Final Exam

- Time: 10:30-13:15
- Do not use "písané písmo" but "paličkové".
- Write your answers on the provided answer sheets. Additional sheets will be supplied upon request. Please ensure that your full name is clearly written on each page of the answer sheets.
- Include detailed computation steps for all solutions. Answers without supporting calculations will receive a score of zero.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Table 1: PRESENT Sbox.

Question 1. (5 marks)

a) (2 mark) Find 21^{-1} mod 160 using the extended Euclidean algorithm

b) (3 marks) Let $f(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$. The set of congruence classes modulo $f(x)$ is a field, in particular:

$$\mathbb{F}_2[x]/(f(x)) = \left\{ \sum_{i=0}^{7} b_i x^i \;\middle|\; b_i \in \mathbb{F}_2 \ \forall i \right\} \cong \mathbb{F}_{2^8}$$

Define φ:

$$\begin{aligned} \varphi : \mathbb{F}_2[x]/(f(x)) &\to \mathbb{F}_2^8 \\ b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 &\mapsto b_7b_6b_5b_4b_3b_2b_1b_0 \end{aligned}$$

Then we have a 1-1 correspondence between elements in $\mathbb{F}_2[x]/(f(x))$ and binary string of length 8, or bytes. During the lecture, we have discussed that with addition and multiplication modulo $f(x)$ in $\mathbb{F}_2[x]/(f(x))$, we can define the corresponding addition and multiplication between bytes. We have also seen that the multiplicative inverse of $g(x) \in \mathbb{F}_2[x]/(f(x))$ can be found using the extended Euclidean algorithm. Consequently, we can find the inverse of a byte as an element in $\mathbb{F}_2[x]/(f(x))$.

Find inverse of $\texttt{5B}_{16} = 01011011_2$ as an element in $\mathbb{F}_2[x]/(f(x))$. Write the final answer in **hexadecimal** format.

Solution.

a) (2 marks) By the Euclidean algorithm:

$$\begin{aligned} 160 &= 21 \times 7 + 13 & 21 &= 13 \times 1 + 8 \\ 13 &= 8 \times 1 + 5 & 8 &= 5 \times 1 + 3 \\ 5 &= 3 \times 1 + 2 & 3 &= 2 \times 1 + 1 \end{aligned}$$

By the extended Euclidean algorithm:

$$\begin{array}{ll} 1 = 3 - 2, & 2 = 5 - 3 \\ 3 = 8 - 5, & 5 = 13 - 8 \\ 8 = 21 - 13, & 13 = 160 - 21 \times 7 \end{array}$$

$$\begin{aligned} 1 &= 3 - (5 - 3) = 3 \times 2 - 5 = 8 \times 2 - 5 \times 3 = 8 \times 2 - (13 - 8) \times 3 \\ &= 8 \times 5 - 13 \times 3 = 21 \times 5 - 13 \times 8 = 21 \times 5 - (160 - 21 \times 7) \times 8 \\ &= 21 \times 61 - 160 \times 8 \end{aligned}$$

Thus $21^{-1} \bmod 160 = 61$

b) (3 marks) By the Euclidean algorithm

$$\begin{aligned} f(x) &= (x^2+1)(x^6+x^4+x^3+x+1) + (x^5+x^3+x^2), \\ x^6+x^4+x^3+x+1 &= x(x^5+x^3+x^2) + (x+1), \\ x^5+x^3+x^2 &= (x^4+x^3+x+1)(x+1) + 1. \end{aligned}$$

By the extended Euclidean algorithm

$$\begin{aligned} 1 &= (x^5+x^3+x^2) + (x^4+x^3+x+1)(x+1) \\ &= (x^5+x^3+x^2) + (x^4+x^3+x+1)((x^6+x^4+x^3+x+1) + x(x^5+x^3+x^2)) \\ &= (x^4+x^3+x+1)(x^6+x^4+x^3+x+1) + (x^5+x^4+x^2+x+1)(x^5+x^3+x^2) \\ &= (x^4+x^3+x+1)(x^6+x^4+x^3+x+1) \\ &\quad +(x^5+x^4+x^2+x+1)(f(x) + (x^2+1)(x^6+x^4+x^3+x+1)) \\ &= (x^5+x^4+x^2+x+1)f(x) + (x^7+x^6+x^5+x^4)(x^6+x^4+x^3+x+1). \end{aligned}$$

