How is multiplication performed in Galois Fields in the context of the AES algorithm?

THURSDAY, 03 AUGUST 2023 PUBLISHED IN CYBERSECURITY, EITC/IS/CCF CLASSICAL CRYPTOGRAPHY FUNDAMENTALS, AES BLOCK CIPHER CRYPTOSYSTEM, INTRODUCTION TO GALOIS FIELDS FOR THE AES, EXAMINATION REVIEW

In the context of the AES algorithm, multiplication in Galois Fields (GF) plays a important role in the encryption and decryption processes. The AES block cipher cryptosystem employs Galois Fields extensively to achieve its security objectives. To understand how multiplication is performed in Galois Fields within the AES algorithm, it is necessary to consider the concepts of Galois Fields, finite fields, and polynomial arithmetic.

Galois Fields, also known as finite fields, are mathematical structures that exhibit properties similar to those of ordinary arithmetic, but with a finite set of elements. The AES algorithm utilizes a specific Galois Field known as GF(2^8), which consists of 256 elements. Each element in this field can be represented as an 8-bit binary number, ranging from 00000000 to 11111111.

In GF(2^8), addition and subtraction are performed using the exclusive OR (XOR) operation, which is equivalent to binary addition without carry. Multiplication in GF(2^8) is more intricate and involves the use of irreducible polynomials. An irreducible polynomial is a polynomial of degree n that cannot be factored into the product of two lower-degree polynomials over GF(2^8).

To multiply two elements in GF(2^8), we utilize a multiplication algorithm known as the "carry-less multiplication" or "bitwise multiplication" algorithm. This algorithm is based on the concept of polynomial multiplication, where the binary representation of each element is treated as a polynomial.

Let's take two elements in GF(2^8), A and B, represented as binary numbers A = a7a6a5a4a3a2a1a0 and B = b7b6b5b4b3b2b1b0. To multiply A and B, we perform the following steps:

1. Initialize a result variable, R, to zero.
2. For each bit in B, starting from the least significant bit (b0):
a. If the current bit is 1, XOR R with A.
b. If the most significant bit of A is 1, left-shift A by one bit and XOR it with the irreducible polynomial, m(x).
c. Right-shift B by one bit.

The irreducible polynomial m(x) used in AES is x^8 + x^4 + x^3 + x + 1, which can be represented as 0x1B in hexadecimal notation.

Let's illustrate the multiplication of two elements, A = 10111001 and B = 00011110, in GF(2^8):

1. Initialize R = 00000000.
2. b0 = 0: No action required.
3. b1 = 1: XOR R with A, resulting in R = 10111001.
a. R = 00000000 XOR 10111001 = 10111001.
4. b2 = 1: XOR R with A, resulting in R = 00000001.
a. R = 10111001 XOR 10111001 = 00000000.
b. Left-shift A by one bit and XOR with m(x):
i. A = 01110010 XOR 00011011 = 01101001.
5. b3 = 1: XOR R with A, resulting in R = 01101001.
a. R = 00000000 XOR 01101001 = 01101001.
6. b4 = 1: XOR R with A, resulting in R = 01010010.
a. R = 01101001 XOR 01101001 = 01010010.
b. Left-shift A by one bit and XOR with m(x):
i. A = 11010010 XOR 00011011 = 11001001.
7. b5 = 0: No action required.
8. b6 = 0: No action required.
9. b7 = 0: No action required.

After performing all the steps, the final result R is 01010010, which corresponds to the product of A and B in GF(2^8).

It is important to note that multiplication in Galois Fields is not commutative, meaning that A * B may not be equal to B * A. Therefore, the order of the elements being multiplied is significant.

Multiplication in Galois Fields within the AES algorithm involves the use of irreducible polynomials and the carry-less multiplication algorithm. By treating the elements as polynomials and performing XOR and left-shift operations, the AES algorithm achieves multiplication in GF(2^8) to ensure the security of the encryption and decryption processes.

Other recent questions and answers regarding AES block cipher cryptosystem:

- Are AES based on finite fields?
- What are the properties of a field?
- Did Rijndael cipher win a competition call by NIST to become the AES cryptosystem?
- Can we tell how many irreducible polynomial exist for GF(2^m) ?
- Why in FF GF(8) irreducible polynomial itself does not belong to the same field?
- What is the AES MixColumn Sublayer?
- Can a field be considered as a set of numbers in which one can add, subtract and multiple but not divide?
- Is the AES cryptosystem based on finite fields?
- Explain the significance of the key size and the number of rounds in AES, and how they impact the level of security provided by the algorithm.
- What are the main operations performed during each round of the AES algorithm, and how do they contribute to the overall security of the encryption process?

View more questions and answers in AES block cipher cryptosystem

More questions and answers:

- Field: Cybersecurity
- Programme: EITC/IS/CCF Classical Cryptography Fundamentals (go to the certification programme)
- Lesson: AES block cipher cryptosystem (go to related lesson)
- Topic: Introduction to Galois Fields for the AES (go to related topic)
- Examination review

Your order

Featured

IT ID

EITCA reviews (Reddit publ.)

About

Contact

Eligibility for EITCA Academy 80% EITCI DSJC Subsidy support

80% of EITCA Academy fees subsidized in enrolment by 19/11/2024

Your valid e-mail address ...

SEND THE SUBSIDY CODE

EITCA Academy Secretary Office

European IT Certification Institute ASBL
Brussels, Belgium, European Union

EITC / EITCA Certification Framework Operator
Governing European IT Certification Standard
Access contact form or call +32 25887351

Follow EITCI on Twitter
Visit EITCA Academy on Facebook
Engage with EITCA Academy on LinkedIn
Check out EITCI and EITCA videos on YouTube

Funded by the European Regional Development Fund (ERDF) and the European Social Fund (ESF), governed by the EITCI Institute since 2008

Information Security Policy | DSRRM and GDPR Policy | Data Protection Policy | Record of Processing Activities | HSE Policy | Anti-Corruption Policy | Modern Slavery Policy

Terms and Conditions | Privacy Policy

CHAT WITH SUPPORT