50.042 Foundations of Cybersecurity
Mid-term Exam Practice Questions

Multiple Choice Questions

Circle the correct answer. There is only **one** correct answer for each question.

1. (Ciphers) Which of the following is a block cipher?
   a. Caesar's cipher → shift cipher
   b. 3DES in ECB mode
   c. SHA-1 hash
   d. OTP → stream cipher.

2. (Modular Arithmetic) What is the logic gate that can be used for **addition** in the field $GF(2)$?
   a. AND
   b. XOR
   c. OR
   d. NAND

3. (Security) What is ***confidentiality***, in the context of cybersecurity?
   a. It is the property that an attacker is not able to decipher any secret data that is being transmitted between legitimate parties
   b. It is the property that an attacker is unable to modify the data that is being transmitted between legitimate parties without being detected
   c. It is the property that the services provided by some party are resilient against interruptions caused by an attacker
   d. It is the property that the identity of the legitimate parties, that are transmitting secret data to each other, are kept confidential

integrity → b
availability → c
privacy → d

4. (Hash functions) The complexity of finding a **collision** for a hash function with an n-bit output is:
   a. $O(n^2)$
   b. $O(n)$
   c. $O(2^n)$
   d. $O(2^{n/2})$

Birthday paradox

2nd preimage attack ?,

5. (Modular Arithmetic) Which one of the following statements is **false**?
   a. $(\mathbb{Z}, \cdot)$ is not a group *('·' is the regular multiplication operation)*
   b. $(\mathbb{Z}_5, +, \cdot)$ is an integer ring *('+' and '·' are modulo 5 operations)*
   c. A finite field with an order of 20 exists
   d. A finite field with an order of 125 exists

text book definition of integer ring

composite number so field cannot exist

$2^2(5)$

5^3, prime power → is a field

6. (Block ciphers) Which of the following statements is **true** regarding the **AES** cipher?
   a. It uses a Feistel network
   b. It does not use any substitution-boxes (i.e. *S*-boxes)
   c. All operations used in AES are invertible
   d. The AES encryption/decryption process involves only one round

