Feedback — Quiz_week3

Help Center

You submitted this quiz on **Tue 3 Feb 2015 9:36 AM PST**. You got a score of **13.00** out of **15.00**.

Question 1

Which of the followings about physical attacks are correct? Check all that apply.

Your Answer		Score	Explanation
☑ Some physical attacks do not need physical access to the system	✔	0.25	
☑ All physical attacks will need the help from some tools and/or equipment	✔	0.25	
☐ All physical attacks will leave tamper trace after attack	✔	0.25	
☐ All physical attacks will make damage to the system	✔	0.25	
Total		1.00 / 1.00	

Question Explanation

grading: 0.25 each

Question 2

Which of the following physical attacks are invasive? Check all that apply.

Your Answer		Score	Explanation
☐ Software attacks	✔	0.25	
☑ Reverse engineering	✔	0.25	
☐ Side channel attacks	✔	0.25	
☑ Microprobing	✔	0.25	
Total		1.00 / 1.00	

Question Explanation

grading: 0.25 each

Question 3

Which of the following non-invasive attacks are passive? Check all that apply.

Your Answer		Score	Explanation
☑ Side channel attack	✔	0.25	side channel attack itself is passive, but it can be combined with other method (such as fault injection) to become active.
☐ Data remanence	✔	0.25	
☐ Brute force	✔	0.25	
☐ Fault injection	✔	0.25	
Total		1.00 / 1.00	

Question Explanation

grading: 0.25 each

Question 4

Which of the following about invasive attacks are true? Check all that apply.

Your Answer		Score	Explanation
☑ With sensor mesh at the top metal layer, any attempt of invasive attack can be	✔	0.25	

detected.		
☑ It is possible to probe into a single bus line and inject data to control bus activity.	✔	0.25
☐ Because invasive attacks need to depackage the chip, all invasive attacks will be very expensive.	✔	0.25
☐ When the bus lines are scrambled, the attackers cannot find the bus lines to probe.	✔	0.25
Total		1.00 / 1.00

Question Explanation

grading: 0.25 each

Question 5

Which of the following statements are true for data remanence on SRAM? Check all that apply.

Your Answer		Score	Explanation
☑ SRAM may retain data shortly after power off, so data may leak.	✔	0.25	
☑ It is possible to freeze data and read it at	✔	0.25	

temperature higher than -20 degree.			
☐ When power up, SRAM's initial value will be random, so no data will leak.	✔	0.25	If data has been in the same SRAM for long, its value might be burned-in.
☐ Data can be extracted from SRAM after multiple write/erase cycles.	✔	0.25	This is for EEPROM and Flash.
Total		1.00 / 1.00	

Question Explanation

grading: 0.25 each

Question 6

When we use the "iterative exponentiation and modular" method to compute $2^4 (mod\ 5)$, starting from 2^1, we will have $2^1 = 2(mod\ 5)$; $2 \times 2 = 4(mod\ 5)$; $4 \times 2 = 3(mod\ 5)$; $3 \times 2 = 1(mod\ 5)$. The results we will see are 2, 4, 3, 1. If we use the same method to compute $3^7 (mod\ 5)$, starting from 3^1, the results we will see are

Your Answer	Score	Explanation
○ 3, 9, 27, 81, 243, 729. 2187		

3, 4, 1, 2, 0, 2, 1		
1, 2, 3, 4, 0, 1, 2		
3, 4, 2, 1, 3, 4, 2	✔	1.00
Total		1.00 / 1.00

Question 7

Which of the following decimal to binary conversion are correct? Check all that apply.

Your Answer		Score	Explanation
19 = 10011	✔	0.50	
124 = 1111100	✔	0.50	
79 = 1001111	✔	0.50	
37 = 101011	✔	0.50	
Total		2.00 / 2.00	

Question Explanation

grading: 0.5 each

Question 8

For e=10,0101,0110, when we compute $a^e (mod\ n)$ with the left to right "square and multiple algorithm (l)", the total number of multiplication (both b*b and b*a) we will do is

You entered:

15

Your Answer		Score	Explanation
15	✔	2.00	
Total		2.00 / 2.00	

Question Explanation

2 multiplications for the leading bit 1: one b*b and one b*a, both are trivial operations, 1*1 and 1*a. If we replace line 2 by b=a; and start the for loop in line 3 with i=s-1; these 2 multiplications can be saved.

Question 9

In the slide of "Montgomery Reduction", which of the following conditions are necessary? Check all the apply.

Your Answer		Score	Explanation
☐ T > N	✔	0.50	we need R>N, not T>N.
☐ N is a prime	✔	0.50	
☐ R is a power of 2	✔	0.50	
☑ gcd (R,N) = 1	✔	0.50	otherwise N inverse mod R may not exist.
☐ gcd (T,N) = 1	✔	0.50	we need gcd(R,N)=1, not gcd(T,N)=1.
☑ T	✔	0.50	otherwise we cannot guarantee t < N.
Total		3.00 / 3.00	

Question Explanation

grading: 0.5 each

Question 10

The Montgomery reduction of 25 modulo 109 w.r.t. 128 is

You entered:

21

Your Answer		Score	Explanation
21	✖	0.00	
Total		0.00 / 2.00	

Question Explanation

Hint: review the slides on Montgomery reduction. Some of the important data you need can be found there, you don't have (and you may not know how to) compute it.