## Hardware Security 2020-21

## Class test - 1

*Answers have been provided in **bold**.*

1. In Von Neumann architecture
   a. The memory is physically shared for data and instruction storage
   b. Memory hierarchy is used to make security better
   c. There are two separate memory buses
   **d. None of the above**

   [1 marks]

2. Basic building block of an FPGA is
   **a. LUT & Flip-flop**
   b. CLB
   c. BRAM
   d. none of the above

   [1 marks]

3. Blocking assignments in Verilog executes in
   **a. series**
   b. parallel
   c. both
   d. None

   [1 marks]

4. always@(_____**posedge rst/negedge rst**_____) . What should be the sensitivity list for asynchronous reset?

   [1 marks]

5. Consider the following C code snippet used to perform a buffer overflow attack:

```
#include<stdio.h>
void simple_call()
{
      int buf[3];
      int *ret;
      ret = buf + ____(ii)___;  //to point to the return
address to main function
      *ret = *ret + ___(iii)____;
}
int main()
{
```

```
        int flag = 1;
        simple_call();
        flag = 0;
        if(flag == 1)
            printf("Statement skipped. Attack successful");
        else
            printf("Attack unsuccessful");
}
```

Here, ret pointer points to the return address of the simple_call(). The stack contains 3 consecutive locations for buf, followed by one location for ret, one location for the base pointer address of the main function and one location for the return address to main function. Each location takes 4bytes.

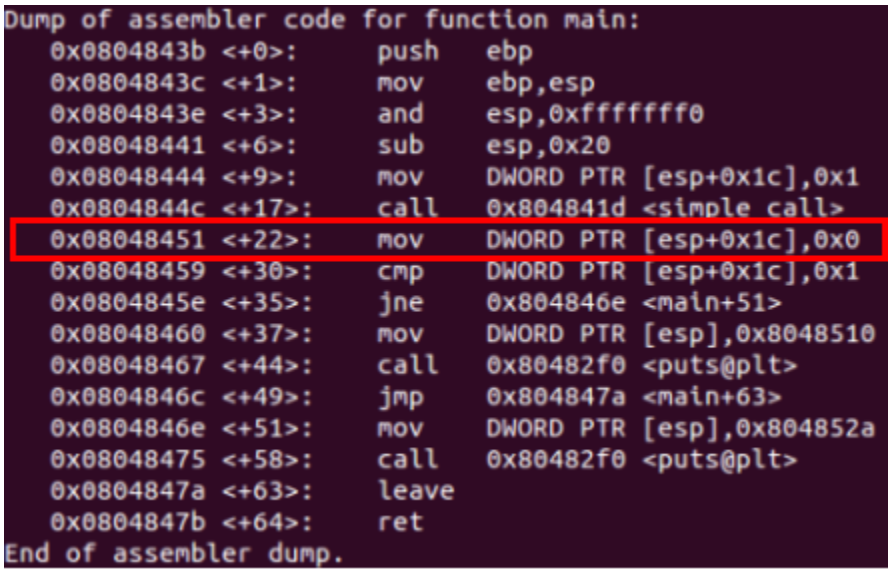
i) If the start address of buf is 0xbfffef98, the return address to the main function is **_____0xbfffefac_____**.

[2 marks]

ii) What should the ret pointer be initialized to? **5**

[1 marks]

iii) In the assembler code dump, the instruction in the red box corresponds to the statement ( flag = 0). To skip this statement, by what value should ret be incremented? **8**




[2 marks]

6. (i) Consider a 4X1 MUX with select lines $S_0$, $S_1$ and data inputs $W_3, W_2, W_1, W_0$ . Also consider that you get 4 input LUTs.How many minimum LUTs are required to construct the MUX? _____2_____

[5 marks]

(ii) What is the minimum number of LUTs required to implement the following functions together on an FPGA. Assume that you can enter complement of signals~(say A') as input.

$F_1$(A, B, C, D, E, F, G, H, I) = ABCDE + F'GHID'E'

$F_2$(A, B, C, D, E, F, G, H, I) = ABCEF + F'GHI

Assume an LUT has 4 inputs.
Answer: 4

[5 marks]

7. The Karatsuba multiplier can be represented as follows:

$$A(X) = A_h X^{m/2} + A_l$$

$$B(X) = B_h X^{m/2} + B_l$$

$$C(X) = A(X)B(X) = A_h B_h X^m + Z_1 X^{m/2} + A_l B_l$$

Which of the following is a correct choice for $Z_1$?