We have

$$\begin{aligned} (x^6+x^4+x^3+x+1)^{-1} \bmod f(x) &= x^7+x^6+x^5+x^4 = 11110000_2 \\ &= \texttt{F0}. \end{aligned}$$

Question 2. (2 marks) Solve the following system of simultaneous linear congruences

$$\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 3 \bmod 5 \\ x &\equiv 2 \bmod 7 \\ x &= ? \bmod 105 \end{aligned}$$

Solution. With the formula we have seen in the lecture, we have $m_1 = 3, m_2 = 5, m_3 = 7, a_1 = 2, a_2 = 3, a_3 = 2,$

$$m = 3 \times 5 \times 7 = 105, \quad M_1 = 35, \quad M_2 = 21, \quad M_3 = 15.$$

Then

$$M_1 = 35 \equiv 2 \bmod 3, \quad M_2 = 21 \equiv 1 \bmod 5, \quad M_3 = 15 \equiv 1 \bmod 7.$$

$$y_1 = M_1^{-1} \bmod 3 = 2, \quad y_2 = M_2^{-1} \bmod 5 = 1, \quad y_3 = M_3^{-1} \bmod 7 = 1.$$

$$\begin{aligned} x &= \sum_{i=1}^{3} a_i y_i M_i = 2 \times 2 \times 35 + 3 \times 1 \times 21 + 2 \times 1 \times 15 \bmod 105 \\ &= 233 \bmod 105 = 23 \bmod 105. \end{aligned}$$

Question 3. (8 marks) In this question, we consider RSA encryption and decryption. Suppose Bob would like to generate his private and public keys for RSA. Bob randomly generates $p = 29$ and $q = 41$.

a) (1 mark) Then he computes
$$n =? \quad \varphi(n) =?$$

b) (1 mark) From $\mathbb{Z}^*_{\varphi(n)}$, Bob chooses his private key $e = 3$. Compute using the extended Euclidean algorithm, the private key d for Bob.

c) (1 mark) Alice would like to send plaintext $m = 2$ to Bob, using Bob's public key n, e. Alice computes ciphertext
$$c =?$$

d) (2 marks) Bob receives a message $c = 142$ from Alice. Then to decrypt the message $c = 142$ with CRT-based RSA, Bob computes
$$m_p =? \quad m_q =? \quad y_p =? \quad y_q =?$$
Using Garner's algorithm, Bob gets
$$m =?$$

e) (3 marks) Now we consider a malicious attacker who carries out a Bellcore attack during the RSA decryption. Suppose she injects fault during the computation of m_p and the faulty $m'_p = 1$. Then the faulty message will be
$$m' =?$$
With the knowledge of m, m' and the public key n, e, how can the attacker recover the secret key d?

Solution.

a) (1 mark)
$$n = 29 \times 41 = 1189, \quad \varphi(n) = 28 \times 40 = 1120.$$

b) (1 mark) By the extended Euclidean algorithm
$$1120 = 3 \times 373 + 1 \Longrightarrow 1 = 1120 - 3 \times 373.$$
Hence Bob's private key $d = -373 \bmod 1120 = 747$.

c) (1 mark) Alice computes
$$c = m^e \bmod n = 2^3 \bmod 1189 = 8.$$

d) (2 marks) After receiving the ciphertext $c = 142$, with CRT-based RSA implementation, Bob computes

$$\begin{aligned} m_p &= c^{d \bmod (p-1)} \bmod p = 142^{747 \bmod 28} \bmod 29 = 26^{19} \bmod 29 = 11, \\ m_q &= c^{d \bmod (q-1)} \bmod q = 142^{747 \bmod 40} \bmod 41 = 19^{27} \bmod 41 = 11. \end{aligned}$$

To compute $26^{19} \bmod 29$, we note that

$$\begin{aligned} 26^2 \bmod 29 &= 9, \\ 26^4 \bmod 29 &= 9^2 \bmod 29 = 23, \\ 26^8 \bmod 29 &= 23^2 \bmod 29 = 7, \\ 26^{16} \bmod 29 &= 7^2 \bmod 29 = 20. \end{aligned}$$

Thus

$$26^{19} \bmod 29 = 26^{16} \times 26^2 \times 26 \bmod 29 = 20 \times 9 \times 26 \bmod 29 = 11.$$

