NATIONAL UNIVERSITY OF SINGAPORE

CS4236 - CRYPTOGRAPHY THEORY AND PRACTICE

(Semester 1: AY2021/2022)

Time allowed: 2 hours

INSTRUCTIONS TO STUDENTS

This assessment paper contains **FIVE (5)** sections totalling **FORTY** (**40**) marks, and comprises **TEN (10)** printed pages including this one.

This is an **OPEN BOOK** assessment, and you are to answer **ALL** questions. You may cite any result in the lecture notes or tutorials. Answer **ALL** questions within the space provided in this booklet (write on the backs of pages if you need more room).

Please write your Student Number below. (Do not write your name).

STUDENT NO: _____

This portion is for examiners use only.

Question		**Marks**	**Remark**
General topics, short answers	Q1 (8)		
MAC and HASH	Q2 (10)		
Symmetric encryption	Q3 (7)		
Asymmetric encryption	Q4 (8)		
Signatures and secrets	Q5 (7)		
Total:	Q1-5 (40)		

Q1 (Short Answer Questions) (8 marks)

In the following short questions, each answer is worth either 1 (ONE) or 2 (TWO) marks.

1.1 Calculate the bias for $x \oplus y$ (with x, y independent) when $\varepsilon(x) = 0.2$ and $\varepsilon(y) = 0.3$. Show your working. (2 marks)

Answer:

1.2 Explain what limits are usually placed on decryption oracles used in adversarial games for defining properties of encryption schemes. (1 mark)

Answer:

1.3 Many Proof of work schemes involve finding something with a lot of zeros. Explain in your own words what is meant by this. What do you need to do to prove you have "done the work:"? (1 mark)

Answer:

Q1 (Short Answer Questions) (Continued)

1.4 Show that $G(x) \stackrel{\text{def}}{=} x \bmod p$, cannot be a PRG. (2 marks)

Answer:

1.5 Calculate the entropy in bits/symbol, of a source emitting the 4 symbols E, X, A and M, with the probability of E being 0.5, X being 0.25, and A and M having equal (0.125) probabilities. Show your working. (2 marks)

Answer:

Q2 (MAC and HASH) (10 marks)

2.1 Assume you were investigating a new MAC scheme based on $Enc_k(H(m))$, where the HASH is SHA3, and the encryption is AES in CBC mode. Show how you could forge a fresh (m', t) pair for any m', but without finding a (HASH) collision. You have an example of a valid (m', t) pair, and control over an AES in CBC encryption mechanism $\text{Enc}_{k,\text{IV}}(p)$. Show clearly each step in your attack. (4 marks)

Answer:

2.2 Rainbow tables and the birthday attack are both attacks applied to hashes. However, each attempts a different task. Explain clearly what each attack attempts to do. (2 marks)

Answer:

Q2 (MAC and HASH) (Continued)

2.3 Show/prove that there exists a MAC that is secure (existentially unforgeable) but that is not strongly secure. (4 marks)

Answer:

Q3 (Symmetric encryption) (7 marks)

3.1 In an authenticated encryption scheme, why is the **encrypt-and-authenticate** scheme considered to be unsafe (or to have issues)? (2 marks)

Answer:

3.2 Briefly explain why in symmetric systems based on rounds, the rounds include both substitutions and permutations. Why could we not have a system based just on rounds of substitution or permutation alone? (2 marks)

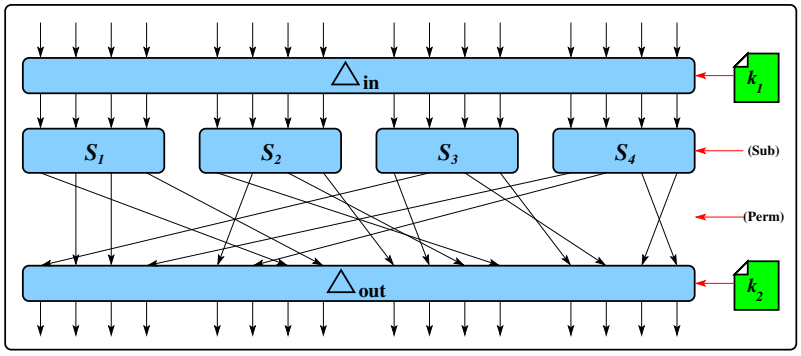
Answer:

Q3 (Symmetric encryption) (Continued)

x	$S(x)$
0	0
1	b
2	5
3	1
4	6
5	8
6	d
7	4
8	f
9	7
a	2
b	c
c	9
d	3
e	e
f	a

z	$P(z)$
1	7
2	2
3	3
4	8
5	12
6	5
7	11
8	9
9	10
10	1
11	14
12	13
13	4
14	6
15	16
16	15

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	4	0	0	0	2	2	2	2	0	0	4	0
2	0	0	0	0	0	2	0	2	0	2	2	4	2	2	0	0
3	0	2	2	4	0	4	0	0	0	0	0	0	0	2	2	0
4	0	0	0	2	2	2	6	0	2	0	0	0	2	0	0	0
5	0	2	2	0	0	0	0	0	4	0	0	0	4	2	2	0
6	0	2	0	2	0	0	0	0	0	2	0	2	0	4	0	4
7	0	2	0	0	2	4	2	2	0	2	0	0	0	2	0	0
8	0	0	0	2	0	0	0	2	0	0	0	2	2	2	2	4
9	0	2	0	2	2	2	0	4	0	2	2	0	0	0	0	0
a	0	0	4	0	2	0	2	4	2	0	2	0	0	0	0	0
b	0	0	2	0	0	0	2	0	0	2	0	0	4	2	4	0
c	0	0	0	0	0	0	0	0	4	4	0	4	0	0	0	4
d	0	4	2	2	0	0	2	2	0	0	0	0	0	0	0	4
e	0	2	4	2	4	0	0	0	0	0	0	0	2	0	2	0
f	0	0	0	0	0	2	2	0	2	0	8	2	0	0	0	0



3.3 Shown above is an example of a single stage of differential analysis, based on the substitution and permutation from the toy example. If the input bits of interest for S_1 were 1001 (i.e. 9), which (16-bit) input and output bits would be most useful for differential analysis, and what would the differential probability $\Pr[\langle \Delta_{\text{in}}, \Delta_{\text{out}} \rangle]$ of this be? (3 marks)

Answer:

Q4 (Asymmetric encryption) (8 marks)

4.1 Textbook RSA is deterministic, and so if someone sends the same message as before, an adversary can know this. Assuming that a challenger never sent the same message twice though, an adversary might still be able to differentiate between (say) two messages it was expecting:

$$m_1 = \text{“Attack at dawn”}$$
$$m_2 = \text{“Attack at noon”}$$

where each message encodes to a single 2048 bit integer m and the adversary snoops the ciphertext $c = m^e mod N$. Explain how an attacker might be able to identify which of the two messages is in the ciphertext, even if the attacker does not know the public or private keys used. (3 marks)

Answer:

4.2 Explain why you might use $g = X$ rather than $g = Y$ for a generator for DHKE. (2 marks)

In your answer you should explain what constraints or issues affect a generator, and why you would choose one generator over another.

Answer:

Q4 (Asymmetric encryption) (Continued)

4.3 Alice is going to send a message to Bob using ECC *encryption*. Bob has a private/secret key $K_S = \langle 4, E_{31}(1,1), (0,1)\rangle$, and public key $K_P = \langle (22,21), E_{31}(1,1), (0,1)\rangle$. If Alice encoded her message as the point $(4,21)$, and chooses a random value $k = 2$, what message does she send to Bob? Show your working.. (3 marks)

Answer:

Q5 (Signatures and secrets) (7 marks)

5.1 Explain why canonical verification of a signature is not possible. (2 marks)

Answer:

5.2 Explain why **hash-and-sign** is better than (say) **sign-and-hash**. (2 marks)

Answer:

5.3 In Feldman's VSS scheme, the key k is masked as $c = \mathscr{H}(a_0) \oplus k$, rather than just being a_0. Explain why this is done in this scheme (and not in Shamir's for example)? (3 marks)

Answer:

=== END OF PAPER ===