**a.** $Z_1 = (A_l - A_h)(B_h - B_l) + A_h B_h + A_l B_l$

b. $Z_1 = (A_l + A_h)(B_h + B_l) - A_h B_h + A_l B_l$

c. Both

d. None

[2 marks]

8. Consider a binary Karatsuba multiplier. The recursive multiplication algorithm reduces the size of the input by 2 in every iteration. The number of multiplications increase by a factor of

a. 2

**b. 3**

c. 4

d. None of the above

[2 marks]

9. For an m-bit multiplier, the size of the inputs for the k-th recursion is

a. $t = 2^{m-k}$

b. $t = 2^{3^{m}-k}$

c. $t = 2^{3m-k}$

**d.** $t = 2^{log_2 m-k}$

[2 marks]

10. Consider a linear cipher as shown in figure below. An adversary has only access to the produced ciphertexts. He has no knowledge about the secret key K and the corresponding plaintext ($P_1$ and $P_2$) but knows the linear operation being performed.

    Which of the following information can be obtained by the adversary from the two ciphertexts $C_1$ and $C_2$?

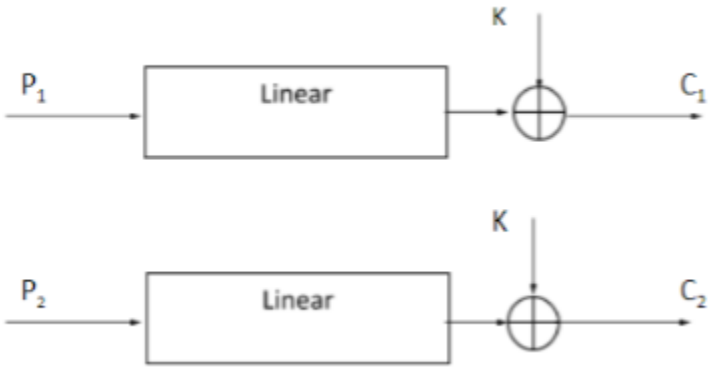
    a. $P_1$ and $P_2$

    **b.** $P_1$ **xor** $P_2$

    c. No information

    d. K

    [2 marks]




11. If there were no affine transformation in AES S-Box (S), then

    **a. S(0) = 0 (0 maps to 0)**

    b. S-Box will become linear

    c. S-box will become identity mapping

    d. All of the above

    [2 marks]

12. In the polynomial basis representation with irreducible polynomial $r(y) = y^2 + \tau y + \mu$, in the composite field $GF((2^4)^2)$ the inverse is represented as $(\delta_1 y + \delta_0)$. $\delta_1$ and $\delta_0$ belongs to

**a.** $GF(2^4)$

b. $GF((2^4)^2)$

c. $GF(2^8)$

d. None of the above

[1 mark]

13. While defining finite extension fields with irreducible polynomials

**a. Degree of the irreducible polynomial should be equal to the logarithm of the order of the field.**

b. Degree of the irreducible polynomial should be greater than the logarithm of the order of the field

c. Degree of the irreducible polynomial should be lesser than the logarithm of the order of the field

d. No such relationship exists

[1 mark]

14. To represent a finite field

a. The irreducible polynomial must be primitive polynomial

**b. The irreducible polynomial may not be primitive polynomial**

c. You do not need primitive polynomial

d. None of the above

[1 mark]

15. Squaring in finite field is usually represented as

**a. A linear operation**

b. A finite field operation

c. A multiplication operation

d. None of the above

[1 mark]

16. Let A=T.B, where A and B are 1 x 4 matrices, and T is a 4 x 4 matrix. $B = A^{2^4}$, where A and B are field elements represented in matrix format. The first row of the matrix T for exponentiation by $2^4$ in GF($2^4$)field (say irreducible polynomial = $x^4 + x + 1$) is

a. 1000
b. 1010
**c. 1100**
d. 0110

[5 marks]

17. The addition chains in Itoh-Tsujii inversion algorithm are used to reduce the number of multiplications required. Let $a \in GF(2^{163})$ and you are asked to find $a^{-1}$ using following addition chain