Similarly,

$$\begin{aligned} 19^2 \bmod 41 &= 33 \\ 19^3 \bmod 41 &= 33 \times 19 \bmod 41 = 12 \\ 19^9 \bmod 41 &= 12^3 \bmod 41 = 6 \\ 19^{27} \bmod 41 &= 6^3 \bmod 41 = 11. \end{aligned}$$

By the extended Euclidean algorithm

$$41 = 29 + 12,\ 29 = 12 \times 2 + 5,\ 12 = 5 \times 2 + 2,\ 5 = 2 \times 2 + 1,$$

which gives

$$\begin{aligned} 1 &= 5 - 2 \times (12 - 5 \times 2) = -2 \times 12 + (29 - 12 \times 2) \times 5 \\ &= 29 \times 5 - 12 \times (41 - 29) = -41 \times 12 + 29 \times 17. \end{aligned}$$

We have

$$\begin{aligned} y_p &= p^{-1} \bmod q = 29^{-1} \bmod 41 = 17 \bmod 41, \\ y_q &= q^{-1} \bmod p = 41^{-1} \bmod 29 = -12 \bmod 29 = 17 \bmod 29. \end{aligned}$$

By Garner's algorithm,

$$m = m_p + ((m_q - m_p)y_p \bmod q)p = 11 + 0 = 11$$

e) (3 marks) The faulty message is given by

$$\begin{aligned} m' &= m'_p + ((m_q - m'_p)y_p \bmod q)p = 1 + ((11 - 1) \times 17 \bmod 41) \times 29 \\ &= 1 + 6 \times 29 = 175. \end{aligned}$$

According to the Bellcore attack,

$$q = \gcd(m' - m, n) = \gcd(175 - 11, 1189) = \gcd(164, 1189).$$

By the Euclidean algorithm

$$\begin{aligned} 1189 = 164 \times 7 + 41, &\quad \gcd(164, 1189) = \gcd(164, 41), \\ 164 = 41 \times 4, &\quad \gcd(164, 41) = 41. \end{aligned}$$

Hence $q = 41$ and

$$p = \frac{n}{q} = 29.$$

Then the attacker can compute

$$\varphi(n) = (p-1)(q-1) = 1120.$$

The private key

$$d = e^{-1} \bmod \varphi(n) = 3^{-1} \bmod 1120.$$

can be found using the extended Euclidean algorithm.

Question 4. (5 marks) We have learned that

Theorem 1. Every Boolean function $\varphi : \mathbb{F}_2^n \to \mathbb{F}_2$ has a unique algebraic normal form representation

$$\varphi(\boldsymbol{x}) = \sum_{\boldsymbol{v} \in \mathbb{F}_2^n} \left(\lambda_{\boldsymbol{v}} \prod_{i=0}^{n-1} x_i^{v_i} \right),$$

the coefficients $\lambda_{\boldsymbol{v}} \in \mathbb{F}_2$ are given by

$$\lambda_{\boldsymbol{v}} = \sum_{\boldsymbol{w} \leq \boldsymbol{v}} \varphi(\boldsymbol{w}),$$

where $\boldsymbol{w} \leq \boldsymbol{v}$ means that $w_i \leq v_i$ for all $0 \leq i \leq n-1$.

The 1**st bit** of PRESENT Sbox output is a Boolean function $\varphi_1 : \mathbb{F}_2^4 \to \mathbb{F}_2$, find the algebraic normal form for φ_1.

Solution. We can construct the following truth table:

$\boldsymbol{x}$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x_3	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
x_2	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$\mathrm{SB}_{\mathrm{PRESENT}}(\boldsymbol{x})$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2
$\varphi_1(\boldsymbol{x})$	0	0	1	1	0	0	1	0	1	1	1	0	0	1	0	1
$\lambda_{\boldsymbol{x}}$	0	0	1	0	0	0	0	1	1	0	1	1	1	1	0	0

The algebraic normal form of φ_1 is then given by

$$\begin{aligned} \varphi_1(\boldsymbol{x}) &= \sum_{\boldsymbol{v} \in \mathbb{F}_2^n} \left(\lambda_{\boldsymbol{v}} \prod_{i=0}^{n-1} x_i^{v_i} \right) = \lambda_{0010} x_1 + \lambda_{0111} x_2 x_1 x_0 + \lambda_{1000} x_3 + \lambda_{1010} x_3 x_1 \\ &\quad + \lambda_{1011} x_3 x_1 x_0 + \lambda_{1100} x_3 x_2 + \lambda_{1101} x_3 x_2 x_0 \\ &= x_1 + x_3 + x_1 x_3 + x_2 x_3 + x_0 x_1 x_2 + x_0 x_1 x_3 + x_0 x_2 x_3 \end{aligned}$$

