happen if it is used twice?)

5. **[22 marks]**

(a) (12 marks) Consider the ElGamal given in Lecture 11. Let us choose $p = 7, g = 3, x = 4$.

i. What is the public key h?
(Hint: The multiplication table of Z_7^* given in Lecture 8 could be useful in the calculation).

ii. Suppose the ciphertext is $\langle 2, 3 \rangle$, what is the plaintext?

iii. Suppose the ciphertext is $\langle 2^{602}, 3^{602} \rangle$, what is the plaintext? (All arithmetic are done with respect to modulo 7)

(b) (10 marks) Bob implemented a commitment scheme based on ElGamal encryption. To commit a message m, Bob randomly chooses a private key x and the public key g, p, h. The commitment is the ciphertext $\langle c_1, c_2 \rangle$ of m encrypted using the key x, g, p, h. To open a commitment, Bob reveals the key x, g, p, h and the message m. To verify that the commitment is valid, one just have to decrypt $\langle c_1, c_2 \rangle$ and check that indeed the plaintext is m. Show that this construction doesn't achieve binding property.

(Hint: Always output a fixed commitment, say $\langle g^2, g^2 \rangle$ for some randomly chosen g, p. Now, show how to open the commitment for two different messages m_1 and m_2)

— End-Of-Paper —