[1, 2, 4, 5, 10, 20, 40, 80, 81, 162]

The number of squarings required in a naïve implementation without addition chain would take

**a. 162 squarings and 161 multiplications**

b. 163 squarings and 161 multiplications

c. 161 squarings and 161 multiplications

d. 163 squarings and 163 multiplications

[2 marks]

18. The addition chains in Itoh-Tsujii inversion algorithm are used to reduce the number of multiplications required. Let $a \in GF(2^{163})$ and you are asked to find $a^{-1}$ using following addition chain

[1, 2, 4, 5, 10, 20, 40, 80, 81, 162]

The number of squarings required with addition chains is

**a. 162**

b. 163

c. 164

d. 165

[2 marks]

19. The addition chains in Itoh-Tsujii inversion algorithm are used to reduce the number of multiplications required. Let $a \in GF(2^{163})$ and you are asked to find $a^{-1}$ using following addition chain

[1, 2, 4, 5, 10, 20, 40, 80, 81, 162]

The number of multiplications required with addition chain is

a. 10

**b. 9**

c. 11

d. 8

[2 marks]

20. The delay of a squarer and a quad for Itoh-Tsujii Algorithm are the same; because

**a. Both have the same delay of 1 LUT**

b. Quad requires lesser number of steps

c. Quad requires lesser number of operations

d. None of the above

[2 marks]

21. Let us assume that we have to perform an inverse on $GF(2^m)$, with an addition chain of length $l$ using a quad circuit. The number of multiplications required

a. $l - 1$

b. $l$
**c.** $l + 1$
d. none

[2 marks]

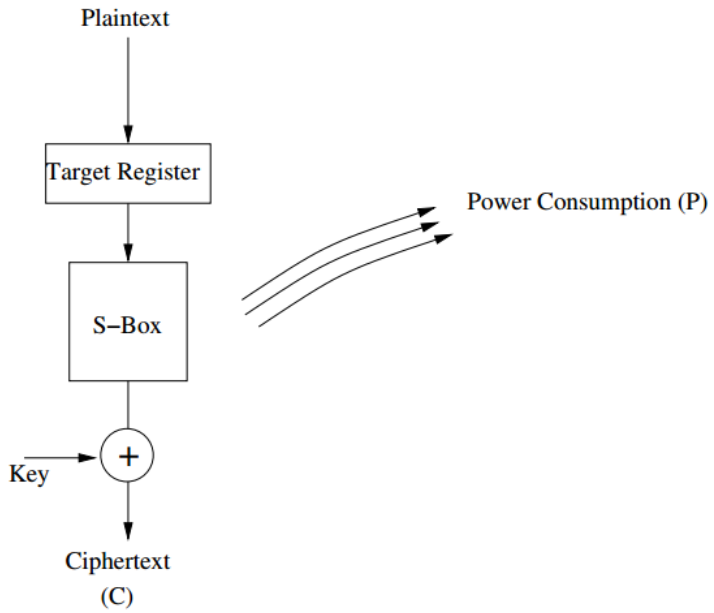
22. Pentanomial $x^4 + x^3 + x^2 + x + 1$ in GF($2^4$) field is:

**a. Irreducible**
b. Primitive
c. Both
d. none

[5 marks]

23. Consider a toy cipher as shown in the below Figure implemented on a smart card. The cipher has a 4 bit plaintext which is not visible to the adversary. However, the adversary has access to the ciphertexts and also the corresponding power consumptions which are represented as integer values. The S-Box of the cipher is as in the following table:

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $S[X]$ | C | 5 | 6 | B | 9 | 0 | A | D | 3 | E | F | 8 | 4 | 7 | 1 | 2 |




The adversary runs the encryptions several times until it obtains all the unique 16 ciphertext values (denoted as C) at least once. It also notes the corresponding power values denoted as P which are denoted in the following table:

| C | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| P | 10 | 15 | 20 | 5 | 10 | 5 | 5 | 15 | 15 | 5 | 10 | 10 | 0 | 15 | 10 | 10 |

a. The key is either 0101 or 1010. Apply the Difference-of-Mean (DOM) technique to determine which is the correct key byte. Target the MSB of the input of the S-Box. Correct key byte is _____0101_____.

[5 mark]