Question 5. (5 marks) In the context of power analysis attacks, we model the leakage at one time sample t, denoted by L_t, as the sum of the signal X_t and noise N_t. Signal refers to the part of the leakage that contains useful information for our attack and the rest is noise. We consider X_t and N_t to be independent.

We have defined the signal-to-noise ratio (SNR) at time sample t to be

$$\mathrm{SNR} = \frac{\mathrm{Var}(X_t)}{\mathrm{Var}(N_t)}.$$

Suppose we are interested in the Hamming weight of an $8-$bit intermediate value at time sample t. In particular, the intermediate value we would like to analyze is from $\mathbb{F}_2^8$. We further assume that the leakage L_t is given by the Hamming weight model.

a) (1 mark) What is X_t for a $\boldsymbol{v} \in \mathbb{F}_2^8$?

b) (3 mark) Compute $\mathrm{Var}(X_t)$.

c) (1 mark) Let σ^2 denote the variance of the noise N_t. Compute the SNR at time sample t.

Solution.

a) (1 mark) $X_t = \mathrm{wt}(\boldsymbol{v})$ for some $\boldsymbol{v} \in \mathbb{F}_2^8$.

b) (3 marks) The variance of the signal is given by $\mathrm{Var}(\mathrm{wt}(\boldsymbol{v}))$ for all $\boldsymbol{v} \in \mathbb{F}_2^8$.

$$\begin{aligned}\mathrm{E}[\mathrm{wt}(\boldsymbol{v})] &= \frac{1}{|\mathbb{F}_2^8|}\sum_{\boldsymbol{v}\in\mathbb{F}_2^8}\mathrm{wt}(\boldsymbol{v}) = \frac{1}{2^8}\sum_{i=1}^{8} i\binom{8}{i} = \frac{1}{2^8}\sum_{i=1}^{8}\frac{8!}{(i-1)!(8-i)!} \\ &= \frac{8}{2^8}\sum_{i=1}^{8}\frac{7!}{(i-1)!(7-(i-1))!} = \frac{8}{2^8}\sum_{j=0}^{7}\binom{7}{j} = \frac{8\times 2^7}{2^8} = 4.\end{aligned}$$

Similarly, we can get

$$\mathrm{E}\left[\mathrm{wt}(\boldsymbol{v})^2\right] = 18$$

Then

$$\mathrm{Var}(X_t) = \mathrm{Var}(\mathrm{wt}(\boldsymbol{v})) = 18 - 4^2 = 2.$$

c) (1 mark)

$$\mathrm{SNR} = \frac{\mathrm{Var}(X_t)}{\mathrm{Var}(N_t)} = \frac{2}{\sigma^2}.$$

Question 6. (5 marks) The stochastic leakage model assumes each bit of the target intermediate value $\boldsymbol{v} = v_{m_v-1}v_{m_v-2}\ldots v_1v_0$ has a different leakage.

$$\mathcal{L}(\boldsymbol{v}) = \sum_{s=0}^{m_v-1}\alpha_s v_s + \text{noise},$$

where noise $\sim \mathcal{N}(0,\sigma^2)$ denotes the noise with variance σ^2 and α_s $(s = 0, 1, \ldots, m_v - 1)$ are real numbers. We have discussed how to profile the DUT to find estimations for α_s. Let

$$\boldsymbol{\ell}_{pf} := (l_{\mathrm{POI}}^{1,pf}, l_{\mathrm{POI}}^{2,pf}, \ldots, l_{\mathrm{POI}}^{M_{pf},pf})$$

be the vector of leakages at $t =$POI from all M_{pf} profiling traces, where $l_{\mathrm{POI}}^{j,pf}$ is the leakage at POI from the jth profiling trace.

