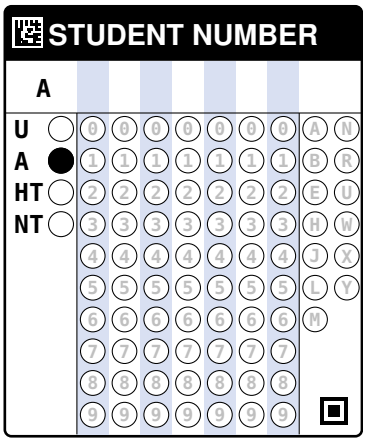
CS2107 Introduction to Information Security

Endterm Exam — Answer Sheet



FOR EXAMINER'S USE

Question	Marks
Q1-Q20	/ 20
Q21-Q25	/ 10
Q26	/ 5
Q27	/ 4
Q28	/ 7
Q29	/ 4
Total	/ 50

1. A B C **D** E
2. A **B** C D E
3. A B C **D** E
4. A B **C** D E
5. A B **C** D E
6. A **B** C D E
7. A B **C** D E
8. **A** B C D E
9. A **B** C D E
10. A B **C** D E
11. A B C D **E**
12. A B C **D** E
13. A B **C** D **E**
14. A B **C** D E
15. **A** B C D E
16. A **B** C D E
17. A B C **D** E
18. A B C **D** E
19. A B **C** D E
20. A **B** C D E
21. A **B** C D E
22. A B **C** D E
23. **A** B C D E
24. A B C **D** E
25. A **B** C D E

26. AES-CBC MAC scheme

(a) Attack Step [3 marks]

orignal tag = t = E(K, IV xor M1)
What mallory want is : t = E(K, IV' xor M2)
Manipulate IV' = IV xor M1 xor M2
Mallory does E(K, IV' xor M2) = E(K, IV xor M1 xor M2 xor M2) = E(K, IV xor M1) = t

(b) Countermeasure [2 marks]

1. The MAC is computed over the encrypted M1, so the attacker cannot manipulate the MAC input to produce meaningful, undetectable changes.
t = MAC(K1, IV xor E(M1,K2)) => without knowing CT, just knowing M1, attacker cannot forge.
2. Use HMAC or CMAC
3. Remove IV or fix a common IV

27. Fill in the blanks [4 marks]

(1) X = g^a mod p

(2) Y = g^b mod p

(3) K_{AB} = g^ab mod p

(4) b' = hash(K_BA) or K_BA

(5) Z = g^b' mod p

(6) U = g^c mod p

(7) a' = hash(K_AB) or b' or K_BA

(8) K_{ABC} = g^b'c mod p or g^K_ABc mod p or U^b' mod p

28. Padding oracle

(a) Last 6 bytes [6 marks]

v'	49	63	4C	75	50	6D	4F	73	4D	x	75,	EB,	A8,	8F,	BC,	88
c	76	51	69	59	37	2E	61	63	41	2E	59	6D	52	73	47	75

(b) Value of $p10$ [1 mark]

43

29. CSRF

(a) Malicious form [3 marks]

```
<form id="changepass" method="POST" action="http://facetalk.com/password.php" target=invisibleframe>
<input type="text" name="password" value="1234">
<input type="submit" value="Change my password"/>
</form>
<script>document.forms[0].submit()</script>
```

(b) Reason [1 mark]

If Alice is not logged in, the request will fail because it lacks a valid session.
Since the website requires an active session to process password changes, the request was rejected due to the absence of a valid session cookie.

— END OF ANSWER SHEET —