DES network

it does

true

layered structure

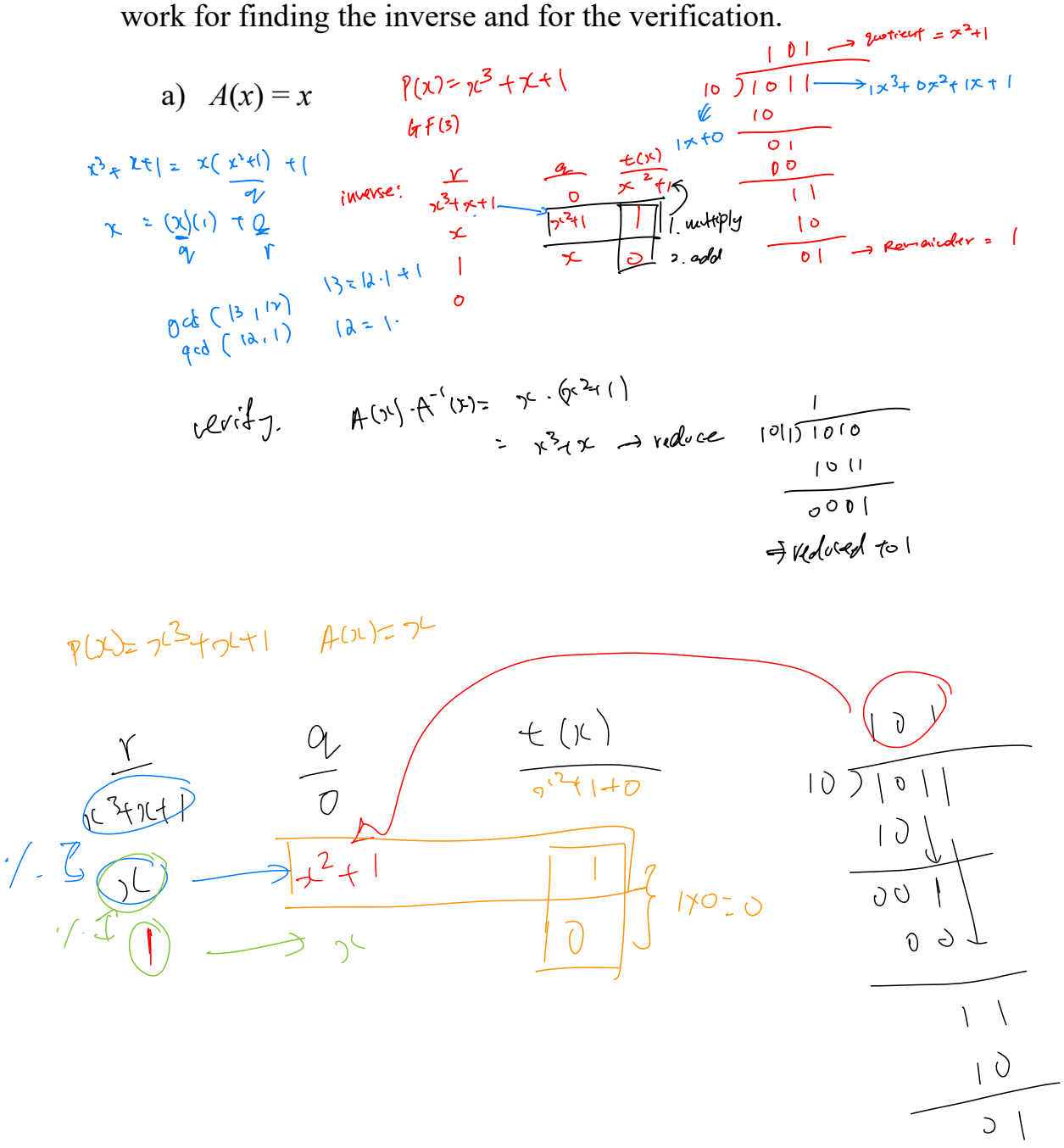
DES operations invertible?

→ no need to invert.

Short answer questions

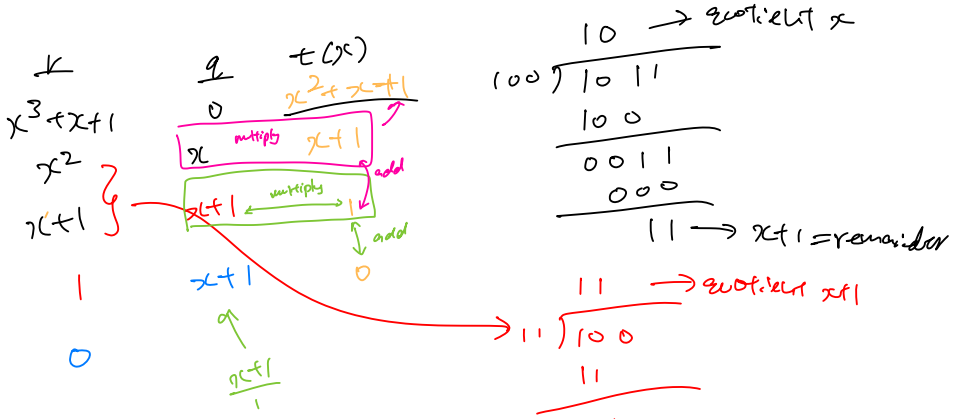
1. (Modular arithmetic) Find the **inverse** of the following polynomials in $GF(2^3)$, using the irreducible polynomial $\boldsymbol{P(x) = x^3 + x + 1}$. After finding each inverse, verify your answer by performing polynomial multiplication of the inverse with its respective polynomial, followed with a reduction by $P(x)$. In other words, after multiplication of a polynomial with its inverse, you should obtain **1** ***mod*** $\boldsymbol{P(x)}$. Show your work for finding the inverse and for the verification.