Furthermore, for the jth profiling trace, let

$$\boldsymbol{v}_j^{pf} = v_{j(m_v-1)}^{pf}\ldots v_{j1}^{pf}v_{j0}^{pf}, \quad j = 1, 2, \ldots, M_{pf}$$

be the corresponding target intermediate value. Then we compute matrix $M_{\boldsymbol{v}}$

$$M_{\boldsymbol{v}} := \begin{pmatrix} v_{10}^{pf} & v_{11}^{pf} & \cdots & v_{1(m_v-1)}^{pf} \\ v_{20}^{pf} & v_{21}^{pf} & \cdots & v_{2(m_v-1)}^{pf} \\ \vdots & \vdots & \ddots & \vdots \\ v_{M_{pf}0}^{pf} & v_{M_{pf}1}^{pf} & \cdots & v_{M_{pf}(m_v-1)}^{pf} \end{pmatrix}$$

The estimated values $\hat{\alpha}_s$ for α_s are given by

$$(\hat{\alpha}_0, \hat{\alpha}_1, \ldots, \hat{\alpha}_{m_v-1}) = \left(M_{\boldsymbol{v}}^T M_{\boldsymbol{v}}\right)^{-1} M_{\boldsymbol{v}}^T \boldsymbol{\ell}_{pf}.$$

Suppose we are interested in the computation of the first round of PRESENT. Our target intermediate value $\boldsymbol{v}$ is the 0th Sbox output in the first round. We have collected $M_{pf} = 5000$ traces.

a) (2 marks) The first trace in our dataset corresponds to the 0th nibble of the plaintext= `4` and the 0th nibble of the first round key= `7`. Thus the intermediate value for the first trace is given by:
$$\boldsymbol{v}_1^{pf} = ?$$

b) (1 mark) The first row of our matrix $M_{\boldsymbol{v}}$ is given by?

c) (1 mark) Suppose we got the following estimated values for α_ss:
$$\hat{\alpha}_0 \approx -0.02019, \quad \hat{\alpha}_1 \approx -0.02027, \quad \hat{\alpha}_2 \approx -0.01920, \quad \hat{\alpha}_3 \approx -0.02039.$$
Then according to the stochastic leakage model, the leakage of $\boldsymbol{v} = v_3v_2v_1v_0$ is given by
$$\mathcal{L}(\boldsymbol{v}) = ?.$$

d) (1 mark) In particular,
$$\mathcal{L}(\mathtt{E}) = ?$$

Solution.

a) The first trace in our dataset corresponds to the 0th nibble of the plaintext= `4` and the 0th nibble of the first round key= `7`. Thus the intermediate value for the first trace is given by:
$$\boldsymbol{v}_1^{pf} = \mathrm{SB}_{\mathrm{PRESENT}}(\mathtt{4} \oplus \mathtt{7}) = \mathrm{SB}_{\mathrm{PRESENT}}(\mathtt{3}) = \mathtt{B} = 1011_2.$$

b) And the first row of our matrix $M_{\boldsymbol{v}}$ is given by
$$\begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix}.$$

c) The leakage of a $\boldsymbol{v} = (v_0, v_1, v_2, v_3)$ is given by
$$\mathcal{L}(\boldsymbol{v}) = \hat{\alpha_0}v_0 + \hat{\alpha_1}v_1 + \hat{\alpha_2}v_2 + \hat{\alpha_3}v_3 + \text{noise}.$$

d) $\mathcal{L}(\mathtt{E}) = \hat{\alpha_1} + \hat{\alpha_2} + \hat{\alpha_3} + \text{noise} = -0.05986 + \text{noise}$.

Question 7. (10 marks) For an Sbox SB: $\mathbb{F}_2^{\omega_1} \to \mathbb{F}_2^{\omega_2}$, the *(extended) difference distribution table (DDT)* of SB is a $2-$dimensional table T of size $(2^{\omega_1}-1)\times 2^{\omega_2}$ such that for any $0 < \delta < 2^{\omega_1}$ and $0 \le \Delta < 2^{\omega_2}$, the entry of T at the Δth row and δth column is given by

$$T[\Delta, \delta] = \{\, \boldsymbol{a} \;\mid\; \boldsymbol{a} \in \mathbb{F}_2^{\omega_1}, \mathrm{SB}(\boldsymbol{a} \oplus \delta) \oplus \mathrm{SB}(\boldsymbol{a}) = \Delta \,\}.$$