   a) $A(x) = x$



b) $B(x) = x^2 \Rightarrow 100$

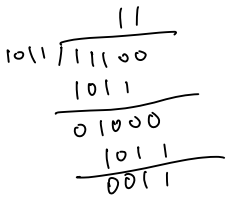
Inverse finding



$B(x)B^{-1}(x) = x^2(x^2+x+1)$

$= x^4 + x^3 + x^2$

reduce $x^4 + x^3 + x^2 \bmod P(x)$

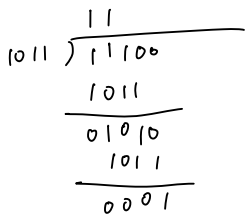


verify: $B(x) = x^2$

$B(x) \cdot B^{-1}(x) = x^2(x^2+x+1)$

$= x^4 + x^3 + x^2 \rightarrow$ now reduce with $P(x)$

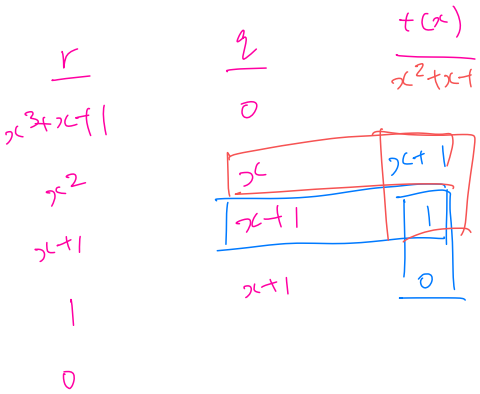
$\Rightarrow$

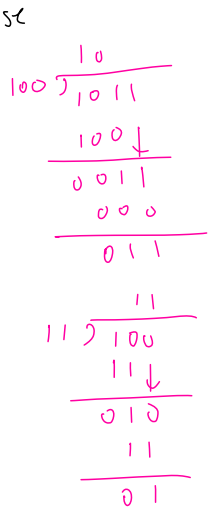


$\Rightarrow$ reduced to 1

verified inverse as 1 is identity element.

$B(x) = x^2 \quad P(x) = x^3 + x + 1$



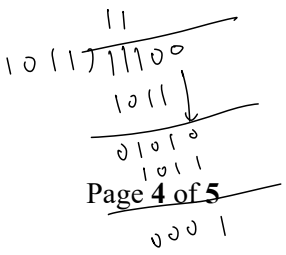


$B(x)B^{-1}(x) = x^2(x^2+x+1)$

$= x^4 + x^3 + x^2$

reduce $x^4 + x^3 + x^2 \bmod P(x)$

$\Rightarrow$ reduce $= 1 \bmod P(x)$



2. (Brute force attacks and feasibility) Suppose Oscar wishes to execute a brute force attack on the AES cipher.
He plans to do this by conducting an exhaustive key search attack, that is, by trying each and every one of the possible keys to decrypt a ciphertext message that was encrypted using the AES block cipher with a **128-bit** key length.

brute force

Oscar has access to a black market *application-specific integrated circuit* (ASIC) that is able to test 5×10^8 keys **per second**. Each of these ASICs costs $100 to purchase on the black market. Oscar has a budget of $1,000,000 and he is willing to purchase as many ASICs as necessary to minimize the overall time taken to perform the exhaustive key search.

a) How many ASICs can Oscar operate in parallel with his budget? Assume that the cost of operating the ASICs is negligible.

$10^6 / 10^2 = 10^4$

b) How long would it take for Oscar to complete the exhaustive key search attack, in **years**? Assume that there are 365 days in every year. Express your answer in scientific form with 2 significant figures (e.g. 3.2×10^{12}, 1.4×10^7, etc.).

$$\frac{2^{128}}{10^4 \times 5 \times 10^8 \times 365 \times 60^2 \times 24} = 2.2 \times 10^{18} \text{ years}$$