Let SB be the following Sbox

x	0	1	2	3	4	5	6	7
SB(x)	4	7	0	5	2	6	3	1

Define

$$\begin{aligned} f : \mathbb{F}_2^3 &\to \mathbb{F}_2^3 \\ \boldsymbol{x} &\mapsto \mathrm{SB}(\boldsymbol{x} \oplus \boldsymbol{a}) \oplus \boldsymbol{b}. \end{aligned}$$

We consider a differential fault analysis attack on f. Our attack assumption is as follows:

- Fault location: input of f
- Fault model: bit flip
- Fault mask: $\varepsilon \in \mathbb{F}_2^4$ s.t. $\boldsymbol{x}' = \boldsymbol{x} \oplus \varepsilon$
- Attacker knowledge: Sbox design, inputs and outputs of f, fault mask
- Attacker goal: recover values of $\boldsymbol{a}$ and $\boldsymbol{b}$
- The Attacker can repeat the computation with the same input (not chosen by the attacker)

We know that with input $\boldsymbol{x} = 3$, the correct output is 4.

a) (4 marks) Complete the DDT for SB

Δ \ δ	1	2	3	4	5	6	7
1		?	?	?	?		
2	?	13			05	24	
3	01		?	?		?	
4	45	02		37			16
5	23		56		14		07
6				04	36	17	25
7		57	12			06	34

b) (2 marks) Suppose the attacker injects one fault with fault mask $\varepsilon_1 = 2$ and the resulting output is 6. What do we know about $\boldsymbol{a}$?

c) (4 marks) Suppose the attacker injects another fault with fault mask $\varepsilon_2 = 3$ and the resulting output is 3. Find the values of $\boldsymbol{a}$ and $\boldsymbol{b}$.

Solution.

a) (4 marks)

Δ \ δ	1	2	3	4	5	6	7
1		46	03	15	27		
2	67	13			05	24	
3	01		47	26		35	
4	45	02		37			16
5	23		56		14		07
6				04	36	17	25
7		57	12			06	34

b) (2 marks) For a fault mask ε, let Δ denote the difference between the correct and faulty output, then

$$\begin{aligned}\Delta &= (\mathrm{SB}(\boldsymbol{x} \oplus \boldsymbol{a}) \oplus \boldsymbol{b}) \oplus (\mathrm{SB}(\boldsymbol{x}' \oplus \boldsymbol{a}) \oplus \boldsymbol{b}) = \mathrm{SB}(\boldsymbol{x} \oplus \boldsymbol{a}) \oplus \mathrm{SB}(\boldsymbol{x}' \oplus \boldsymbol{a}) \\ &= \mathrm{SB}(\boldsymbol{x} \oplus \boldsymbol{a}) \oplus \mathrm{SB}(\boldsymbol{x} \oplus \boldsymbol{a} \oplus \varepsilon).\end{aligned}$$

We can conclude that he value $\boldsymbol{x} \oplus \boldsymbol{a}$ is in the entry of DDT corresponding to input difference $\delta = \varepsilon$ and output difference Δ.
With fault mask 2 and

$$\Delta = 4 \oplus 6 = 2,$$

we know that the value $\boldsymbol{x} \oplus \boldsymbol{a}$ is in the entry of DDT corresponding to input difference 2 and output difference 2. Thus the possible values of $\boldsymbol{x} \oplus \boldsymbol{a}$ are given by 1 and 3. Knowing that $\boldsymbol{x} = 3$, the possible values of $\boldsymbol{a}$ are 2 and 0.

c) (4 marks) Similarly, with fault mask 3 and

$$\Delta = 4 \oplus 3 = 7,$$

we know that the value $\boldsymbol{x} \oplus \boldsymbol{a}$ is in the entry of DDT corresponding to input difference 3 and output difference 7. Thus the possible values of $\boldsymbol{x} \oplus \boldsymbol{a}$ are given by 1 and 2. Knowing that $\boldsymbol{x} = 3$, the possible values of $\boldsymbol{a}$ are 2 and 1. Together with the previous answer, we know that the value of $\boldsymbol{a} = 2$.

We also know that when $\boldsymbol{x} = 3$,

$$\mathrm{SB}(3 \oplus \boldsymbol{a}) \oplus \boldsymbol{b} = 4,$$

which gives

$$\boldsymbol{b} = \mathrm{SB}(3 \oplus 2) \oplus 4 = \mathrm{SB}(1) \oplus 4 = 7 \oplus 4 = 3.$$